Cisco MDS 9000 Series Command Reference

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

A Commands

1G-speed-mode

To configure 1 Gbps link speed on an IP storage interface on the Cisco MDS 24/10 port SAN Extension Module, use the **1G-speed-mode** command.

1G-speed-mode

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
7.3(0)DY(1)	This command was introduced.

Usage Guidelines

This command will only be accepted for an interface range of whole IPStorage port groups because all interfaces in an IPStorage port group must have the same link speed. IPStorage interface port groups are as follows:

- Cisco MDS 9250i Switch: 1-2
- Cisco MDS 24/10 port SAN Extension Module: 1-4, 5-8

Examples

The following example shows how to configure 1 Gbps link speed on an IP storage interface on Cisco MDS 24/10 port SAN Extension Module:

```
switch# config terminal
switch(config)# interface IPStorage 5/1-4
switch(config-if)# 1G-speed-mode
This speed change will disrupt FCIP/iSCSI traffic for 60 seconds on selected IPStorage
ports.If FCIP tunnels are configured please make sure max-bw <= 1000 Mbps and tcp-connections
 set to 2.
Do you wish to continue(y/n)? [n]
switch(config-if)# end
```

Related Commands

Command	Description
10G-speed-mode	Configures 10 Gbps link speed on an IP storage interface.
show ips status	Displays the operational speed of the IP storage interface.

10G-speed-mode (FC ports)

To enable 10 gig speed mode, use the 10G-speed-mode command. To disable this feature, use the no form of the command.

10G-speed-mode
no 10G-speed-mode

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Interface Configuration mode.

Command History

Release	Modification
5.x	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable the 10 Gig speed mode:

```
switch# config terminal
switch(config-if)# 10G-speed-mode
switch(config-if)#
```

Related Commands

Command	Description
show interface fc x/y brief	Displays the interface brief information.
show running-config interface fc **x/y**	Displays the running configuration of the interface.

10G-speed-mode (IP Storage Ports)

To configure 10 Gbps link speed on an IP storage interface on the Cisco MDS 24/10 port SAN Extension Module, use the **10G-speed-mode** command.

10G-speed-mode

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
7.3(0)DY(1)	This command was introduced.

Usage Guidelines

This command will only be accepted for an interface range of whole IPStorage port groups because all interfaces in an IPStorage port group must have the same link speed. IPStorage interface port groups are as follows:

- Cisco MDS 9250i Switch: 1-2
- Cisco MDS 24/10 port SAN Extension Module: 1-4, 5-8

Examples

The following example shows how to configure 10 Gbps link speed on an IP storage interface on Cisco MDS 24/10 port SAN Extension Module:

```
switch# config terminal
switch(config)# interface IPStorage 5/5-8
switch(config-if)# 10G-speed-mode
This speed change will disrupt FCIP/iSCSI traffic for 60 seconds on select IPStorage ports.
Do you wish to continue(y/n)? [n]
switch(config-if)# end
```

Related Commands

Command	Description
1G-speed-mode	Configures 1 Gbps link speed on an IP storage interface.
show ips status	Displays the operational speed of the IP storage interface.

16G-speed-mode

To enable 2, 4, 8 and 16G speed mode, use the 16G-speed-mode command. To disable this feature, use the no form of the command.

16G-speed-mode
no 16G-speed-mode

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Interface Configuration mode.

Command History

Release	Modification
6.x	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable the 16 Gig speed mode:

```
switch# config terminal
switch(config-if)# 16G-speed-mode
switch(config-if)#
```

Related Commands

Command	Description
show interface fc x/y brief	Displays the interface brief information.
show running-config interface fc **x/y**	Displays the running configuration of the interface.

aaa accounting default

To configure the default accounting method, use the aaa accounting default command. To revert to the default local accounting, use the **no** form of the command.

aaa accounting default {**group** {*group-name* **[none]|none**}|**local [none]|none**}
no aaa accounting default {**group** {*group-name* **[none]|none**}|**local [none]|none**}

Syntax Description

group *group-name*	Specifies the group authentication method. The group name is a maximum of 127 characters.
none	(Optional) No authentication, everyone permitted.
local	Specifies the local authentication method.

Command Default

Local accounting.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Specify the currently configured command preceded by a **no** in order to revert to the factory default.

Examples

The following example enables accounting to be performed using remote TACACS+ servers which are members of the group called TacServer, followed by the local accounting method:

```
switch# config t
switch(config)# aaa accounting default group TacServer
```

The following example turns off accounting:

```
switch(config)# aaa accounting default none
```

The following example reverts to the local accounting (default):

```
switch(config)# no aaa accounting default group TacServer
```

Related Commands

Command	Description
show aaa accounting	Displays the configured accounting methods.

aaa accounting logsize

To set the size of the local accounting log file, use the aaa accounting logsize command to set the size of the local accounting log file. To revert to the default log file size of 250000 bytes, use the **no** form of the command.

aaa accounting logsize *integer*
no aaa accounting logsize

Syntax Description

logsize	Configures local accounting log file size (in bytes).
integer	The size limit of the local accounting log file in bytes from 0 to 250000.

Command Default

25,0000.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows the log file size configured at 29000 bytes:

```
switch# config terminal
switch(config)# aaa accounting logsize 29000
```

Related Commands

Command	Description
show accounting logsize	Displays the configured log size.
show accounting log	Displays the entire log file.

aaa authentication dhchap default

To configure DHCHAP authentication method, use the **aaa authentication dhchap default** command in configuration mode. To revert to factory defaults, use the **no** form of the command.

aaa authentication dhchap default {**group** {*group-name* **[none]**|**none**}|**local [none]**|**none**}
no aaa authentication dhchap default {**group** {*group-name* **[none]**|**none**}|**local [none]**|**none**}

Syntax Description

group *group-name*	Specifies the group name authentication method. The group name is a maximum of 127 characters.
none	(Optional) Specifies no authentication.
local	Specifies local user name authentication (default).

Command Default

Local user name authentication.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The **local** option disables other authentication methods and configures local authentication to be used exclusively.

Specify the currently configured command preceded by a **no** in order to revert to the factory default.

Examples

The following example enables all DHCHAP authentication to be performed using remote TACACS+ servers which are members of the group called TacServers, followed by the local authentication:

```
switch# config terminal
switch(config)# aaa authentication dhchap default group TacServer
```

The following example reverts to the local authentication method (default):

```
switch(config)# no aaa authentication dhcahp default group TacServer
```

Related Commands

Command	Description
show aaa authentication	Displays the configured authentication methods.

aaa authentication iscsi default

To configure the iSCSI authentication method, use the **aaa authentication iscsi default** command in configuration mode. To negate the command or revert to factory defaults, use the **no** form of this command.

aaa authentication iscsi default {**group** {*group-name* **[none]**|**none**}|**local [none]**|**none**}
no aaa authentication iscsi default {**group** {*group-name* **[none]**|**none**}|**local [none]**|**none**}

Syntax Description

group *group-name*	Specifies the group name. The group name is a maximum of 127 characters.
none	(Optional) Specifies no authentication.
local	Specifies local user name authentication (default).

Command Default

Local user name authentication.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The **local** option disables other authentication methods and configures local authentication to be used exclusively.

Specify the currently configured command preceded by a **no** in order to revert to the factory default.

Examples

The following example enables all iSCSI authentication to be performed using remote TACACS+ servers which are members of the group called TacServers, followed by the local authentication:

```
switch# config terminal
switch(config)# aaa authentication iscsi default group TacServer
```

The following example reverts to the local authentication method (default):

```
switch(config)# no aaa authentication iscsi default group TacServer
```

Related Commands

Command	Description
show aaa authentication	Displays the configured authentication methods.

aaa authentication login

To configure the authentication method for a login, use the **aaa authentication login** command in configuration mode. To revert to local authentication, use the **no** form of the command.

aaa authentication login {{**default**|**fallback**|**error**|**local**|**group** *group-name* **[none]**|**none**|**local** **[none]**|**none**}|**console** {{**fallback**|**error**|**local**|*group-name* **[none]**|**none**}|**local** **[none]**|**none**|**error-enable**|**mschap enable**}}
no aaa authentication login {{**default**|**fallback**|**error**|**local**|**group** *group-name* **[none]**|**none**|**local** **[none]**|**none**}|**console** {{**fallback**|**error**|**local**|*group-name* **[none]**|**none**}|**local** **[none]**|**none**|**error-enable**|**mschap enable**}}

Syntax Description

default	Specifies the default method.
fallback	Specifies the fallback mechanism configuration error.
error	Specifies the authentication error. The maximum size is 32 characters.
local	Specifies the fallback to local authentication.
group *group-name*	Specifies the group name. The group name is a maximum of 127 characters.
none	(Optional) Sets no authentication; everyone is permitted.
local	Specifies the local authentication method.
console	Configures the console authentication login method.
error-enable	Enables login error message display.
mschap enable	Enables MS-CHAP authentication for login.

Command Default

Local user name authentication.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	Added fallback, error, and local keywords to the syntax description.
1.3(1)	This command was introduced.
3.0(1)	Added the **mschap** option.

Usage Guidelines

Use the **console** option to override the console login method.

Specify the currently configured command preceded by a **no** to revert to the factory default.

Examples

The following example shows how to configure a default method:

```
switch# config t
switch(config)# aaa authentication login default fallback error local
switch(config)#
```

The following example shows how to configure a console method:

```
switch# config t
switch(config)# aaa authentication login console fallback error local
switch(config)#
```

The following example enables all login authentication to be performed using remote TACACS+ servers, which are members of the group called TacServer, followed by the local login method:

```
switch# config t
switch(config)# aaa authentication login default group TacServer
```

The following example enables console authentication to use the group called TacServer, followed by the local login method:

```
switch(config)# aaa authentication login console group TacServer
```

The following example turns off password validation:

```
switch(config)# aaa authentication login default none
```

The following example reverts to the local authentication method (default):

```
switch(config)# no aaa authentication login default group TacServer
```

The following example enables MS-CHAP authentication for login:

```
switch(config)# aaa authentication login mschap enable
```

The following example reverts to the default authentication method for login, which is the Password Authentication Protocol (PAP):

```
switch(config)# no aaa authentication login mschap enable
```

Related Commands

Command	Description
show aaa authentication	Displays the configured authentication methods.

aaa authentication login ascii-authentication

To enable ASCII authentication, use the aaa authentication login ascii-authentication command. To disable this feature, use the no form of the command.

aaa authentication login ascii-authentication
no aaa authentication login ascii-authentication

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 4.1(3a)	aaa authentication login password-aging enable command changed to aaa authentication login ascii-authentication.

Usage Guidelines

Password aging notification is initiated when the user authenticates to a Cisco MDS 9000 switch with a TACACS+ account. The user is notified when a password is about to expire or has expired. If the password has expired, the user is prompted to change the password.

Note As of Cisco MDS SAN-OS Release 3.2(1), only TACACS+ supports password aging notification. If you try to use RADIUS servers by enabling this feature, RADIUSs will generate a SYSLOG message and authentication will fall back to the local database. Cisco ACS TACACS+ server must have chpass enabled as well.

- Password change—You can change your password by entering a blank password.
- Password aging notification—Notifies password aging. Notification happens only if the AAA server is configured and MSCHAP and MSCHAPv2 is disabled.
- Password change after expiration—Initiates password change after the old password expires. Initiation happens from the AAA server.

Note Password aging notification fails if you do not disable MSCHAP and MSCHAPv2 authentication.

Examples

The following example shows how to enable ASCII authentication:

```
switch(config)# aaa authentication login ascii-authentication
switch#(config)#
```

Related Commands

Command	Description
show aaa authentication login ascii-authentication	Displays the configured ASCII authentication method.

aaa authentication login chap enable

To enable CHAP authentication for login, use the aaa authentication login chap enable command. To disable CHAP authentication, use the no form of the command.

aaa authentication login chap enable
no aaa authentication login chap enable

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to enable CHAP authentication for login:

```
switch(config)# aaa authentication login chap enable
switch(config)#
```

Related Commands

Command	Description
show aaa authentication login CHAP	Displays CHAP authentication for login.

aaa authentication login mschapv2 enable

To enable MS-CHAPv2 authentication for login, use the aaa authentication login mschapv2 enable command. To disable MS-CHAPv2 authentication, use the no form of the command.

aaa authentication login mschapv2 enable
no aaa authentication login mschapv2 enable

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

MS-CHAPv2 cannot be configured when MS-CHAP or ASCII authentication is configured and also when a TACACS group is configured for authentication.

Examples

The following example shows how to enable MS-CHAPv2 authentication for login:

```
switch(config)# aaa authentication login mschapv2 enable
switch(config)#
```

Related Commands

Command	Description
show aaa authentication login mschapv2	Displays MS-CHAPv2 authentication for login.

aaa authorization

To configure authorization for a function, use the aaa authorization command. To disable authorization for a function, use the no form of the command.

aaa authorization {**commands|config-commands**} **default** {{[**group** *group-name*]|**[local]**}|{[**group** *group-name*]|**[none]**}}
no aaa authorization {**commands|config-commands**} **default** {{[**group** *group-name*]|**[local]**}|{[**group** *group-name*]|**[none]**}}

Syntax Description

commands	Specifies authorization for all exec-mode commands.
config-commands	Specifies authorization for all commands under config mode L2 and L3.
default	Specifies the default methods.
group **group-name**	(Optional) Specifies the server group and group name..
local	(Optional) Specifies the local username authentication.
none	(Optional) Specifies no authorization.

Command Default

Authorization is disabled for all actions (equivalent to the method keyword none). If the aaa authorization command for a particular authorization type is entered without a specifies named method list. The default method list is automatically applied to all interfaces or lines (where this authorization type applies for except those that have a named method list explicitly defined. A defined method list overrides the default method list if no default method list is defined, then no authorization takes place.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None

Examples

The following example shows how to configure authorization for a configuration command function:

```
switch(config)# aaa authorization config-commands default group tac1 local
switch(config)#
```

The following example shows how to configure authorization for a command function:

```
switch(config)# aaa authorization commands default group tac1 local none
switch(config)#
```

Related Commands

Command	Description
show aaa authorization all	Displays all authorization information.

aaa authorization ssh-certificate

To configure SSH certificate authorization, use the aaa authorization ssh-certificate command. To disable this feature, use the no form of the command.

aaa authorization ssh-certificate default [{**group**|**local**}]

Syntax Description

default	Specifies default SSH methods.
group	Specifies server groups.
local	Specifies local user name authentication.

Command Default

None

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None

Examples

```
The following example shows how to use local user name authentication:
switch(config)# aaa authorization ssh-certificate default local
switch(config)#
The following example shows how to specify server groups:
switch(config)# aaa authorization ssh-certificate default group ldap1
switch#
```

Related Commands

Command	Description
show aaa authorization all	Displays all authorization information.

aaa authorization ssh-publickey

To configure SSH public key authorization, use the aaa authorization ssh-publickey command. To disable this feature, use the no form of the command.

aaa authorization ssh-publickey default [{**group**|**local**}]
no aaa authorization ssh-publickey default [{**group**|**local**}]

Syntax Description

default	Specifies default SSH methods.
group	(Optional) Specifies server groups.
local	(Optional) Specifies local user name authentication.

Command Default

None

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None

Examples

```
The following example shows how to use local user name authentication:
switch(config)# aaa authorization ssh-publickey default local
switch(config)#
The following example shows how to specify server groups:
switch(config)# aaa authorization ssh-publickey default group ldap1
switch#
```

Command	Description
show aaa authorization all	Displays all authorization information.

aaa group server

To configure one or more independent server groups, use the **aaa group server** command in configuration mode. To remove the server group, use the **no** form of this command to remove the server group.

aaa group server {**radius**|**tacacs**+|**ldap**} *group-name* **server** *server-name* **no server** *server-name*
no aaa group server {**radius**|**tacacs**+|**ldap**} *group-name* **server** *server-name* **no server** *server-name*

Syntax Description

radius	Specifies the RADIUS server group.
tacacs+	Specifies the TACACS+ server group.
ldap	Specifies LDAP server group name.
group-name	Identifies the specified group of servers with a user-defined name. The name is limited to 64 alphanumeric characters.
no server *server-name*	Specifies the server name to add or remove from the server group.

Command Default

None

Command Modes

Sub configuration mode

Command History

Release	Modification
NX-OS 5.0(1)	Added ldap keyword to the syntax description.
1.3(1)	This command was introduced.

Usage Guidelines

You can configure these server groups at any time but they only take effect when you apply them to a AAA service using the **aaa authentication login** or the **aaa accounting** commands.

LDAP groups cannot be used for AAA accounting commands.

Examples

The following example shows how to configure LDAP server group name:

```
switch(config)# aaa group server ldap a
switch(config-ldap)#
switch# config terminal
switch(config)# aaa group server tacacs+ TacacsServer1
switch(config-tacacs+)# server ServerA
switch(config-tacacs+)# exit
switch(config)# aaa group server radius RadiusServer19
switch(config-radius)# server ServerB
switch(config-radius)# no server ServerZ
```

Related Commands

Command	Description
show aaa groups	Displays all configured server groups.
show radius-server groups	Displays configured RADIUS server groups.
show tacacs-server groups	Displays configured TACACS server groups.

abort

To discard a Call Home configuration session in progress, use the **abort** command in Call Home configuration submode.

abort

Syntax Description

This command has no other arguments or keywords.

Command Default

None

Command Modes

Call Home configuration submode

Command History

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

Usage Guidelines

None

Examples

The following example shows how to discard a Call Home configuration session in progress:

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

Related Commands

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

absolute-timeout

To set the interval for closing the connection, use the **absolute-timeout** command in line configuration mode. To restore the default, use the **no** form of this command.

absolute-timeout *minutes*
no absolute-timeout

Syntax Description

minutes	Number of minutes after which the user session will be terminated. The range is from 0 to 10000 minutes.

Command Default

No timeout interval is automatically set.

Command Modes

Line configuration

Command History

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

Usage Guidelines

Use the **absolute-timeout** command to configure the EXEC to terminate when the configured number of minutes occurs on the virtual terminal (vty) line. The **absolute-timeout** command terminates the connection after the specified time period has elapsed, regardless of whether the connection is being used at the time of termination. You can specify an absolute-timeout value for each port. The user is given 20 seconds notice before the session is terminated. You can use this command along with the **logout-warning** command to notify users of an impending logout.

Examples

The following example sets an interval of 60 minutes on line 5:

```
switch# configure terminal
switch(config)# line vty 5
switch(config-line)# absolute-timeout 60
```

Related Commands

Command	Description
logout-warning	Sets and displays a warning for users about an impending forced timeout.

action cli

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

action number [**.number2**] **cli command1** [**command2...**] **[local]**
no action number [**.number2**] **cli command1** [**command2...**] **[local]**

Syntax Description

number	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.
local	(Optional) Specifies the action that is to be executed in the same module on which the event occurs.

Command Default

None.

Command Modes

Embedded Event Manager 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 a CLI command:

```
switch# configure terminal
switch(config)# event manager applet cli-applet
switch(config-applet)# action 1.0 cli "show interface e 3/1"
switch(config-applet)#
```

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action counter

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

action number [**.number2**] **counter name counter value val op** {**dec**|**inc**|**nop**|**set**}
no action number [**.number2**] **counter name counter value val op** {**dec**|**inc**|**nop**|**set**}

Syntax Description

number .number2	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.
name name	The counter name can be any case-sensitive, alphanumeric string up to 32 characters.
value val	Specifies the value of the counter. The value can be an integer from 0 to 2147483647 or a substituted parameter.
op {dec | inc | nop | set}	The following operations can be performed: • dec—Decrement the counter by the specified value. • inc—Increment the counter by the specified value. • nop—Only print the specified value. • set—Set the counter to the specified value.

Command Default

None

Command Modes

Embedded Event Manager mode

Command History

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

Usage Guidelines

None

Examples

The following example shows how to set or modify the counter when the EEM counter applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet counter-applet
switch(config-applet)# action 2.0 counter name mycounter value 20 op
switch(config-applet)#
```

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action event-default

To execute the default action for the associated event, use the action event-default command. To disable the default action, use the no form of the command.

action number [**.number2**] **event-default**
no action number [**.number2**] **event-default**

Syntax Description

number . number2	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.

Command Default

None

Command Modes

Embedded Event Manager mode

Command History

Release	Modification
NX-OS 4.2(1)	Added a note.
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

If you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the event default action statement. For example, if you match a CLI command in a match statement, you must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute.

Examples

The following example shows how to specify that the default action of the event be performed when an EEM applet is triggered:

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

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action exception log

To log an exception if the specific conditions are encountered when an Embedded Event Manager (EEM) applet is triggered, use the action exception log command.

action number [**.number2**] **exception log module module syserr error devid id errtype type errcode code phylayer layer ports list harderror error** [**desc string**]

Syntax Description

number .number2	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.
module module	Records an exception for the specified module. Enter a module word.
syserr error	Records an exception for the specified system error. Enter an error word.
devid id	Records an exception for the specified device ID. Enter an ID word.
errtype type	Records an exception for the specified error type. Enter a type word.
errcode code	Records an exception for the specified error code. Enter a code word.
phylayer layer	Records an exception for the specified physical layer. Enter a layer word.
ports list	Records an exception for the specified ports. Enter a list word.
harderror error	The reset reason is a quoted alphanumeric string up to 80 characters.
desc string	(Optional) Describes the exception logging condition.

Command Default

None

Command Modes

Embedded Event Manager mode

Command History

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

Usage Guidelines

None

Examples

The following example shows how to log an EEM applet exception:

```
switch# configure terminal
switch(config)# event manager applet exception-applet
switch(config-applet)# action 1.42 exceptionlog module 1 syserr 13 devid 1 errtype fatal
errcode 13 phylayer 2 ports 1-42 harderror 13 desc “fatal exception logging”
switch(config-applet)#
```

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action forceshut

To configure a forced shutdown of a module, a crossbar, ASCII, or the entire switch when an Embedded Event Manager (EEM) applet is triggered, use the action forceshut command.

action number [**.number2**] **forceshut** [{**module slot**|**xbar xbar-number**}] **reset-reason string**

Syntax Description

number .number2	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.
module slot	(Optional) Specifies slot range. The range is from 1 to 10, or a substituted parameter.
xbar xbar-number	(Optional) Specifies an xbar number. The range is from 1 to 4 or a substituted parameter.
reset-reason string	Specifies reset reason. The reason is an alphanumeric string up to 80 characters.

Command Default

None

Command Modes

Embedded Event Manager mode

Command History

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

Usage Guidelines

None

Examples

The following example shows how to log an EEM applet exception:

```
switch# configure terminal
switch(config)# event manager applet exception-applet
switch(config-applet)# action 1.0 forceshut module 2 reset-reason “flapping links”
switch(config-applet)#
```

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action overbudgetshut

To configure the shutdown of a module or the entire switch due to an overbudget power condition when an Embedded Event Manager (EEM) applet is triggered, use the action overbudgetshut command.

action number [*.number2*] **overbudgetshut** [**module slot** [*– slot*]]

Syntax Description

number .number2	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.
module slot -slot	(Optional) Specifies the slot range: • For 6slot the range is from 1 to 6. • For 9slot the range is from 1 to 9. • For 13slot the range is from 1 to 13.

Command Default

None

Command Modes

Embedded Event Manager

Command History

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

Usage Guidelines

None

Examples

The following example shows how to configure a power overbudget shutdown of module 3-5 when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet overbudget-applet
switch(config-applet)# action 1.0 overbudgetshut module 3-5
switch(config-applet)#
```

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action policy-default

To enable the default actions of the policy being overridden, use the action policy-default command.

action number [**.number2**] **policy-default**

Syntax Description

number .number2	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.

Command Default

None

Command Modes

Embedded Event Manager mode

Command History

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

Usage Guidelines

None

Examples

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

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

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action reload

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

Syntax Description

number .number2	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.
module slot -slot	(Optional) Specifies the slot range. The range is from 1 to 10, or a substituted parameter.

Command Default

None

Command Modes

Embedded Event Manager mode

Command History

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

Usage Guidelines

None

Examples

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

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

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action snmp-trap

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

action number [**.number2**] **snmp-trap** [**intdata1 integer** [**intdata2 integer**] [**strdata string**]]
no action number [**.number2**] **snmp-trap** [**intdata1 integer** [**intdata2 integer**] [**strdata string**]]

Syntax Description

number .number2	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.
intdata1 integer	(Optional) Specifies an integer to be sent in the SNMP trap message to the SNMP agent.
intdata2 integer	(Optional) Specifies a second integer to be sent in the SNMP trap message to the SNMP agent.
strdata string	(Optional) Specifies a string to be sent in the SNMP trap message to the SNMP agent. If the string contains embedded blanks, enclose it in double quotation marks.

Command Default

None

Command Modes

Embedded Event Manager mode.

Command History

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

Usage Guidelines

None

Examples

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

```
switch# configure terminal
switch(config)# event manager applet snmp-applet
switch(config-applet)# action 1.0 snmp-trap strdata “temperature problem”
switch(config-applet)#
```

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action syslog

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

action number [**.number2**] **syslog** [**priority prio-val**] **msg error-message**
no action number [**.number2**] **syslog** [**priority prio-val**] **msg error-message**

Syntax Description

number	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.
priority prio-val	(Optional) Specifies the priority level of the syslog messages. If this keyword is not selected, all syslog messages are set at the informational priority level. If this keyword is selected, the priority level argument must be defined. There are three ways of defining the priority level: • Define the priority level using one of these methods: – 0—System is unusable. – 1—Immediate action is needed. – 2—Critical conditions. – 3—Error conditions. – 4—Warning conditions. – 5—Normal but significant conditions. – 6—Informational messages. This is the default. – 7—Debugging messages. • Enter the priority by selecting one of the priority keywords: –emergencies—System is unusable. – alerts—Immediate action is needed. – critical—Critical conditions. – errors—Error conditions. – warnings—Warning conditions. – notifications—Normal but significant conditions. – informational—Informational messages. This is the default. – debugging—Debugging messages.
msg error message	Specifies the error message. The message can be any quoted alphanumeric string up to 80 characters.

Command Default

None

Command Modes

Embedded Event Manager 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 a syslog message to save when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet syslog-applet
switch(config-applet)# action 1.0 syslog priority notifications msg "cpu high"
switch(config-applet)#
```

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

active equals saved

To automatically write any changes to the block, prohibit or port an address name to the IPL file, use the **active equals saved** command. To disable the configuration or to revert to factory defaults, use the **no** form of the command.

active equals saved
no active equals saved

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Enabled (when a FICON VSAN is configured).

Command Modes

FICON configuration submode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Enabling **active equals saved** ensures that you do not have to perform the **copy running-config startup-config** command to save the FICON configuration as well as the running configuration. If your switch or fabric consists of multiple FICON-enabled VSANs, and one of these VSANs has **active equals saved** enabled, changes made to the non-FICON configuration causes all FICON-enabled configurations to be saved to the IPL file.

The following example enables the automatic save feature for a VSAN:

```
switch(config)# ficon vsan 2
switch(config-ficon)# active equals saved
```

The following example disables the automatic save feature for this VSAN:

```
switch(config-ficon)# no active equals saved
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration.
ficon vsan	Enables FICON on the specified VSAN.
show ficon	Displays configured FICON details.

add-session vsan

To add sessions to a job, use the add-session vsan command in configuration mode.

add-session vsan *vsan-id* {**pwwn** *tgt-pwwn* **all-luns**|**lun** *lun-id* **algorithm** *name-id*}

Syntax Description

vsan-id	Specifies the VSAN ID of the target.
pwwn tgt-pwwn	Specifies the pWWN of the target.
all-luns	Specifies all of the LUNs in the Secure Erase session.
lun lun-id	Specifies the LUN ID of the Secure Erase session.
algorithm name/id	Specifies the algorithm that should be used for the session.

Command Default

None

Command Modes

Configuration Secure Erase job submode

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to add a VI to a specific Secure Erase job:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 job 1
switch(config-se-job)# add-session vsan 1 pwwn 20:04:00:a0:b8:16:92:18 all-luns algorithm
RCMP
```

Related Commands

Command	Description
add-session job	Adds sessions to the job.

add-step dynamic

To add a dynamic pattern step to a specific algorithm, use the add-step dynamic command in configuration mode.

add-step dynamic [{**0**|**1**}]

Syntax Description

0	(Optional) Specifies that the pattern is generated using a random number generator.
1	(Optional) Specifies that the pattern is complimentary to the previous pattern.

Command Default

None

Command Modes

Configuration Secure Erase algorithm submode

Command History

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

Usage Guidelines

None

Examples

The following example shows how to add a dynamic pattern step to a specific algorithm:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 algorithm 0
switch(config-se-algo)#
switch(config-se-algo)# add-step dynamic 0
```

Related Commands

Command	Description
add-step static	Adds static pattern step to a specific algorithm.

add-step static

To add a static pattern step to a specific algorithm, use the add-step static command in configuration mode.

add-step static pattern

Syntax Description

pattern	Specifies the static pattern step. The pattern is to write ranges from 1 to 512 bytes and can consist of only characters 0 to 9 and A to F.

Command Default

None

Command Modes

Configuration Secure Erase algorithm submode

Command History

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

Usage Guidelines

None

Examples

The following example shows how to add a static step to a specific algorithm:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 algorithm 0
switch(config-se-algo)#
switch(config-se-algo)# add-step static 1
```

Related Commands

Command	Description
add-step dynamic	Adds a dynamic pattern step to a specific algorithm.

add-tgt vsan

To define target enclosure and add multiple target ports for a specific Secure Erase job, use the add-tgt vsan command in configuration mode.

add-tgt vsan vsan-id pwwn target port pwwn

Syntax Description

vsan-id	Specifies the VSAN ID of the target port added to a Secure Erase job.
pwwn target port pwwn	Specifies the port world-wide name (pWWN) of the target port.

Command Default

None

Command Modes

Configuration Secure Erase job submode

Command History

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

Usage Guidelines

The target ports added to a specific job can be part of a different VSAN. The Secure Erase application creates VIs in a specific VSAN.

Note VIs and targets from different VSANs can be added to a job. A storage array may have multiple storage ports belonging to a different VSAN. You can create one job for one storage array.

Examples

The following example shows how to define a target enclosure and add multiple target ports for a specific Secure Erase job:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 job 1
switch(config-se-job)# add-tgt vsan 1 pwwn 20:04:00:a0:b8:16:92:18
```

Related Commands

Command	Description
add-session vsans	Adds sessions to a job.
add-VI job	Adds a VI to a specific Secure Erase job.
secure-erase create job	Creates a Secure Erase job.

add-vi vsan

To add a VI to a specific Secure Erase job, use the add-vi vsan command in configuration mode.

{**add-vi vsan vsan-id all**|**pwwn VI pwwn**}

Syntax Description

vsan-id	Specifies the VSAN ID of the target where a VI exists.
all	Adds all the VSAN IDs of the target.
pwwn VI pwwn	Adds a specific VI in a given VSAN to the job.

Command Default

None

Command Modes

Configuration Secure Erase job submode

Command History

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

Usage Guidelines

You must add at least one VI in each VSAN where a Secure Erase target is present.

All VIs that are part of the same job and the VSAN must have same target view. The same set of targets and LUNs must be exposed for all VIs in the same VSAN.

Note VI-CPP can not be added to a job. To know the WWN of the VI-CPP, please run the show isapi virtual-nport database command on SSM module.

Examples

The following example shows how to add all VIs to a given Secure Erase job:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 job 1
switch(config-se-job)# add-vi vsan 1 all
The following example shows how to add a VI to a given Secure Erase job:
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 job 1
switch(config-se-job)# add-vi vsan 1 pwwn 2c:0d:00:05:30:00:43:64
```

Related Commands

Command	Description
add-session job	Adds sessions to the job.

Command	Description
add-VI job	Adds a VI to a specific Secure Erase job.
secure-erase create job	Creates a Secure Erase job.

alert-group

To override the default data attached to a Call Home message, use the **alert-group** command in Call Home configuration submode. To remove the customization, use the **no** form of the command.

alert-group
{**All**|**Cisco-TAC**|**Environmental**|**Inventory**|**License**|**Linecard-Hardware**|**RMON**|**Supervisor-Hardware**|**Syslog-group-port**|**System**|**Test**}
{**script-name** *script.tar*|**user-def-cmd** *commands*}
no alert-group
{**All**|**Cisco-TAC**|**Environmental**|**Inventory**|**License**|**Linecard-Hardware**|**RMON**|**Supervisor-Hardware**|**Syslog-group-port**|**System**|**Test**}
{**script-name** *script.tar*|**user-def-cmd** *commands*}

Syntax Description

All	Specifies an alert group consisting of events from all the Call Home messages.
Cisco-TAC	Specifies an alert group consisting of events that are meant only for Cisco TAC.
Environmental	Specifies an alert group consisting of power, fan, and temperature-related events.
Inventory	Specifies an alert group consisting of inventory status events.
License	Specifies an alert group consisting of license status events.
Linecard-Hardware	Specifies an alert group consisting of module-related events.
RMON	Specifies an alert group consisting of RMON status events.
Supervisor-Hardware	Specifies an alert group consisting of supervisor-related events.
Syslog-group-port	Specifies an alert group consisting of syslog port group status events.
System	Specifies an alert group consisting of software-related events.
Test	Specifies an alert group consisting of user-generated test events.
script-name *script.tar*	Maps a script to the alert group that should trigger it.
user-def-cmd *command*	Configures a CLI command for an alert-group. The maximum size is 512.

Command Default

None

Command Modes

Call Home configuration submode (config-callhome)

Command History

Release	Modification
7.3(1)DY(1)	Added the **script-name** keyword.
3.0(1)	This command was introduced.

Usage Guidelines

The **user-def-cmd** argument allows you to define a command whose outputs should be attached to the Call Home message being sent. Only **show** commands can be specified and they must be associated with an alert group. Five commands can be specified per alert group. Invalid commands are rejected.

Caution The script-name option is only for use by certain customers. Do not configure it if you are not approved by Cisco to use it.

Note Make sure the destination profiles for the non-Cisco-TAC alert group, with a predefined show command, and the Cisco-TAC alert group are not the same.

Examples

The following example shows how to define a set of commands to be used for the supervisor-hardware alert group:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# alert-group supervisor-hardware user-def-cmd show version
switch(config-callhome)# alert-group supervisor-hardware user-def-cmd show environment power
switch(config-callhome)# alert-group supervisor-hardware user-def-cmd show cores
```

The following example shows how to configure a script for all Call Home alerts:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# alert-group all script-name m9700.tar
```

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.

arp

To enable the Address Resolution Protocol (ARP) for the switch, use the arp command.To disable ARP for the switch, use the no form of the command.

arp *hostname*
no arp *hostname*

Syntax Description

hostname	Specifies the name of the host. Maximum length is 20 characters.

Command Default

Enabled

Command Modes

Configuration mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example disables the Address Resolution Protocol configured for the host with the IP address 10.1.1.1:

```
switch(config)# no arp 10.1.1.1
switch(config)#
```

Related Commands

Command	Description
clear arp	Deletes a specific entry or all entries from the ARP table.
show arp	Displays the ARP table.

attach

To connect to a specific module, use the attach command in EXEC mode.

attach module *slot-number*

Syntax Description

module *slot-number*	Specifies the slot number of the module.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can use the attach module command to view the standby supervisor module information, but you cannot configure the standby supervisor module using this command.

You can also use the attach module command on the switching module portion of the Cisco MDS 9216 supervisor module, which resides in slot 1 of this two-slot switch.

To disconnect, use the **exit** command at the module-number# prompt, or type **$.** to forcibly abort the attach session.

Examples

The following example connects to the module in slot 2. Note that after you connect to the image on the module using the attach module command, the prompt changes to module-number#:

```
switch# attach module 1
Attaching to module 1 ...
To exit type 'exit', to abort type '$.'
module-1# exit
switch#
```

Related Commands

Command	Description
exit	Disconnects from the module.
show module	Displays the status of a module.

attachpriv

To connect to a specific ILC line card as a privilege, use the attachpriv command in EXEC mode.

attachpriv module *slot-number*

Syntax Description

module *slot-numbe*r	Specifies the slot number of the module.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.1(3)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to connect to a specific ILC line card as a privilege:

```
switch# attachpriv module 1
Attaching to module 1 ...
To exit type 'exit', to abort type '$.'
module-1# exit
```

Related Commands

Command	Description
exit	Disconnects from the module.
show module	Displays the status of a module.

attribute failover auto

To configure an automatic fallback failover for a virtual device, use the attribute failover auto command. To revert to the default, use the **no** form of the command.

attribute failover auto [fallback]
no attribute failover auto [fallback]

Syntax Description

fallback	(Optional) Enables a switchback with an automatic failover.

Command Default

Disabled

Command Modes

Virtual device submode

Command History

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

Usage Guidelines

None

Examples

The following example shows how to configure an automatic failover for a specific virtual device:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# sdv virtual-device name vdev1 vsan 1
switch#(config-sdv-virt-dev)# attribute failover auto
switch#(config-sdv-virt-dev)#
```

The following example shows how to configure an attribute of a virtual device:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# sdv virtual-device name vdev1 vsan 1
switch#(config-sdv-virt-dev)# attribute failover auto fallback
```

switch(config-sdv-virt-dev)#

attribute qos

To configure a QoS attribute, use the **attribute qos** command in Inter-VSAN Routing (IVR) zone configuration submode. To disable this feature, use the **no** form of this command.

attribute qos {**high**|**low**|**medium**}
no attribute qos {**high**|**low**|**medium**}

Syntax Description

high	Configures frames matching zone to get high priority.
low	Configures frames matching zone to get low priority (default).
medium	Configures frames matching zone to get medium priority.

Command Default

Disabled

Command Modes

IVR zone configuration submode

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to configure an IVR zone QoS attribute to low priority:

```
switch# config terminal

Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ivr zone name IvrZone

switch(config-ivr-zone)# attribute qos priority low
```

Related Commands

Command	Description
show ivr zone	Displays IVR zone configuration.

attributes (DMM job configuration submode)

To set the attributes of a data migration job, use the **attributes** command in DMM job configuration submode. To remove the attributes of a data migration job, use the no form of the command.

attributes job_type {**1**|**2**} **job_mode** {**1**|**2**} **job_rate** {**1**|**2**|**3**|**4**} **job_method** {**1**|**2**}
no attributes job_type {**1**|**2**} **job_mode** {**1**|**2**} **job_rate** {**1**|**2**|**3**|**4**} **job_method** {**1**|**2**}

Syntax Description

job_type 1 | 2	Specifies the job type. Specify 1 for a server type job and 2 for a storage type job.
job_mode 1 | 2	Specifies the job mode. Specify 1 for an online job and 2 for an offline job.
job_rate 1 | 2 | 3 | 4	Specifies the job rate. Specify 1 for the default rate, 2 for a slow rate, 3 for a medium rate, and 4 for a fast rate.
job_method 1|2	Specifies the job method. Specify 1 for Method 1 and 2 for Method 2.

Command Default

None

Command Modes

DMM job configuration submode

Command History

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

Usage Guidelines

None

Examples

The following example sets the job type to storage, the job mode to online, and the job rate to fast:

```
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)# attributes job_type 2 job_mode 1 job_rate 4 job_method 1
switch(config-dmm-job)#
```

Related Commands

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

authentication (IKE policy configuration submode)

To configure the authentication method for an IKE protocol policy, use the **authentication** command in IKE policy configuration submode. To revert to the default authentication method, use the **no** form of the command.

authentication {**pre-share**|**rsa-sig**}
no authentication {**pre-share**|**rsa-sig**}

Syntax Description

pre-share	Configures the preshared key as the authentication method.
rsa-sig	Configures RSA signatures as the authentication method.

Command Default

Preshared key.

Command Modes

IKE policy configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

To use this command, enable the IKE protocol using the **crypto ike enable** command. In addition, you must configure the identity authentication mode using the fully qualified domain name (FQDN) before you can use RSA signatures for authentication. Use the **identity hostname** command for this purpose.

Examples

The following example shows how to configure the authentication method using the preshared key:

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# policy 1
switch(config-ike-ipsec-policy)# authentication pre-share
```

The following example shows how to configure the authentication method using the RSA signatures:

```
switch(config-ike-ipsec-policy)# authentication rsa-sig
```

The following example shows how to revert to the default authentication method (preshared key):

```
switch(config-ike-ipsec-policy)# no
authentication rsa-sig
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
identity hostname	Configures the identity for the IKE protocol.

Command	Description
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

authentication

To change the authentication behavior, use the authentication command. To disable this feature, use the no form of the command.

authentication {**compare** [**password-attribute password-attribute**]|**bind-first** [**append-with-baseDN string**]}
no authentication {**compare** [**password-attribute password-attribute**]|**bind-first** [**append-with-baseDN string**]}

Syntax Description

compare	Specifies the compare option to be used for authentication.
password-attribute password-attribute	(Optional) Overides the default password attribute.The maximum length is 128 characters.
bind-first	Specifies that the client use bind and search instead of search and bind.
append-with-baseDN string	(Optional) Overrides the default string appended with baseDN.

Command Default

userPassword.

append-with-baseDN default value is (cn=$userid).

Command Modes

Configuration submode

Command History

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

Usage Guidelines

The password-attribute keyword provdes a method for chaning the attribute type of password.

Examples

```
The following example shows how to change the default attribute:
switch(config-ldap)# authentication compare password-attribute 1
switch(config-ldap)#
```

Related Commands

Command	Description
show aaa authentication	Displays the configured authentication methods.

auth-mechanism plain

To set the authentication mechanism as plain, use the auth-mechanism plain command in configuration mode. To disable this feature, use the no form of the command.

auth-mechanism plain
no auth-mechanism plain

Syntax Description

This command has no arguments or keywords.

Command Default

Plain.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

```
The following example shows how to set the authentication mechanism as plain:
switch(config-ldap)# auth-mechanism plain
switch(config-ldap)#
```

Related Commands

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

autonomous-fabric-id (IVR service group configuration)

To configure an autonomous fabric ID (AFID) into an IVR service group, use the autonomous-fabric-id command in IVR service group configuration submode. To remove the autonomous fabric ID, use the **no** form of the command.

autonomous-fabric-id *afid* **vsan-ranges** *vsan-id*
no autonomous-fabric-id *afid* **vsan-ranges** *vsan-id*

Syntax Description

afid	Specifies the AFID to the local VSAN.
vsan-ranges *vsan-id*	Configures up to five ranges of VSANs to be added to the service group. The range is 1 to 4093.

Command Default

None

Command Modes

IVR service group configuration submode

Command History

Release	Modification
2.1	This command was introduced.

Usage Guidelines

Before configuring an IVR service group, you must enable the following:

- IVR using the **ivr enable** command
- IVR distribution using the **ivr distribute** command
- Automatic IVR topology discovery using the **ivr vsan-topology auto command**

To change to IVR service group configuration submode, use the **ivr service-group activate command.**

Examples

The following command enters the IVR service group configuration submode and configures AFID 10 to be in IVR service group serviceGroup1:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr enable
switch(config)# ivr distribute
switch(config)# ivr vsan-topology auto
switch(config)# ivr ?
  abort                 Flushes cached data without commiting and releases the lock
  commit                Commits cached data (of all msg types) and releases the lock
  distribute            Enables/disables fabric distribution using cfs.
  enable                Enable/Disable IVR
  nat                   Enable FCID address translation (NAT) for IVR traffic
  service-group         Configure IVR servive group
  virtual-fcdomain-add  Add IVR virtual domain(s) to fcdomain list
  vsan-topology         Configure or activate VSAN topology for inter-VSAN routing
  zone                  Configure a inter vsan zone
  zoneset               Configure inter vsan routing zoneset
switch(config)# ivr service-group name serviceGroup1
switch(config-ivr-sg)# ?
```

```
service grp. membership cmds:
  afid  Enter Autonomous Fabric ID
  do    EXEC command
  exit  Exit from this submode
  no    Negate a command or set its defaults
switch(config-ivr-sg)# <TBD - Information Needed>
switch(config-ivr-sg)# afid ?
  <1-64>  Enter an autonomous fabic ID
switch(config-ivr-sg)# afid 10 ?
  vsan-ranges  Enter VSANs within this afid
switch(config-ivr-sg)# afid 10 vsan 1-4 ?
  ,     Comma
  <cr>  Carriage Return
switch(config-ivr-sg)# autonomous-fabric-id 10 vsan 1-4
IVR service group is used only when VSAN Topology is in AUTO mode
```

Related Commands

Command	Description
ivr enable	Enables the Inter-VSAN Routing (IVR) feature.
ivr service-group name	Configures an IVR service group and changes to IVR service group configuration submode.
show autonomous-fabric-id database	Displays the contents of the AFID database.
show ivr	Displays IVR feature information.

autonomous-fabric-id (IVR topology database configuration)

To configure an autonomous fabric ID (AFID) into the Inter-VSAN Routing (IVR) topology database, use the autonomous-fabric-id command. To remove the fabric ID, use the **no** form of the command.

autonomous-fabric-id *fabric-id* **switch-wwn** *swwn* **vsan-ranges** *vsan-id*
no autonomous-fabric-id *fabric-id* **switch-wwn** *swwn* **vsan-ranges** *vsan-id*

Syntax Description

fabric-id	Specifies the fabric ID for the IVR topology. **Note** For Cisco MDS SAN-OS images prior to Release 2.1(1a), the *fabric-id value is limited to 1.* For Releases 2.1(1a) and later images, the *fabric-id* range is 1 to 64.
switch-wwn *swwn*	Configures the switch WWN in dotted hex format.
vsan-ranges *vsan-id*	Configures up to five ranges of VSANs to be added to the database. The range is 1 to 4093.

Command Default

None

Command Modes

IVR topology database configuration submode

Command History

Release	Modification
1.3(1)	This command was introduced.
2.1(1a)	Modified range for *fabric-id.*

Usage Guidelines

The following rules apply to configuring AFIDs to VSANs:

- The default AFID of a VSAN is 1.
- Each VSAN belongs to one and only one AFID.
- A switch can be a member of multiple AFIDs.
- AFIDs at a switch must not share any VSAN identifier (for example, a VSAN at a switch can belong to only one AFID).
- A VSAN identifier can be reused in different AFIDs, without merging the VSANs, as long as those AFIDs do not share a switch.

You can have up to 64 VSANs (or 128 VSANs for Cisco MDS SAN-OS Release 2.1(1a) or later) in an IVR topology. Specify the IVR topology using the following information:

- The switch WWNs of the IVR-enabled switches.
- A minimum of two VSANs to which the IVR-enabled switch belongs.
- The autonomous fabric ID (AFID), which distinguishes two VSANs that are logically and physically separate, but have the same VSAN number. Cisco MDS SAN-OS Release 1.3(1) and NX-OS Release 4.1(1b) supports only one default AFID (AFID 1) and does not support non-unique VSAN IDs in the network. As of Cisco MDS SAN-OS Release 2.1(1a), you can specify up to 64 AFIDs.

Note Two VSANs with the same VSAN number but different fabric IDs are counted as two VSANs out of the 128 total VSANs allowed in the fabric.

Examples

The following command enters the configuration mode, enables the IVR feature, enters the VSAN topology database, and configures the pWWN-VSAN association for VSANs 2 and 2000:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr enable
switch(config)# ivr vsan-topology database
switch(config-ivr-topology-db)# autonomous-fabric-id 1 switch 20:00:00:00:30:00:3c:5e
vsan-ranges 2,2000
```

Related Commands

Command	Description
ivr enable	Enables the Inter-VSAN Routing (IVR) feature.
ivr vsan-topology database	Configures a VSAN topology database.
show autonomous-fabric-id database	Displays the contents of the AFID database.
show ivr	Displays IVR feature information.

autonomous-fabric-id database

To configure an autonomous fabric ID (AFID) database, use the autonomous-fabric-id database command. To remove the fabric AFID database, use the **no** form of the command.

autonomous-fabric-id database
no autonomous-fabric-id database

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

You must configure the IVR VSAN topology to auto mode, using the **ivr vsan-topology auto** command, before you can use the **autonomous-fabric-id database** command to modify the database. The **autonomous-fabric-id database** command also enters AFID database configuration submode.

Note In user-configured VSAN topology mode, the AFIDs are specified in the IVR VSAN topology configuration itself and a separate AFID configuration is not needed.

Examples

The following example shows how to create an AFID database and enters AFID database configuration submode:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# autonomous-fabric-id ?
  database  Configure autonomous fabric identifier (AFID) database
switch(config)# autonomous-fabric-id database ?
  <cr>  Carriage Return
switch(config)# autonomous-fabric-id database
AFID database is used only when VSAN Topology is in AUTO mode
switch(config-afid-db)#
```

Related Commands

Command	Description
ivr vsan-topology auto	Configures a VSAN topology for Inter-VSAN Routing (IVR) to auto configuration mode.
switch-wwn	Configures a switch WWN in the autonomous fabric ID (AFID) database

Command	Description
show autonomous-fabric-id database	Displays the contents of the AFID database.
show ivr	Displays IVR feature information.

auto-volgrp

To configure the automatic volume grouping, use the auto-volgrp command. To disable this feature, use the no form of the command.

auto-volgrp
no auto-volgrp

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Cisco SME cluster configuration submode

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

If Cisco SME recognizes that the tape's barcode does not belong to an existing volume group, then a new volume group is created when automatic volume grouping is enabled.

Examples

The following example enables automatic volume grouping:

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

The following example disables automatic volume grouping:

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

Related Commands

Command	Description
show sme cluster	Displays Cisco SME cluster information.

B Commands

banner motd

To configure a message of the day (MOTD) banner, use the **banner motd** command in configuration mode.

banner motd [*delimiting-character message delimiting-character*]
no banner motd [*delimiting-character message delimiting-character*]

Syntax Description

delimiting-character	(Optional) Identifies the delimiting character.
message	(Optional) Specifies the banner message that is restricted to 40 lines with a maximum of 80 characters in each line.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

The configured MOTD banner is displayed before the login prompt on the terminal whenever a user logs in to a Cisco MDS 9000 Family switch.

Follow these guidelines when choosing your delimiting character:

- Do not use the *delimiting-character* in the *message* string.
- Do not use **"** and **%** as delimiters.

You can include tokens in the form $(token) in the message text. Tokens will be replaced with the corresponding configuration variable. For example:

- $(hostname) displays the host name for the switch
- $(line) displays the vty or tty line no or name
- The $(line-desc) and $(domain) tokens are not supported.

Examples

The following example configures a banner message with the following text “Testing the MOTD Feature:”

```
switch# config terminal
switch(config)# banner motd # Testing the MOTD Feature. #
```

The following example spans multiple lines and uses tokens to configure the banner message:

```
switch# config terminal
switch(config)# banner motd #
Enter TEXT message. End with the character '#'.
Welcome to switch $(hostname).
You tty line is $(line).
#
```

Related Commands

Command	Description
show banner motd	Displays the configured banner message.

boot

To perform operations on the system, use the **boot** command in configuration mode. To negate this feature or return to factory defaults, use the **no** form of the command.

boot {**asm-sfn** {**bootflash:**|**slot0:**|**tftp:**} [*image*] [**module** [*slot-number*]]|**auto-copy**|**kickstart** {**bootflash:**|**slot0:**|**tftp:**} [*image*] [{**sup-1** **[sup-2]**|**sup-2**}]|**lasilc** {**bootflash:**|**slot0:**|**tftp:**} [*image*] [**module** [*slot-number*]]|**ssi** {**bootflash:**|**slot0:**}|**system** {**bootflash:**|**slot0:**|**tftp:**} [*image*] [{**sup-1** **[sup-2]**|**sup-2**}]}
no boot {**asm-sfn** {**bootflash:**|**slot0:**|**tftp:**} [*image*] [**module** [*slot-number*]]|**auto-copy**|**kickstart** {**bootflash:**|**slot0:**|**tftp:**} [*image*] [{**sup-1** **[sup-2]**|**sup-2**}]|**lasilc** {**bootflash:**|**slot0:**|**tftp:**} [*image*] [**module** [*slot-number*]]|**ssi** {**bootflash:**|**slot0:**}|**system** {**bootflash:**|**slot0:**|**tftp:**} [*image*] [{**sup-1** **[sup-2]**|**sup-2**}]}

Syntax Description

asm-sfn	Configures the virtualization image.
bootflash:	Specifies system image URI for bootflash.
slot0:	Specifies system image URI for slot 0.
tftp:	Specifies system image URI for TFTP.
image	(Optional) Specifies the image file name.
module *slot-number*	(Optional) Specifies the slot number of the SSM.
auto-copy	Configures auto-copying of boot variable images.
kickstart	Configures the kickstart image.
lasilc	Configures the boot image.
ssi	Configures the SSI image.
system	Configures the system image.
sup-1	(Optional) The upper supervisor.
sup-2	(Optional) The lower supervisor.

Disabled.The default state for **auto-copy** is enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(2)	This command was introduced
3.0(1)	Changed the default state for **auto-copy** to enabled.

Usage Guidelines

The boot kickstart slot0:*image* command is currently not allowed. For kickstart, only bootflash: is allowed.

When the **boot auto-copy** command is issued, the system copies the boot variable images which are local (present) in the active supervisor module (but not in the standby supervisor module) to the standby supervisor module. For kickstart and system boot variables, only those images that are set for the standby supervisor module are copied. For modules (line card) images, all modules present in standby's corresponding locations (bootflash: or slot0:) will be copied.

Examples

The following example adds the new system image file to the SYSTEM environment variable:

```
switch(config)# boot system bootflash:system.img
```

The following example boots from the CompactFlash device (slot0:). The switch updates the SYSTEM environment variable to reflect the new image file in the specified flash device:

```
switch(config)# boot system slot0:system.img
```

The following example overwrites the old Kickstart environment variable in the configuration file:

```
switch(config)# boot kickstart bootflash:kickstart.img
```

The following example specifies the SSM image to be used:

```
switch(config)# boot asm-sfn bootflash:m9000-ek9-asm-sfn-mz.1.2.2.bin
```

The following example enables automatic copying of boot variables from the active supervisor module to the standby supervisor module:

```
switch(config)# boot auto-copy
The following example disables the automatic copy feature (default).
switch(config)# no boot auto-copy
```

Related Commands

Command	Description
show boot	Displays the configured boot variable information.

bport

To configure a B port mode on a FCIP interface, use the**bport** option. To disable a B port mode on a FCIP interface, use the no form of the command.

bport
no bport

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to configure a B port mode on an FCIP interface:

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# bport
```

Related Commands

Command	Description
bport-keepalive	Configures B port keepalive responses.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

bport-keepalive

To configure keepalive responses for B port FCIP interfaces, use the **bport-keepalive** option. To disable keepalive responses for B port FCIP interfaces, use the no form of the command.

bport-keepalive
no bport-keepalive

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to configure keepalive responses for B port FCIP interfaces:

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# bport-keepalives
```

Related Commands

Command	Description
bport	Configures a B port FCIP interface.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

broadcast

To enable the broadcast frames attribute in a zone attribute group, use the **broadcast** command. To revert to the default, use the **no** form of the command.

broadcast
no broadcast

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Zone attribute configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

Broadcast frames are sent to all Nx ports.

If any NL port attached to an FL port shares a broadcast zone with the source of the broadcast frame,

then the frames are broadcast to all devices in the loop.

This command only configures the broadcast attribute for enhanced zoning. To enable broadcast zoning for basic mode, use the **attribute broadcast** subcommand after entering zone configuration mode using the **zone name** command.

Examples

The following example shows how to set the broadcast attribute for a zone attribute group:

```
switch# config terminal
switch(config)# zone-attribute-group name admin-attributes vsan 10
switch(config-attribute-group)# broadcast
```

Related Commands

Command	Description
show zone-attribute-group	Displays zone attribute group information.
zone mode enhanced vsan	Enables enhanced zoning for a VSAN.
zone name	Configures zone attributes.
zone-attribute-group name	Configures zone attribute groups.

C Commands

callhome

To configure the Call Home function, use the **callhome** command.

callhome

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The Call Home configuration commands are available in the (config-callhome) submode.

A Call Home message is used to contact a support person or organization in case an urgent alarm is raised.

Once you have configured the contact information, you must enable the Call Home function. The **enable** command is required for the Call Home function to start operating. When you disable the Call Home function, all input events are ignored.

Note Even if Call Home is disabled, basic information for each Call Home event is sent to syslog.

The user-def-cmd command allows you to define a command whose outputs should be attached to the Call Home message being sent. Only show commands can be specified and they must be associated with an alert group. Five commands can be specified per alert group. Invalid commands are rejected.

Note Customized **show** commands are only supported for full text and XML alert groups. Short text alert groups (short-txt-destination) do not support customized **show** commands because they only allow 128 bytes of text.

To assign show commands to be executed when an alert is sent, you must associate the commands with the alert group. When an alert is sent, Call Home associates the alert group with an alert type and attaches the output of the show commands to the alert message.

Note Make sure the destination profiles for the non-Cisco-TAC alert group, with a predefined show command, and the Cisco-TAC alert group are not the same.

The following example assigns contact information:

```
switch# config terminal
config terminal
```

```
switch# snmp-server contact personname@companyname.com
switch(config)# callhome
switch(config-callhome)# email-contact username@company.com
switch(config-callhome)# phone-contact +1-800-123-4567
switch(config-callhome)# streetaddress 1234 Picaboo Street, Any city, Any state, 12345
switch(config-callhome)# switch-priority 0
switch(config-callhome)# customer-id Customer1234
switch(config-callhome)# site-id Site1ManhattanNY
switch(config-callhome)# contract-id Company1234
```

The following example configures a user-defined **show** command for an alert-group license:

```
switch(config-callhome)# alert-group license user-def-cmd "show license usage"
```

Note The **show** command must be enclosed in double quotes.

The following example removes a user-defined **show** command for an alert-group license:

```
switch(config-callhome)# no alert-group license user-def-cmd "show license usage"
```

Related Commands

Command	Description
alert-group	Customizes a Call Home alert group with user-defined **show** commands.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

callhome mft-put

To copy the file from the bootflash directory to a secure remote support service, use the **callhome mft-put** command.

callhome mft-put *filename*

Syntax Description

filename	The name of the file to be transferred to a secure remote support service.

Command Default

None

Command Modes

User EXEC (#)
Privileged EXEC (#)

Command History

Release	Modification
NX-OS 7.3(1)DY(1)	This command was introduced.

Usage Guidelines

The **callhome mft-put** command is used to transfer files such as syslogs, output of the **show tech-support** command, and so on, to a secure remote support service.

Examples

The following example shows how to copy a file bootflash to a secure remote support service:

```
switch# callhome mft-put zone_sdb.log
Trying to copy file using mft-put to remote location
Successfully sent file using mft-put
```

Related Commands

Command	Description
callhome	Configures Call Home functions.
show callhome	Displays configured Call Home information.

callhome test

To simulate a Call Home message generation, use the **callhome test** command.

callhome test [inventory]

Syntax Description

inventory	(Optional) Sends a dummy Call Home inventory.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can simulate a message generation by entering a **callhome test** command.

Examples

The following example sends a test message to the configured destinations:

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

The following example sends a test inventory message to the configured destinations:

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

Related Commands

Command	Description
callhome	Configures Call Home functions.
show callhome	Displays configured Call Home information.

callhome test-keepalive

To check for the connectivity between Call Home and a secure remote support service, use the **callhome test-keepalive** command.

callhome test-keepalive

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User EXEC (#)
Privileged EXEC (#)

Command History

Release	Modification
NX-OS 7.3(1)DY(1)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to initiate a keepalive message communication with a secure remote support service:

```
switch# callhome test-keepalive
Initiating callhome test-keepalive
```

Related Commands

Command	Description
callhome	Configures Call Home functions.
show callhome	Displays configured Call Home information.

cd

To change the default directory or file system, use the **cd** command.

cd {*directory*|**bootflash : [directory]**|**slot0 : [directory]**|**volatile : [directory]**}

Syntax Description

directory	(Optional) Name of the directory on the file system.
bootflash:	URI or alias of the bootflash or file system.
slot0:	URI or alias of the slot0 file system.
volatile:	URI or alias of the volatile file system.

Command Default

The initial default file system is flash:. For platforms that do not have a physical device named flash:, the keyword flash: is aliased to the default flash device.

If you do not specify a directory on a file system, the default is the root directory on that file system.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

For all EXEC commands that have an optional file system argument, the system uses the file system specified by the cd command when you omit the optional file system argument. For example, the dir command, which displays a list of files on a file system, contains an optional file system argument. When you omit this argument, the system lists the files on the file system specified by the cd command.

Examples

The following example sets the default file system to the flash memory card inserted in slot 0:

```
switch# pwd

bootflash:/
switch# cd slot0:

switch# pwd
slot0:/
```

Related Commands

Command	Description
copy	Copies any file from a source to a destination.
delete	Deletes a file on a flash memory device.
dir	Displays a list of files on a file system.
pwd	Displays the current setting of the cd command.

Command	Description
show file systems	Lists available file systems and their alias prefix names.
undelete	Recovers a file marked deleted on a Class A or Class B flash file system.

cdp

To globally configure the Cisco Discovery Protocol parameters, use the **cdp** command. Use the **no** form of this command to revert to factory defaults.

cdp { **enable** | **advertise** { **v1** |**v2** } | **holdtime** *holdtime-seconds* | **timer** *timer-seconds* }
no cdp { **enable** |**advertise** | **holdtime** *holdtime-seconds* | **timer** *timer-seconds* }

Syntax Description

enable	Enables CDP globally on all interfaces on the switch.
advertise	Specifies the EXEC command to be executed.
v1	Specifies CDP version 1.
v2	Specifies CDP version 2.
holdtime	Sets the hold time advertised in CDP packets.
holdtime-seconds	The holdtime in seconds. The default is 180 seconds and the valid range is from 10 to 255 seconds.
timer	Sets the refresh time interval.
timer-seconds	The time interval in seconds. The default is 60 seconds and the valid range is from 5 to 255 seconds.

Command Default

CDP is enabled.

The hold time default interval is 180 seconds.

The refresh time interval is 60 seconds.

Command Modes

Configuration mode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Use the **cdp enable** command to enable the Cisco Discovery Protocol (CDP) feature at the switch level or at the interface level. Use the **no** form of this command to disable this feature. When the interface link is established, CDP is enabled by default

CDP version 1 (v1) and version 2 (v2) are supported in Cisco MDS 9000 Family switches. CDP packets with any other version number are silently discarded when received.

Examples

The following example disables the CDP protocol on the switch. When CDP is disabled on an interface, one packet is sent to clear out the switch state with each of the receiving devices:

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

```
Operation in progress. Please check global parameters
switch(config-console)#
```

The following example enables (default) the CDP protocol on the switch. When CDP is enabled on an interface, one packet is sent immediately. Subsequent packets are sent at the configured refresh time.

```
switch(config)# cdp enable
Operation in progress. Please check global parameters
switch(config)#
```

The following example configures the Gigabit Ethernet interface 8/8 and disables the CDP protocol on this interface. When CDP is disabled on an interface, one packet is sent to clear out the switch state with each of the receiving devices.

```
switch(config)#
interface gigbitethernet 8/8
switch(config-if)#
no cdp enable
Operation in progress. Please check interface parameters
switch(config-console)#
```

The following example enables (default) the CDP protocol on the selected interface. When CDP is enabled on this interface, one packet is sent immediately. Subsequent packets are sent at the configured refresh time.

```
switch(config-if)#
cdp enable
Operation in progress. Please check interface parameters
switch(config)#
```

The following example globally configures the refresh time interval for the CDP protocol in seconds. The default is 60 seconds and the valid range is from 5 to 255 seconds.

```
switch#
config terminal
switch(config)#
cdp timer 100
switch(config)#
```

The following example globally configures the hold time advertised in CDP packet in seconds. The default is 180 seconds and the valid range is from 10 to 255 seconds.

```
switch#
config terminal
switch(config)#
cdp holdtime 200
switch(config)#
```

The following example globally configures the CDP version. The default is version 2 (v2). The valid options are v1 and v2.

```
switch# config terminal
switch(config)# cdp advertise v1
switch(config)#
```

Related Commands

Command	Description
clear cdp	Clears global or interface-specific CDP configurations.
show cdp	Displays configured CDP settings and parameters.

cfs distribute

To enable or disable Cisco Fabric Services (CFS) distribution on the switch, use the **cfs distribute** command in configuration mode. To disable this feature, use the **no** form of the command.

cfs distribute
no cfs distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

CFS distribution is enabled.

Command Modes

Configuration mode

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

By default CFS is in the distribute mode. In the distribute mode, fabric wide distribution is enabled. Applications can distribute data/configuration to all CFS-capable switches in the fabric where the application exists. This is the normal mode of operation.

If CFS distribution is disabled, using the **no cfs distribute** command causes the following to occur:

- CFS and the applications using CFS on the switch are isolated from the rest of the fabric even though there is physical connectivity.
- All CFS operations are restricted to the isolated switch.
- All the CFS commands continue to work similar to the case of a physically isolated switch.
- Other CFS operations (for example, lock, commit, and abort) initiated at other switches do not have any effect at the isolated switch.
- CFS distribution is disabled over both Fibre Channel and IP.

Examples

The following example shows how to disable CFS distribution:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no cfs distribute
```

The following example shows how to reenable CFS distribution:

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

Related Commands

Command	Description
show cfs status	Displays whether CFS distribution is enabled or disabled.

cfs ipv4 distribute

To enable Cisco Fabric Services (CFS) distribution over IPv4 for applications that want to use this feature, use the **cfs ipv4 distribute** command in configuration mode. To disable this feature, use the **no** form of the command.

cfs ipv4 distribute
no cfs ipv4 distribute

Syntax Description

This command has no arguments or keywords.

Command Default

CFS distribution is enabled.

CFS over IP is disabled.

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

All CFS over IP enabled switches with similar multicast addresses form one CFS over IP fabric. CFS protocol specific distributions, such as the keep-alive mechanism for detecting network topology changes, use the IP multicast address to send and receive information.

Observe the following guidelines when using this command:

- If a switch is reachable over both IP and Fibre Channel, application data will be distributed over Fibre Channel.
- You can select either an IPv4 or IPv6 distribution when CFS is enabled over IP.
- Both IPv4 and IPv6 distribution cannot be enabled on the same switch.
- A switch that operate IPv4 distribution enabled cannot detect a switch that IPv6 distribution enabled. The switches behave as if they are in two different fabrics even though they are connected to each other.

Examples

The following example shows how to disable CFS IPv4 distribution:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no cfs ipv4 distribute
This will prevent CFS from distributing over IPv4 network.
Are you sure? (y/n)  [n]
```

The following example shows how to reenable CFS IPv4 distribution:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# cfs ipv4 distribute
```

Related Commands

Command	Description
cfs ipv4 mcast-address	Configures an IPv4 multicast address for Cisco Fabric Services (CFS) distribution over IPv4.
show cfs status	Displays whether CFS distribution is enabled or disabled.

cfs ipv4 mcast-address

To configure an IPv4 multicast address for Cisco Fabric Services (CFS) distribution over IPv4, use the **cfs ipv4 mcast-address** command in configuration mode. To disable this feature, use the **no** form of the command.

cfs ipv4 mcast-address ipv4-address
no cfs ipv4 mcast-address ipv4-address

Syntax Description

ipv4-address	Specifies an IPv4 multicast address for CFS distribution over IPv4. The range of valid IPv4 addresses is 239.255.0.0 through 239.255.255.255, and 239.192.0.0 through 239.251.251.251.

Command Default

Multicast address: 239.255.70.83.

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Before using this command, enable CFS distribution over IPv4 using the **cfs ipv4 distribute** command.

All CFS over IP enabled switches with similar multicast addresses form one CFS over IP fabric. CFS protocol specific distributions, such as the keepalive mechanism for detecting network topology changes, use the IP multicast address to send and receive information.

Note CFS distributions for application data use directed unicast.

You can configure a value for a CFS over IP multicast address. The default IPv4 multicast address is 239.255.70.83.

Examples

The following example shows how to configure an IP multicast address for CFS over IPv4:

```
switch# config t
switch(config)# cfs ipv4 mcast-address 239.255.1.1
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure? (y/n) [n] y
```

The following example shows how to revert to the default IPv4 multicast address for CFS distribution over IPv4. The default IPv4 multicast address for CFS is 239.255.70.83:

```
switch(config)# no cfs ipv4 mcast-address 10.1.10.100
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure? (y/n) [n] y
```

Related Commands

Command	Description
cfs ipv4 distribute	Enables or disables Cisco Fabric Services (CFS) distribution over IPv4.
show cfs status	Displays whether CFS distribution is enabled or disabled.

cfs ipv6 distribute

To enable Cisco Fabric Services (CFS) distribution over IPv6 for applications that want to use this feature, use the **cfs ipv6 distribute** command in configuration mode. To disable this feature, use the **no** form of the command.

cfs ipv6 distribute
no cfs ipv6 distribute

Syntax Description

This command has no arguments or keywords.

Command Default

CFS distribution is enabled.

CFS over IP is disabled.

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

All CFS over IP enabled switches with similar multicast addresses form one CFS over IP fabric. CFS protocol specific distributions, such as the keepalive mechanism for detecting network topology changes, use the IP multicast address to send and receive information.

Observe the following guidelines when using this command:

- If a switch is reachable over both IP and Fibre Channel, application data will be distributed over Fibre Channel.
- You can select either an IPv4 or IPv6 distribution when CFS is enabled over IP.
- Both IPv4 and IPv6 distribution cannot be enabled on the same switch.
- A switch that operate IPv4 distribution enabled cannot detect a switch that IPv6 distribution enabled. The switches behave as if they are in two different fabrics even though they are connected to each other.

Examples

The following example shows how to disable CFS IPv6 distribution:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no cfs ipv6 distribute
This will prevent CFS from distributing over IPv6 network.
Are you sure? (y/n)  [n]
```

The following example shows how to reenable CFS IPv6 distribution:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# cfs ipv6 distribute
```

Related Commands

Command	Description
cfs ipv6 mcast-address	Configures an IPv6 multicast address for Cisco Fabric Services (CFS) distribution over IPv6.
show cfs status	Displays whether CFS distribution is enabled or disabled.

cfs ipv6 mcast-address

To configure an IPv6 multicast address for Cisco Fabric Services (CFS) distribution over IPv6, use the **cfs ipv6 mcast-address** command in configuration mode. To disable this feature, use the **no** form of the command.

cfs ipv6 mcast-address ipv6-address
no cfs ipv6 mcast-address ipv6-address

Syntax Description

ipv6-address	An IPv6 multicast address or CFS distribution over IPv6. The IPv6 Admin scope range is [ff15::/16, ff18::/16].

Command Default

Multicast address: ff15::efff:4653.

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Before using this command, enable CFS distribution over IPv6 using the **cfs ipv6 distribute** command.

All CFS over IP enabled switches with similar multicast addresses form one CFS over IP fabric. CFS protocol specific distributions, such as the keepalive mechanism for detecting network topology changes, use the IP multicast address to send and receive information.

Note CFS distributions for application data use directed unicast.

You can configure a CFS over IP multicast address value for IPv6. The default IPv6 multicast address is ff15::efff:4653. Examples of the IPv6 Admin scope range are ff15::0000:0000 to ff15::ffff:ffff and ff18::0000:0000 to ff18::ffff:ffff.

Examples

The following example shows how to configure an IP multicast address for CFS over IPv6:

```
switch# config t
switch(config)# cfs ipv6 mcast-address
ff13::e244:4754
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure? (y/n) [n] y
```

The following example shows how to revert to the default IPv6 multicast address for CFS distribution over IPv6. The default IPv6 multicast address for CFS is ff13:7743:4653.

```
switch(config)# no cfs ipv6
ff13::e244:4754
Distribution over this IP type will be affected
```

```
Change multicast address for CFS-IP ?
Are you sure? (y/n) [n] y
```

Related Commands

Command	Description
cfs ipv6 distribute	Enables or disables Cisco Fabric Services (CFS) distribution over IPv6.
show cfs status	Displays whether CFS distribution is enabled or disabled.

cfs region

To create a region that restricts the scope of application distribution to the selected switches, use the cfs region command in the configuration mode. To disable this feature, use the no form of this command.

cfs region region-id
no cfs region region-id

Syntax Description

region-id	Assigns an application to a region. A total of 200 regions are supported.

Command Default

None.

Configuration mode

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

An application can only be a part of one region on a given switch. By creating the region ID and assigning it to an application, the application distribution is restricted to switches with a similar region ID.

Cisco Fabric Services (CFS) regions provide the ability to create distribution islands within the application scope. Currently, the regions are supported only for physical scope applications. In the absence of any region configuration, the application will be a part of the default region. The default region is region ID 0. This command provides backward compatibility with the earlier release where regions were not supported. If applications are assigned to a region, the configuration check will prevent the downgrade. Fabric Manager supports CFS regions.

Examples

The following example shows how to create a region ID:

```
switch# config
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# cfs region 1
```

The following example shows how to assign an application to a region:

```
switch# cfs region 1
switch# config
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# cfs region 1
switch(config-cfs-region)# ntp
```

Note The applications assigned to a region have to be registered with CFS.

The following example shows how to remove an application assigned to a region:

```
switch# cfs region 1
```

```
switch# config
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# cfs region 1
switch(config-cfs-region)# no ntp
```

The following example shows how to remove all the applications from a region:

```
switch(config)# no cfs region 1
WARNING: All applications in the region wiil be  moved to default region.
Are you sure? (y/n)  [n] y
```

Related Commands

Command	Description
show cfs regions	Displays all configured applications with peers.

cfs static-peers

To enable static peers interface, use the **cfs static-peers** command. To disable this feature, use the **no** form of the command.

cfs static-peers
no cfs static-peers

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

This command enables the static peers with status and all the peers in the physical fabric.

Note The no cfs static-peers displays a warning string, and changes the entire fabric from static to dynamic.

Examples

The following example shows how to enable static peers interface:

```
Switch(config)# cfs static-peers
Warning: This mode will stop dynamic discovery and relay only on these peers.
Do you want to continue?(y/n) [n] y
Switch(config-cfs-static)#ip address 209.165.200.226
Switch(config-cfs-static)#ip address 209.165.200.227
Switch(config-cfs-static)#exit
Switch(config)#
```

Related Commands

Command	Description
show cfs static peers	Displays configured static peers with status.

channel mode active

To enable channel mode on a PortChannel interface, use the **channel mode active** command. To disable this feature, use the **no** form of the command.

channel mode active
no channel mode

Syntax Description

This command has no other arguments or keywords.

Command Default

Enabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

This command determines the protocol operate for all the member ports in the channel group associated with the port channel interface.

Examples

The following example shows how to disable channel mode on a PortChannel interface:

```
switch# config terminal
switch(config)# interface port-channel 10
switch(config-if)# no channel mode active
```

Related Commands

Command	Description
show interface port-channel	Displays PortChannel interface information.

channel-group

To add a port to a PortChannel group, use the **channel-group** command. To remove a port, use the **no** form of the command.

channel-group port-channel number force
no channel-group port-channel number force

Syntax Description

port-channel number	The PortChannel number. The range is 1 to 256.
force	Specifies the PortChannel to add a port, without compatibility check of port parameters, port mode and port speed.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
NX-OS 4.1(3)	Deleted auto keyword from the syntax description.
3.0(1)	This command was introduced.

Usage Guidelines

When ports are added to a PortChannel, manager checks for incompatibility in the port mode and port speed. If the ports are being added to the PortChannel, do not have compatible parameters, the ports will not be added to the PortChannel. The force option bypasses, the port parameter compatibility check, and adds the port to a PortChannel. It also forces the individual member interfaces to inherit the port parameters configured on the PortChannel itself. If you configure switchport speed 4000 on the PortChannel then the member inerface is forced to that setting.

force option is used to override the port's parameters. The auto mode support is not available after Release 4.x. To convert auto PortChannel to active mode PortChannel, use the port-channel persistent command. This command needs to be run on both sides of the auto Port Channel.

Examples

The following example shows how to add a port to the PortChannel:

```
switch# config terminal
switch(config)# interface fc 1/1
switch(config-if)# channel-group 2 force
fc1/1 added to port-channel 2 and disabled
please do the same operation on the switch at the other end of the port-channel,
then do "no shutdown" at both end to bring them up
switch(config-if)#
```

Related Commands

Command	Description
show interface port-channel	Displays the PortChannel interface information.

cimserver

To configure the Common Information Models (CIM) parameters, use the **cimserver** command. Use the **no** form of this command to revert to factory defaults.

cimserver {**certificate** {**bootflash:***filename*|**slot0 :** *filename*|**volatile:***filename*}|**clearcertificate** *filename*|**enable**|**enablehttp**|**enablehttps**}
no cimserver {**certificate** {**bootflash :** *filename*|**slot0 :** *filename*|**volatile :** *filename*}|**clearcertificate** *filename*|**enable**|**enablehttp**|**enablehttps**}

Syntax Description

certificate	Installs the Secure Socket Layer (SSL) certificate
bootflash:	Specifies the location for internal bootflash memory.
filename	The name of the license file with a .pem extension.
slot0: filename	Specifies the location for the CompactFlash memory or PCMCIA card.
volatile: filename	Specifies the location for the volatile file system.
clearcertificate filename	Clears a previously installed SSL certificate.
enable	Enables and starts the CIM server.
enablehttp	Enables the HTTP (non-secure) protocol for the CIM server (default).
enablehttps	Enables the HTTPS (secure) protocol for the CIM server.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
1.3(1)	This command was introduced.
5.2(1)	This command was deprecated.

Usage Guidelines

A CIM client is required to access the CIM server. The client can be any client that supports CIM.

Examples

The following example installs a Secure Socket Layer (SSL) certificate specified in the file named with a .pem extension:

```
switch#
config terminal
switch(config)# cimserver certificateName bootflash:simserver.pem
```

The following example clears the specified SSL certificate:

```
switch(config)#

cimserver clearCertificateName bootflash:simserver.pem
```

Related Commands

Command	Description
show csimserver	Displays configured CIM settings and parameters.

cimserver clearcertificate

To clear the cimserver certificate, use the cimsever clearcertificate command in configuration mode.

cimserver clearcertificate

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
3.3(1a)	This command was introduced.
5.2(1)	This command was deprecated.

Usage Guidelines

You need not specify the certificate name.

Examples

The following example shows how to clear the cimserver certificate:

```
switch# config
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# cimserver clearcertificate
```

Related Commands

Command	Description
show cimserver certificate name	Displays the cimserver certificate filename.

cimserver loglevel

To configure the cimserver log level filter, use the cimsever loglevel command in configuration mode.

cimserver loglevel filter value

Syntax Description

filter value	1–Specifies the cimserver log filter levels. The range is 1 to 5.
	2–Sets the current value for the log level property to trace.
	3–Sets the current value for the log level property to information.
	4–Sets the current value for the log level property to warning.
	5–Sets the current value for the log level property to severe.
	6–Sets the current value for the log level property to fatal.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
3.3(1a)	This command was introduced.
5.2(1)	This command was deprecated.

Usage Guidelines

None

Examples

The following example displays the cimserver log level:

```
switch# config
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# cimserver loglevel 2
Current value for the property logLevel is set to "INFORMATION" in CIMServer.
```

Related Commands

Command	Description
show cimserver logs	Displays the cimserver logs.

class

To select a QoS policy map class for configuration, use the **class** command in QoS policy map configuration submode. To disable this feature, use the **no** form of the command.

class *class-map-name*
no class *class-map-name*

Syntax Description

class-map-name	The QoS policy class map to configure.

Command Default

Disabled

Command Modes

QoS policy map configuration submode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Before you can configure a QoS policy map class you must complete the following:

- Enable the QoS data traffic feature using the **qos enable** command.
- Configure a QoS class map using the **qos class-map** command.
- Configure a QoS policy map using the **qos policy-map** command.

After you configure the QoS policy map class, you can configure the Differentiated Services Code Point (DSCP) and priority for frames matching this class map.

Examples

The following example shows how to select a QoS policy map class to configure:

```
switch# config terminal
switch(config)# qos enable
switch(config)# qos class-map class-map1
switch(config)# qos policy-map policyMap1
switch(config-pmap)# class class-map1
```

Related Commands

Command	Description
dscp	Configures the DSCP in the QoS policy map class.
qos class-map	Configures a QoS class map.
qos enable	Enables the QoS data traffic feature on the switch.
qos policy-map	Configures a QoS policy map.
priority	Configures the priority in the QoS policy map class.

Command	Description
show qos	Displays the current QoS settings.

clear accounting log

To clear the accounting log, use the **clear accounting log** command.

clear accounting log

Syntax Description

This command has no other arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None

Examples

The following example clears the accounting log:

```
switch# clear accounting session
```

Related Commands

Command	Description
show accounting log	Displays the accounting log contents.

clear arp-cache

To clear the ARP cache table entries, use the **clear arp-cache** command in EXEC mode.

clear arp-cache

Syntax Description

This command has no arguments or keywords.

Command Default

The ARP table is empty by default.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Examples

The following example shows how to clear the arp-cache table entries:

```
switch# clear arp-cache
```

Related Commands

Command	Description
show arp	Displays Address Resolution Protocol (ARP) entries.

clear asic-cnt

To clear ASCI counters, use the **clear asic-cnt** command in EXEC mode.

clear asic-cnt {**all**|**device-id**|**list-all-devices**}

Syntax Description

all	Clears the counter for all device types.
device-id	Clears the counter for device type device ID.
list-all-devices	Lists all device types.

Command Default

None

Command Modes

EXEC mode

Command History

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

Examples

The following example shows how to clear all counters on the module:

```
switch(config)# attach module 4
Attaching to module 4 ...
To exit type 'exit', to abort type '$.'
Last login: Mon Jan  5 13:04:02 2009 from 127.1.1.8 on pts/0
Linux lc04 2.6.10_mvl401-pc_target #1 Tue Dec 16 22:58:32 PST 2008 ppc GNU/Linux
module-4# clear asic-cnt all
Cleared counters for asic type id = 63, name = 'Stratosphere'
Cleared counters for asic type id = 46, name = 'transceiver'
Cleared counters for asic type id = 57, name = 'Skyline-asic'
Cleared counters for asic type id = 60, name = 'Skyline-ni'
Cleared counters for asic type id = 59, name = 'Skyline-xbar'
Cleared counters for asic type id = 58, name = 'Skyline-fwd'
Cleared counters for asic type id = 52, name = 'Tuscany-asic'
Cleared counters for asic type id = 54, name = 'Tuscany-xbar'
Cleared counters for asic type id = 55, name = 'Tuscany-que'
Cleared counters for asic type id = 53, name = 'Tuscany-fwd'
Cleared counters for asic type id = 73, name = 'Fwd-spi-group'
Cleared counters for asic type id = 74, name = 'Fwd-parser'
Cleared counters for asic type id = 10, name = 'eobc'
Cleared counters for asic type id = 1, name = 'X-Bus IO'
Cleared counters for asic type id = 25, name = 'Power Mngmnt Epld'
module-4#
```

The following example shows how to clear the specific counter:

```
module-4# clear asic-cnt device-id 1
Clearing counters for devId = 1, name = 'X-Bus IO'
module-4#
```

The following example shows how to list all device IDs:

```
module-4# clear asic-cnt list-all-devices
           Asic Name  |         Device ID
        Stratosphere  |                63
         transceiver  |                46
        Skyline-asic  |                57
          Skyline-ni  |                60
        Skyline-xbar  |                59
         Skyline-fwd  |                58
        Tuscany-asic  |                52
        Tuscany-xbar  |                54
         Tuscany-que  |                55
         Tuscany-fwd  |                53
       Fwd-spi-group  |                73
          Fwd-parser  |                74
                eobc  |                10
            X-Bus IO  |                 1
   Power Mngmnt Epld  |                25
module-4#
```

Related Commands

Command	Description
show arp	Displays Address Resolution Protocol (ARP) entries.

clear callhome session

To clear Call Home Cisco Fabric Services (CFS) session configuration and locks, use the **clear callhome session** command.

clear callhome session

Syntax Description

This command has no other arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to clear the Call Home session configuration and locks:

```
switch# clear callhome session
```

Related Commands

Command	Description
show callhome	Displays Call Home information.

clear cdp

To delete global or interface-specific CDP configurations, use the **clear cdp** command.

clear cdp {**counters**|**table**} [**interface** {**gigabitethernet** *slot/port*|**mgmt 0**}]

Syntax Description

counters	Enables CDP on globally or on a per-interface basis.
table	Specifies the EXEC command to be executed.
interface	(Optional) Displays CDP parameters for an interface.
gigabitethernet	Specifies the Gigabit Ethernet interface.
slot/*port*	Specifies the slot number and port number separated by a slash (/).
mgmt 0	Specifies the Ethernet management interface.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

You can use this command for a specified interface or for all interfaces (management and Gigabit Ethernet interfaces).

Examples

The following example clears CDP traffic counters for all interfaces:

```
switch# clear cdp counters
switch#
```

The following example clears CDP entries for the specified Gigabit Ethernet interface:

```
switch# clear cdp table interface gigabitethernet 4/1
switch#
```

Related Commands

Command	Description
cdp	Configures global or interface-specific CDP settings and parameters.
show cdp	Displays configured CDP settings and parameters.

clear cores

To clear all core dumps for the switch, use the **clear cores** command in EXEC mode.

clear cores

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The system software keeps the last few cores per service and per slot and clears all other cores present on the active supervisor module.

Examples

The following example shows how to clear all core dumps for the switch:

```
switch# clear cores
```

Related Commands

Command	Description
show cores	Displays core dumps that have been made.

clear counters (EXEC mode)

To clear the interface counters, use the **clear counters** command in EXEC mode.

clear counters {**all**|**interface** {**fc**|**mgmt**|**port-channel**|**sup-fc**|**vsan**} **number**}

Syntax Description

all	Clears all interface counters.
interface	Clears interface counters for the specified interface.
number	The number of the slot or interface being cleared.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The following table lists the number ranges interface types:

Keyword	Interface Type	Number
fc	Fibre Channel	1– 2 or 1– 9 (slot)
gigabitethernet	Gigabit Ethernet	1– 2 or 1– 9 (slot)
mgmt	Management	0–0 (management interface)
port-channel	PortChannel	1–128 (PortChannel)
sup-fc	Inband	0–0 (Inband interface)
vsan	VSAN	1– 4093 (VSAN ID)

This command clears counters displayed in the **show interface** command output.

Examples

The following example shows how to clear counters for a VSAN interface:

```
switch# clear counters interface vsan 13
```

Related Commands

Command	Description
show interface	Displays interface information.

clear counters (SAN extension N port configuration mode)

To clear SAN extension tuner N port counters, use the **clear counters** command.

clear counters

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

SAN extension N port configuration submode

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to clear SAN extension tuner N port counters:

```
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)# clear counters
```

Related Commands

Command	Description
show san-ext-tuner	Displays SAN extension tuner information.

clear counters interface

To clear the aggregate counters for the interface, use the **clear counters** interface command.

clear counters interface interface snmp

Syntax Description

interface	Specifies the interface.
snmp	Clears SNMP interface counters.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	Added the snmp option to the syntax description.

Usage Guidelines

This command clears counter displayed in the **show interface** command output.

Examples

The following example shows how to clear the aggregate counters for the interface:

```
switch(config)# clear counters interface e2/1 snmp
switch(config)#
```

Related Commands

Command	Description
show interface	Displays interface information.

clear counters interface all

To clear all interface counters, use the **clear counters** interface all command.

clear counters interface all snmp

Syntax Description

snmp	Clears SNMP interface counters.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	Added the snmp option to the syntax description.

Usage Guidelines

This command clears counter displayed in the **show interface** command output.

Examples

The following example shows how to clear all SNMP interface counters:

```
switch(config)# clear counters interface all snmp
switch(config)#
```

Related Commands

Command	Description
show interface	Displays interface information.

clear crypto ike domain ipsec sa

To clear the IKE tunnels for IPsec, use the **clear crypto ike domain ipsec sa** command.

clear crypto ike domain ipsec sa [*tunnel-id*]

Syntax Description

tunnel-id	(Optional) The tunnel ID. The range is 1 to 2147483647.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

If the tunnel ID is not specified, all IKE tunnels are cleared.

Note The crypto ikes feature is not supported on the Cisco MDS 9148 and Cisco MDS 9148S, and Cisco MDS 9396S Switches.

Examples

The following example shows how to clear all IKE tunnels:

```
switch# clear crypto ike domain ipsec sa
```

Related Commands

Command	Description
crypto ike domain ipsec	Configures IKE information.
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

clear crypto sa domain ipsec

To clear the security associations for IPsec, use the **clear crypto sa domain ipsec** command.

clear crypto sa domain ipsec interface gigabitethernet *slot / port* {**inbound**|**outbound**} **sa** *sa-index*

Syntax Description

interface gigabitethernet *slot*/*port*	Specifies the Gigabit Ethernet interface.
inbound	Specifies clearing inbound associations.
outbound	Specifies clearing output associations.
sa *sa-index*	Specifies the security association index. The range is 1 to 2147483647.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To clear security associations, IPsec must be enabled using the **crypto ipsec enable** command.

Examples

The following example shows how to clear a security association for an interface:

```
switch# clear crypto sa domain ipsec interface gigabitethernet 1/2 inbound sa 1
```

Related Commands

Command	Description
show crypto sad domain ipsec	Displays IPsec security association database information.

clear debug-logfile

To delete the debug log file, use the **clear debug-logfile** command in EXEC mode.

clear debug-logfile *filename*

Syntax Description

filename	The name (restricted to 80 characters) of the log file to be cleared. The maximum size of the log file is 1024 bytes.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Examples

The following example shows how to clear the debug logfile:

```
switch# clear debug-logfile debuglog
```

Related Commands

Command	Description
show debug logfile	Displays the log file contents.

clear device-alias

To clear device alias information, use the **clear device-alias** command.

clear device-alias {**database**|**session**|**statistics**}

Syntax Description

database	Clears the device alias database.
session	Clears session information.
statistics	Clears device alias statistics.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to clear the device alias session:

```
switch# clear device-alias session
```

Related Commands

Command	Description
show device-alias	Displays device alias database information.

clear dpvm

To clear Dynamic Port VSAN Membership (DPVM) information, use the **clear dpvm** command.

clear dpvm {**auto-learn** [**pwwn** *pwwn-id*]|**session**}

Syntax Description

auto-learn	Clears automatically learned (autolearn) DPVM entries.
pwwn *pwwn-id*	(Optional) Specifies the pWWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
session	Clears the DPVM session and locks.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, DVPM must be enabled using the **dpvm enable** command.

Examples

The following example shows how to clear a single autolearned entry:

```
switch# clear dpvm auto-learn pwwn 21:00:00:20:37:9c:48:e5
```

The following example shows how to clear all autolearn entries:

```
switch# clear dpvm auto-learn
```

The following example shows how to clear a session:

```
switch# clear dpvm session
```

Related Commands

Command	Description
dpvm enable	Enables DPVM.
show dpvm	Displays DPVM database information.

clear dpvm merge statistics

To clear the DPVM merge statistics, use the clear dpvm merge statistics command.

clear dpvm merge statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to clear the DPVM merge statistics:

```
switch#(config)# clear dpvm merge statistics
switch#(config)#
```

Related Commands

Command	Description
show dpvm merge statistics	Displays the DPVM merge statistics.

clear fabric-binding statistics

To clear fabric binding statistics in a FICON enabled VSAN, use the **clear fabric-binding statistics** command in EXEC mode.

clear fabric-binding statistics vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the FICON-enabled VSAN. The ID of the VSAN is from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None

Examples

The following example clears existing fabric binding statistics in VSAN 1:

```
switch# clear
 fabric-binding statistics vsan 1
```

Related Commands

Command	Description
show fabric-binding efmd statistics	Displays existing fabric binding statistics information.

clear fcanalyzer

To clear the entire list of configured hosts for remote capture, use the **clear fcanalyzer** command in EXEC mode.

clear fcanalyzer

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command clears only the list of configured hosts. Existing connections are not terminated.

Examples

The following example shows how to clear the entire list of configured hosts for remote capture:

```
switch# clear fcanalyzer
```

Related Commands

Command	Description
show fcanalyzer	Displays the list of hosts configured for a remote capture.

clear fcflow stats

To clear Fibre Channel flow statistics, use the **clear fcflow stats** command in EXEC mode.

clear fcflow stats [aggregated] module module-number index flow-number

Syntax Description

aggregated	(Optional) Clears the Fibre Channel flow aggregated statistics.
module	Clears the statistics for a specified module.
module-number	Specifies the module number.
index	Clears the Fibre Channel flow counters for a specified flow index.
flow-number	Specifies the flow index number.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
1.0(2)	This command was introduced.

Examples

The following example shows how to clear aggregated Fibre Channel flow statistics for flow index 1 of module 2:

```
switch(config)# clear fcflow stats aggregated module 2 index 1
```

Related Commands

Command	Description
show fcflow	Displays the fcflow statistics.

clear fcns statistics

To clear the name server statistics, use the **clear fcns statistics** command in EXEC mode.

clear fcns statistics vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Clears FCS statistics for a specified VSAN ranging from 1 to 4093.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
1.0(3)	This command was introduced.

Examples

The following example shows how to clear the name server statistics:

```
switch# show fcns statistics
Name server statistics for vsan 1
==================================
registration requests received = 0
deregistration requests received = 0
queries received = 23
queries sent = 27
reject responses sent = 23
RSCNs received = 0
RSCNs sent = 0
switch# clear fcns statistics vsan 1
switch# show fcns statistics
Name server statistics for vsan 1
==================================
registration requests received = 0
deregistration requests received = 0
queries received = 0
queries sent = 0
reject responses sent = 0
RSCNs received = 0
RSCNs sent = 0
switch#
```

Related Commands

Command	Description
show fcns statistics	Displays the name server statistics.

clear fc-redirect config

To delete a FC-Redirect configuration on a switch, use the clear fc-redirect config command.

clear fc-redirect config vt vt-pwwn [local-switch-only]

Syntax Description

vt vt-pwwn	Specify the VT pWWN for the configuration to be deleted.
local-switch-only	(Optional) The configuration is deleted locally only.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

This command is used as a last option if deleting the configuration through the application is not possible.

This command will delete any configuration (including active configurations) on FC-Redirect created by applications such as SME/DMM that may lead to data loss. When you enter this command, the host server communicates to the storage array directly by passing the individual Intelligent Service Applications causing data corruption. Use this command as a last option to clear any leftover configuration that cannot be deleted from the application (DMM/SME). Use this command while decommissioning the switch.

Examples

The following example clears the FC-Redirect configuration on the switch:

```
switch# clear fc-redirect config vt 2f:ea:00:05:30:00:71:64
Deleting a configuration MAY result in DATA CORRUPTION.
Do you want to continue? (y/n) [n] y
```

Related Commands

Command	Description
show fc-redirect active-configs	Displays all active configurations on the switch.

clear fc-redirect decommission-switch

To remove all existing FC-Redirect configurations and disable any further FC-Redirect configurations on a switch, use the clear fc-redirect decommission-switch command.

clear fc-redirect decommission-switch

Syntax Description

This command has no other arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

This command is used after write erase. The command is also used to move a switch from a fabric with FC-Redirect configurations to another fabric. After using this command, disconnect the switch from the fabric and reboot the switch before using it in another fabric.

Examples

The following example shows how to decommission FC-Redirect on a switch:

```
switch# clear fc-redirect decommission-switch
This Command removes any FC-Redirect configuration and disables
FC-Redirect on this switch. Its usage is generally recommended in
the following cases:
   1) After 'write erase'
   2) When removing the switch from the fabric.
If NOT for the above, Decommissioning a switch MAY result in
DATA CORRUPTION.

Do you want to continue? (Yes/No) [No] Yes

Please check the following before proceeding further:
   1) Hosts / targets connected locally are NOT involved in any
      FC-Redirect configuration.
   2) No application running on this switch created an FC-Redirect
      Configuration
   Please use the command 'show fc-redirect active-configs' to check
   these.

Do you want to continue? (Yes/No) [No] Yes
switch#
```

Related Commands

Command	Description
show fc-redirect active-configs	Displays all active configurations on a switch.

clear fcs statistics

To clear the fabric configuration server statistics, use the **clear fcs statistics** command in EXEC mode.

clear fcs statistics vsan vsan-id

Syntax Description

vsan *vsan-id*	FCS statistics are to be cleared for a specified VSAN ranging from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Examples

The following example shows how to clear the fabric configuration server statistics for VSAN 10:

```
switch# clear fcs statistics vsan 10
```

Related Commands

Command	Description
show fcs statistics	Displays the fabric configuration server statistics information.

clear fctimer session

To clear fctimer Cisco Fabric Services (CFS) session configuration and locks, use the **clear fctimer session** command.

clear fctimer session

Syntax Description

This command has no other arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to clear fctimer session:

```
switch# clear fctimer session
```

Related Commands

Command	Description
show fctimer	Displays fctimer information.

clear ficon

Use the **clear ficon** command in EXEC mode to clear the FICON information for the specified VSAN.

clear ficon vsan *vsan-id* [{**allegiance**|**timestamp**}]

Syntax Description

vsan *vsan-id*	Specifies the FICON-enabled VSAN. The ID of the VSAN is from 1 to 4093.
allegiance	(Optional) Clears the FICON device allegiance.
timestamp	(Optional) Clears the FICON VSAN specific timestamp.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The **clear ficon vsan** *vsan-id* **allegiance** command aborts the currently executing session.

Examples

The following example clears the current device allegiance for VSAN 1:

```
switch# clear ficon vsan 1 allegiance
```

The following example clears the VSAN clock for VSAN 20:

```
switch# clear ficon vsan 20 timestamp
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.

clear fspf counters

To clear the Fabric Shortest Path First statistics, use the **clear fspf counters** command in EXEC mode.

clear fspf counters vsan *vsan-id* [**interface** *type*]

Syntax Description

vsan	Indicates that the counters are to be cleared for a VSAN.
vsan-id	The ID of the VSAN is from 1 to 4093.
interface *type*	(Optional). The counters are to be cleared for an interface. The interface types are fc for Fibre Channel, and port-channel for PortChannel.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If the interface is not specified, then all of the counters of a VSAN are cleared. If the interface is specified, then the counters of the specific interface are cleared.

Examples

The following example clears the FSPF t statistics on VSAN 1:

```
switch# clear fspf counters vsan 1
```

The following example clears FSPF statistics specific to the Fibre Channel interface in VSAN 1, Slot 9 Port 32:

```
switch#  clear fspf counters vsan 1 interface fc 9/32
```

Related Commands

Command	Description
show fspf	Displays global FSPF information for a specific VSAN.

clear install failure-reason

To remove the upgrade failure reason log created during in-service software upgrades (ISSUs) on the Cisco MDS 9124 Fabric Switch, use the clear install failure-reason command.

Caution If you remove the upgrade failure reason log, then you will not have any information to help you debug in the event of an ISSU failure.

clear install failure-reason

Syntax Description

This command has no other arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This command is supported only on the Cisco MDS 9124 Fabric Switch.

Examples

The following example removes all upgrade failure reason logs on a Cisco MDS 9124 Fabric Switch:

```
switch# clear install failure-reason
```

Related Commands

Command	Description
show install all failure-reason	Displays the reasons why an upgrade cannot proceed in the event of an ISSU failure.
show install all status	Displays the status of an ISSU on a Cisco MDS 9124 Fabric Switch.

clear ip access-list counters

To clear IP access list counters, use the **clear ip access-list counters** command in EXEC mode.

clear ip access-list counters *list-name*

Syntax Description

list-name	Specifies the IP access list name (maximum 64 characters).

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

The following example clears the counters for an IP access list:

```
switch# clear ip access-list counters adminlist
```

Related Commands

Command	Description
show ip access-list	Displays IP access list information.

clear ips arp

To clear ARP caches, use the **clear ips arp** command in EXEC mode.

clear ips arp {**address ip-address**|**interface gigabitethernet module-number**}

Syntax Description

address	Clears fcflow aggregated statistics.
ip-address	Enters the peer IP address.
interface gigabitethernet	Specifies the Gigabit Ethernet interface.
module-number	Specifies the slot and port of the Gigabit Ethernet interface.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

The ARP cache can be cleared in two ways: clearing just one entry or clearing all entries in the ARP cache.

The following example clears one ARP cache entry:

```
switch# clear ips arp address 10.2.2.2 interface gigabitethernet 8/7
arp clear successful
```

The following example clears all ARP cache entries:

```
switch# clear ips arp interface gigabitethernet 8/7
arp clear successful
```

clear ips stats

To clear IP storage statistics, use the **clear ips stats** command in EXEC mode.

clear ips stats {**all** [**interface gigabitethernet** *slot/port*]|**buffer interface gigabitethernet** *slot/port*|**dma-bridge interface gigabitethernet** *slot/port*|**icmp interface gigabitethernet** *slot/port*|**ip interface gigabitethernet** *slot/port*|**ipv6 traffic interface gigabitethernet** *slot/port*|**mac interface gigabitethernet** *slot/port*|**tcp interface gigabitethernet** *slot/port*}

Syntax Description

all	Clears all IPS statistics.
interface gigabitethernet	(Optional) Clears the Gigabit Ethernet interface.
slot/port	Specifies the slot and port numbers.
buffer	Clears IP storage buffer information.
dma-bridge	Clears direct memory access (DMA) statistics.
icmp	Clears ICMP statistics.
ip	Clears IP statistics.
ipv6	Clears IPv6 statistics.
mac	Clears Ethernet MAC statistics.
tcp	Clears TCP statistics.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Examples

The following example clears all IPS statistics on the specified interface:

```
switch# clear ips all interface gigabitethernet 8/7
switch#
```

clear ips stats fabric interface

To clear the statistics for a given iSCSI or FCIP interface on a Cisco MDS 9000 18/4-Port Multi Service Module IPS linecard, use the clear ips stats fabric interface command.

clear ips stats fabric interface [{**iscsi slot/port**|**fcip N**}]

Syntax Description

iscsi slot/port	(Optional) Clears Data Path Processor (DPP) fabric statistics for the iSCSI interface.
fcip N	(Optional) Clears DPP fabric statistics for the FCIP interface.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example clears the statistics for a given iSCSI or FCIP interface:

```
switch# clear ips stats fabric interface fcip ?
<1-255>  Fcip interface number
switch# clear ips stats fabric interface fcip 1
switch#
switch# clear ips stats fabric interface iscsi 1/1
switch#
```

Related Commands

Command	Description
show ips stats fabric interface	Displays the fabric-related statistics for the given iSCSI or FCIP interface on a Cisco MDS 9000 18/4-Port Multi Service Module IPS linecard.

clear ipv6 access-list

To clear IPv6 access control list statistics, use the **clear ipv6 access-list** command.

clear ipv6 access-list [list-name]

Syntax Description

access-list	Displays a summary of access control lists (ACLs).
list-name	(Optional) Specifies the name of the ACL. The maximum size is 64.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

You can use the **clear ipv6 access-list command to clear IPv6-ACL statistics.**

Examples

The following example displays information about an IPv6-ACL:

```
switch# clear ipv6 access-list testlist
switch#
```

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6-ACL.
show ipv6	Displays IPv6 configuration information.

clear ipv6 neighbors

To clear the IPv6 neighbor cache table, use the **clear ipv6 neighbors** command.

clear ipv6 neighbors

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

None.

Examples

The following example flushes the IPv6 neighbor cache table:

```
switch# clear ipv6 neighbors
switch#
```

Related Commands

Command	Description
ipv6 nd	Configures IPv6 neighbor discovery commands.
show ipv6 neighbors	Displays IPv6 neighbors configuration information.

clear islb session

To clear a pending iSLB configuration, use the **clear islb session** command.

clear islb session

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can use the **clear islb session** command to clear a pending iSLB configuration. This command can be executed from any switch by a user with admin privileges.

Examples

The following example clears a pending iSLB configuration:

```
switch# clear
 islb session
```

Related Commands

Command	Description
islb abort	Discards a pending iSLB configuration.
show islb cfs-session status	Displays iSLB session details.
show islb pending	Displays an iSLB pending configuration.
show islb pending-diff	Displays iSLB pending configuration differences.
show islb session	Displays iSLB session information.
show islb status	Displays iSLB CFS status.
show islb vrrp	Displays iSBL VRRP load balancing information.

clear ivr fcdomain database

To clear the IVR fcdomain database, use the **clear ivr fcdomain database** command in EXEC mode.

clear ivr fcdomain database

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

None

Examples

The following example clears all IVR fcdomain database information:

```
switch# clear ivr fcdomain database
```

Related Commands

Command	Description
show ivr fcdomain database	Displays IVR fcdomain database entry information.

clear ivr service-group database

To clear an inter-VSAN routing (IVR) service group database, use the **clear ivr service-group database** command.

clear ivr service-group database

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None

Examples

The following example clears the **ivr service-group database:**

```
switch# clear ivr service-group database
```

Related Commands

Command	Description
show ivr service-group database	Displays an IVR service group database.

clear ivr zone database

To clear the Inter-VSAN Routing (IVR) zone database, use the **clear ivr zone database** command in EXEC mode.

clear ivr zone database

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
1.3(1)	This command was introduced.

Examples

The following example clears all configured IVR information:

```
switch# clear ivr zone database
```

clear license

To uninstall a license, use the **clear license** command in EXEC mode.

clear license filename

Syntax Description

filename	Specifies the license file to be uninstalled.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
1.3(2)	This command was introduced.

Examples

The following example clears a specific license:

```
switch# clear license Ficon.lic
Clearing license Ficon.lic:
SERVER this_host ANY
VENDOR cisco
# An example fcports license
INCREMENT SAN_EXTN_OVER_IP cisco 1.000 permanent 1 HOSTID=VDH=ABCD \
        NOTICE=<LicFileID>san_extn2.lic</LicFileID><LicLineID>1</LicLineID> \
        SIGN=67CB2A8CCAC2

Do you want to continue? (y/n) y
Clearing license ..done
switch#
```

Related Commands

Command	Description
show license	Displays license information.

clear line

To clear VTY sessions, use the **clear line** command in EXEC mode.

clear line vty-name

Syntax Description

vty-name	Specifies the VTY name (maximum 64 characters).

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
1.2(1)	This command was introduced.

Examples

The following example clears one ARP cache entry:

```
switch# clear line Aux
arp clear successful
```

Related Commands

Command	Description
show line	Displays line information.

clear logging

To delete the syslog information, use the **clear logging** command in EXEC mode.

clear logging {**logfile**|**nvram**|**onboard information** [**module slot**]|**session**}

Syntax Description

logfile	Clears log file messages.
nvram	Clears NVRAM logs.
onboard *information*	Clears onboard failure logging (OBFL) information. The types of information include **boot-uptime**, **cpu-hog**, **device-version**, **endtime**, **environmental-history**, **error-stats**, **exception-log**, **interrupt-stats**, **mem-leak**, **miscellaneous-error**, **module**, **obfl-history**, **obfl-log**, **register-log**, **stack-trace**, **starttime**, **status**, and **system-health**.
module *slot*	(Optional) Clears OBFL information for a specified module.
session	Clears a logging session.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **onboard**, **module** and **session** options.

Examples

The following example shows how to clear the debug log file:

```
switch# clear logging logfile
```

The following example shows how to clear the onboard system health log file:

```
switch# clear logging onboard system-health
!!!WARNING! This will clear the selected logging buffer!!
Do you want to continue? (y/n)  [n]
```

Related Commands

Command	Description
show logging	Displays logging information.

clear ntp

To clear Network Time Protocol (NTP) information, use the **clear ntp** command in EXEC mode.

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

Syntax Description

session	Clears NTP CFS session configuration and locks.
statistics	Clears NTP statistics.
all-peers	Clears I/O statistics for all peers.
io	Clears I/O statistics for I/O devices.
local	Clears I/O statistics for local devices.
memory	Clears I/O statistics for memory.

Command Default

None

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 clear NTP statistics for all peers:

```
switch# clear ntp statistics all-peers
```

The following example shows how to clear NTP statistics for I/O devices:

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

The following example shows how to clear NTP statistics for local devices:

```
switch# clear ntp statistics local
```

The following example shows how to clear NTP statistics for memory:

```
switch# clear ntp statistics memory
```

Related Commands

Command	Description
show ntp	Displays the configured server and peer associations.

clear port-security

To clear the port security information on the switch, use the **clear port-security** command in EXEC mode.

Syntax Description

database	Clears the port security active configuration database.
auto-learn	Clears the auto-learn entries for a specified interface or VSAN.
interface fc *slot/port*	Clears entries for a specified interface.
port-channel *port*	Clears entries for a specified PortChannel. The range is 1 to 128.
session	Clears the port security CFS configuration session and locks.
statistics	Clears the port security counters.
vsan vsan-id	Clears entries for a specified VSAN ID. The range is 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.2(1)	This command was introduced.
2.0(x)	Added the **session** option.

Usage Guidelines

The active database is read-only and **clear port-security database** command can be used when resolving conflicts.

Examples

The following example clears all existing statistics from the port security database for a specified VSAN:

```
switch# clear port-security statistics vsan 1
```

The following example clears learnt entries in the active database for a specified interface within a VSAN:

```
switch# clear port-security database auto-learn interface fc1/1 vsan 1
```

The following example clears learnt entries in the active database up to for the entire VSAN:

```
switch# clear port-security database auto-learn vsan 1
```

Related Commands

Command	Description
show port-security	Displays the configured port security information.

clear processes log

To clear the log files on the switch, use the **clear processes log** command in EXEC mode.

clear processes log {**all**|**pid pid-number**}

Syntax Description

all	Deletes all of the log files.
pid	Deletes the log files of a specific process.
pid-number	Specifies the process ID, which must be from 0 to 2147483647.

Command Default

None

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 clear all of the log files on the switch :

```
switch# clear processes log all
```

Related Commands

Command	Description
show processes	Displays the detailed running or log information of processes or high availability applications.

clear qos statistics

To clear the quality of services statistics counters, use the **clear qos statistics** command in EXEC mode.

clear qos statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to clear the quality of service counters:

```
switch# clear qos statistics
```

Related Commands

Command	Description
show qos statistics	Displays the current QoS settings, along with a number of frames marked high priority.

clear radius-server statistics

To clear radius server statistics, use the clear radius-server statistics command.

clear radius-server statistics name

Syntax Description

name	Specifies the RADIUS name or IP address.

Command Default

None

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None

Examples

The following example shows how to clear the statistics sent or received from the specified server:

```
switch(config)# clear radius-server statistics 10.64.65.57
switch(config)#
```

Related Commands

Command	Description
tacacs+ enable	Enables TACACS+.

clear radius session

To clear RADIUS Cisco Fabric Services (CFS) session configuration and locks, use the **clear radius session** command.

clear radius session

Syntax Description

This command has no other arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to clear RADIUS session:

```
switch# clear radius session
```

Related Commands

Command	Description
show radius	Displays RADIUS CFS distribution status and other details.

clear rlir

To clear the Registered Link Incident Report (RLIR), use the **clear rlir** command in EXEC mode.

clear rlir {**history**|**recent** {**interface fc** *slot-port*|**portnumber** *port-number*}|**statistics 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

history	Clears RLIR link incident history.
recent	Clears recent link incidents.
interface fc slot/port	Clears entries for a specified interface.
bay *port* | **ext** *port*	Clears entries for a specified interface on a Cisco Fabric Switch for HP c-Class BladeSystem and on a Cisco Fabric Switch for IBM BladeCenter.
portnumber *port-number*	Displays the port number for the link incidents.
statistics	Clears RLIR statistics.
vsan *vsan-id*	Specifies the VSAN ID for which the RLIR statistics are to be cleared.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.3(1)	This command was introduced.
3.1(2)	Added the **interface bay** | **ext** option.

Usage Guidelines

None.

Examples

The following example clears all existing statistics for a specified VSAN:

```
switch# clear rlir statistics vsan 1
```

The following example clears the link incident history:

```
switch# clear rlir history
```

The following example clears recent RLIR information for a specified interface:

```
switch# clear rlir recent interface fc 1/2
```

The following example clears recent RLIR information for a specified port number:

```
switch# clear rlir recent portnumber 16
```

Related Commands

Command	Description
show rscn	Displays RSCN information.

clear rmon alarms

To clear all the 32-bit remote monitoring (RMON) alarms from the running configuration, use the clear **rmon alarms** command**.**

clear rmon alarms

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

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

Usage Guidelines

You must save the changes to startup configuration to make them permanent.

Examples

The following example clears all 32-bit RMON alarms from the running configuration:

```
switch# clear rmon alarms
switch#
```

Related Commands

Command	Description
clear rmon all-alarms	Clears all the 32-bit and 64-bit RMON alarms.
clear rmon hcalarms	Clears all the 64-bit RMON alarms.
clear rmon log	Clears RMON log information.

clear rmon all-alarms

To clear all the 32-bit and 64-bit RMON alarms from the running configuration, use the clear **rmon all-alarms** command**.**

clear rmon all-alarms

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

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

Usage Guidelines

You must save the changes to startup configuration to make them permanent.

Examples

The following example clears all the 32-bit and 64-bit RMON alarms from the running configuration:

```
switch# clear rmon all-alarms
switch#
```

Related Commands

Command	Description
clear rmon alarms	Clears all the 32-bit RMON alarms.
clear rmon hcalarms	Clears all the 64-bit RMON alarms.
clear rmon log	Clears RMON log information.

clear rmon hcalarms

To clear all the 64-bit RMON alarms from the running configuration, use the clear **rmon hcalarms** command.

clear rmon hcalarms

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

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

Usage Guidelines

You must save the changes to startup configuration to make them permanent.

Examples

The following example clears all the 64-bit RMON alarms from the running configuration:

```
switch# clear rmon hcalarms
switch#
```

Related Commands

Command	Description
clear rmon all-alarms	Clears all the 32-bit and 64-bit RMON alarms.
clear rmon alarms	Clears all the 32-bit RMON alarms.
clear rmon log	Clears RMON log information.

clear rmon log

To clear all entries from RMON log on the switch, use the clear **rmon log** command**.**

clear rmon log

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

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

Usage Guidelines

None

Examples

The following example clears all entries from RMON log on the switch:

```
switch# clear rmon log
switch#
```

Related Commands

Command	Description
clear rmon alarm	Clears all the 32-bit RMON alarms.
clear rmon hcalarms	Clears all the 64-bit RMON alarms.
clear rmon all-alarms	Clears all the 32-bit and 64-bit RMON alarms.

clear role session

To clear authentication role Cisco Fabric Services (CFS) session configuration and locks, use the **clear role session** command.

clear role session

Syntax Description

This command has no other arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to clear authentication role CFS session:

```
switch# clear role session
```

Related Commands

Command	Description
show role	Displays role configuration information.

clear rscn session vsan

To clear a Registered State Change Notification (RSCN) session for a specified VSAN, use the **clear rscn session vsan** command.

clear rscn session vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN where the RSCN session should be cleared. The ID of the VSAN is from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None

Examples

The following example clears an RSCN session on VSAN 1:

```
switch# clear rscn session vsan 1
```

Related Commands

Command	Description
rscn	Configures an RSCN.
show rscn	Displays RSCN information.

clear rscn statistics

To clear the registered state change notification RSCN statistics for a specified VSAN, use the **clear rscn statistics** command in EXEC mode.

clear rscn statistics vsan vsan-*id*

Syntax Description

vsan	The RSCN statistics are to be cleared for a VSAN.
vsan-id	The ID for the VSAN for which you want to clear RSCN statistics.

Command Default

None

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 clear RSCN statistics for VSAN 1:

```
switch# clear rscn statistics 1
```

Related Commands

Command	Description
show rscn	Displays RSCN information.

clear santap module

To clear SANTap information, use the **clear santap module** command.

clear santap module slot-number {**avt avt-pwwn** [**lun avt-lun**]|**itl target-pwwn host-pwwn**|**session session-id**}

Syntax Description

slot-number	Specifies the Storage Services Module (SSM) module number. The range is 1 through 13.
avt *avt-pwwn*	Removes the appliance virtual target (AVT) pWWN. The format is *hh:hh:hh:hh:hh:hh:hh:hh* .
lun *avt-lun*	(Optional) Removes the appliance virtual target (AVT) LUN. The format is *0xhhhh* [*:hhhh* [*:hhhh* [*:hhhh*]]].
itl *target-pwwn host-pwwn*	Removes the SANTap Initiator Target LUN (ITL) triplet. The format of the *target-pwwn* and the *host-pwwn* is *hh:hh:hh:hh:hh:hh:hh:hh* .
session *session-id*	Removes a session. The range for session ID is 0 through 2147483647.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to remove a SANTap session:

```
switch# clear santap module 13 session 2020
```

Related Commands

Command	Description
santap module	Configures the mapping between the Storage Services Module (SSM) and the VSAN where the appliance is configured.
show santap module	Displays the configuration and statistics of the SANTap feature.

clear scheduler logfile

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

clear scheduler logfile

Syntax Description

This command has no other arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to clear the command scheduler logfile:

```
switch# clear scheduler logfile
```

Related Commands

Command	Description
show scheduler	Displays command scheduler information.

clear screen

To clear the terminal screen, use the **clear screen** command in EXEC mode.

clear screen

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to clear the terminal screen:

```
switch# clear screen
```

clear scsi-flow statistics

To clear the SCSI flow statistics counters, use the **clear scsi-flow statistics** command.

clear scsi-flow statistics flow-id *flow-id*

Syntax Description

flow-id *flow-id*	Configures the SCSI flow identification number.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
2.0(2)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to clear the SCSI flow statistics counters for SCSI flow ID 3:

```
switch# clear sc
screen     scsi-flow
switch# clear scsi-flow ?
  statistics  Clear statistics counters
switch# clear scsi-flow statistics ?
  flow-id  Clear statistics for particular flow
switch# clear scsi-flow statistics flow-id ?
  <1-65535>  Enter the index of the SCSI flow
switch# clear scsi-flow statistics flow-id 3 ?
  <cr>  Carriage Return
switch# clear scsi-flow statistics flow-id 3
```

Related Commands

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

clear sdv

To clear specified SAN device virtualization parameters, use the **clear sdv** command in EXEC mode.

clear sdv {**database vsan vsan-id**|**session vsan vsan-id**|**statistics vsan vsan-id**}

Syntax Description

database	Clears the SDV database.
vsan *vsan-id*	Specifies the number of the VSAN. The range is 1 to 4093.
session	Clears the SDV session.
statistics	Clears the SDV statistics.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.1(2)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to clear SDV statistics:

```
switch# clear sdv statistics vsan 2
```

Related Commands

Command	Description
sdv enable	Enables or disables SAN device virtualization.
show sdv statistics	Displays SAN device virtualization statistics.

clear snmp hostconfig

To clear all SNMP hosts from the running configuration, use the clear **snmp hostconfig** command**.**

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

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

Usage Guidelines

You must save the changes to startup configuration to make them permanent:

Examples

The following example clears the SNMP host list.

```
switch# clear snmp hostconfig
switch#
```

Related Commands

Command	Description
show snmp host	Displays the SNMP status and setting information.

clear ssh hosts

To clear trusted SSH hosts, use the **clear ssh hosts** command in EXEC mode.

clear ssh hosts

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to clear reset-reason information from NVRAM and volatile storage:

```
switch# clear ssh hosts
```

Related Commands

Command	Description
show ssh hosts	Displays SSH host information.

clear ssm-nvram santap module

To clear the SANTap configuration for a specific slot stored on the supervisor flash, use the clear ssm-nvram santap module command in the configuration mode.

clear ssm-nvram santap module slot

Syntax Description

slot	Displays SANTap configuration for a module in the specified slot.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to clear the SANTap configuration for a slot 2:

```
switch# clear ssm-nvram santap module 2
```

Related Commands

Command	Description
ssm enable feature	Enables the SANTap feature on the SSM.

clear system reset-reason

To clear the reset-reason information stored in NVRAM and volatile persistent storage, use the **clear system reset-reason** command in EXEC mode.

clear system reset-reason

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.3(2a)	This command was introduced.

Usage Guidelines

Use this command as follows for these switches:

- In a Cisco MDS 9500 Series switch, this command clears the reset-reason information stored in NVRAM and volatile persistent storage in the active and standby supervisor modules.
- In a Cisco MDS 9200 Series switch, this command clears the reset-reason information stored in NVRAM and volatile persistent storage in the active supervisor module.

Examples

The following example shows how to clear trusted SSH hosts:

```
switch# clear system reset-reason
```

Related Commands

Command	Description
show system reset-reason	Displays system reset-reason information.

clear tacacs+ session

To clear TACACS+ Cisco Fabric Services (CFS) session configuration and locks, use the **clear tacacs+ session** command.

clear tacacs+ session

Syntax Description

This command has no other arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, TACACS+ must be enabled using the **tacacs+ enable** command.

Examples

The following example shows how to clear the TACACS+ session:

```
switch# clear tacacs+ session
```

Related Commands

Command	Description
show tacacs+	Displays TACACS+ CFS distribution status and other details.
tacacs+ enable	Enables TACACS+.

clear tacacs-server statistics

To clear TACACS server statistics, use the clear tacacs-server statistics command.

clear tacacs-server statistics name

Syntax Description

name	Specifies the TACACS name or IP address.

Command Default

None

Command Modes

EXEC mode

Command History

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

Usage Guidelines

None

Examples

The following example shows how to clear the tacacs server statistics:

```
switch(config)# clear tacacs-server statistics 10.64.65.57
switch(config)#
```

Related Commands

Command	Description
tacacs+ enable	Enables TACACS+.

clear tlport alpa-cache

To clear the entire contents of the alpa-cache, use the **clear tlport alpa-cache** command in EXEC mode.

clear tlport alpa-cache

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
NX-OS 5.0 and later releases	This command was deprecated.
1.3(5)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to clear a TL port ALPA cache:

```
switch# clear tlport alpa-cache
```

Related Commands

Command	Description
show tlport alpa-cache	Displays TL port alpa-cache information.

clear user

To clear trusted SSH hosts, use the **clear user** command in EXEC mode.

clear user *username*

Syntax Description

username	Specifies the user name to clear.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to log out a specified user:

```
switch# clear user vsam
```

Related Commands

Command	Description
show users	Displays user information.

clear vrrp

To clear all the software counters for the specified virtual router, use the **clear vrrp** command in EXEC mode.

clear vrrp statistics [{**ipv4**|**ipv6**}] **vr** *number* **interface** {**gigabitethernet** *slot/port*|**mgmt 0**|**port-channel** *portchannel-id*|**vsan** *vsan-id*}

Syntax Description

statistics	Clears global VRRP statistics.
ipv4	(Optional) Clears IPv4 virtual router statistics.
ipv6	(Optional) Clears IPv6 virtual router statistics.
vr *number*	Clears specific virtual router statistics and specifies a VR number from 1 to 255.
interface	Clears an interface.
gigabitethernet *slot/port*	**Clears a specified Gigabit Ethernet interface**.
mgmt 0	Specifies the management interface.
port-channel *port-channel-id*	**Clears a specified** PortChannel interface.The ID of the PortChannel interface is from 1 to 128.
vsan *vsan-id*	**Clears a specified** VSAN. The ID of the VSAN is from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **ipv4** and **ipv6** arguments.

Usage Guidelines

None

Examples

The following example shows how to clear all the software counters for virtual router 7 on VSAN 2:

```
switch# clear vrrp vr 7 interface vsan2
```

Related Commands

Command	Description
show vrrp	Displays VRRP configuration information.

Command	Description
vrrp	Enables VRRP.

clear zone

To clear all configured information in the zone server for a specified VSAN, use the **clear zone** command in EXEC mode.

clear zone {**database**|**lock**|**statistics** {**lun-zoning**|**read-only-zoning**}} **vsan** *vsan-id*

Syntax Description

database	Clears zone server database information.
lock	Clears a zone server database lock.
statistics	Clears zone server statistics.
lun-zoning	Clears LUN-zoning related statistics.
read-only-zoning	Clears read-only zoning related statistics.
vsan	Clears zone information for a VSAN.
vsan-id	The ID of the VSAN is from 1 to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **lock** option.

Usage Guidelines

After issuing a **clear zone database** command, you need to explicitly issue the **copy running-config startup-config** to ensure that the running configuration is used when you next start the switch.

When you issue the **clear zone lock** command from a remote switch, only the lock on that remote switch is cleared. When you issue the **clear zone lock** command from the switch where the lock originated, all locks in the VSAN are cleared.

Note The recommended method to clear a session lock on a switch where the lock originated is by issuing the **no zone commit vsan** command.

Examples

The following example shows how to clear all configured information in the zone server for VSAN 1:

```
switch# clear zone database vsan 1
```

Related Commands

Command	Description
show zone	Displays zone information for any configured interface.

clear zone smart-zoning

To clear the smart zoning configuration, use the **clear zone smart-zoning** command.

Syntax Description

fcalias name	Specifies auto-convert commands for an fcalias.
fcalias-name	Specifies the fcalias name. The maximum size is 64 characters.
vsan	Specifies the auto convert commands for a VSAN.
vsan-id	Specifies the VSAN ID. The range is from 1 to 4093.
zone name	Specifies the auto convert commands for a given zone.
zone-name	Specifies the zone name. The maximum size is 64 characters.
zoneset name	Specifies the auto convert commands for a zoneset.
zoneset-name	Specifies the zoneset name. The maximum size is 64 characters.
vsan	Specifies the VSAN.
vsan-id	Specifies the VSAN ID. The range is from 1to 4093.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
5.2(6)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to clear the smart zoing command for a VSAN:

```
switch(config)# clear zone smart-zoning vsan 1
WARNING: This command will clear smart zoning configs from the specified zone/zo
neset/fcalias/vsan. Do you want to continue? (y/n) [n] y
switch(config)#
```

Related Commands

Command	Description
show zone	Displays zone information for any configured interface.

cli

To execute Cisco NX-OS commands verbosely in Tcl, use the **cli** command.

cli *arguments*

Syntax Description

arguments	*arguments* takes the form of a single NX-OS command line to execute in a subprocess. This may include pipes and semicolon separated commands. Normal abbreviations of NX-OS keywords are allowed. Enclosing *arguments* in quotes ("") is optional, but good style that adds clarity to code. The specified NX-OS command line must not cause any prompts for input from the user.

Command Default

None.

Command Modes

Interactive Tcl shell and Tcl script.

Command History

Release	Modification
NX-OS 5.1(1)	This command was introduced.

Usage Guidelines

The **cli** command prints the output of the specified command to the terminal and returns the output as a single string to Tcl. This would be the preferred behavior when using the interactive Tcl shell as it allows the user to verify the output of the executed NX-OS commands.

In a Tcl script, the **cli** or **clis** command is required to execute NX-OS commands.

In the Tcl shell interactive mode, the **cli** and **clis** commands are optional to execute NX-OS commands; commands that are not recognized by the Tcl shell are passed to the NX-OS shell for execution.

Examples

The following example enables the locator LED for module 1 in an interactive Tcl shell:

```
switch# tclsh
switch-tcl# cli "locator-led module 1"
switch-tcl#
```

The following example shows how to quote a variable and use the pipe in an interactive Tcl shell. It creates a list of Supervisor-3 modules in the system and assigns it to the variable *sups*. *string trimright* removes the trailing blank line from the variable added by Tcl, but not from the terminal output:

```
switch-tcl# set type "Supervisor Module-3"
Supervisor Module-3
switch-tcl# set sups [split [string trimright [cli "show module | include \"$type\""]] '\n']

5 0 Supervisor Module-3 DS-X97-SF1-K9 active *
6 0 Supervisor Module-3 DS-X97-SF1-K9 ha-standby

switch-tcl#
```

Related Commands

Command	Description
clis	Execute an NX-OS CLI command silently from Tcl.
open	Open a file or command pipeline and return a channel identifier.

cli alias name

To define a command alias name, use the **cli alias name** command in configuration submode. To remove the user-defined command alias, use the **no** form of the command.

cli alias name command definition
no cli alias name command definition

Syntax Description

command	Specifies an alias command name. The maximum size is 30 characters.
definition	Specifies the alias command definition. The maximum size is 80 characters.

Command Default

alias command.

Command Modes

Configuration submode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

When defining a command alias follow these guidelines:

- Command aliases are global for all user sessions.
- Command aliases persist across reboots.
- Commands being aliased must be typed in full without abbreviation.
- Command alias translation always takes precedence over any keyword in any configuration mode or submode.
- Command alias support is only available on the supervisor module, not the switching modules.
- Command alias configuration takes effect for other user sessions immediately.
- You cannot override the default command alias alias, which is an alias for show cli alias.
- Nesting of command aliases is permitted to a maximum depth of 1. One command alias can refer to another command alias that refers to a valid command, not to another command alias.
- A command alias always replaces the first command keyword on the command line.
- You can define command aliases in either EXEC mode or configuration submode.

Examples

The following example shows how to define command aliases in configuration submode:

```
switch# config
 t
switch(config)# cli alias name gigint interface gigabitethernet
switch(config)# cli alias name shintbr show interface brief
switch(config)# cli alias name shfcintup shintbr| include up | include fc
```

You can display the command aliases defined on the switch using the alias default command alias.

The following example shows how to display the command aliases defined on the switch:

```
switch(config)# alias
```

```
CLI alias commands
==================
alias       :show cli alias
shfcintup   :shintbr | include up | include fc
switch(config)# shfcintup
fc3/1      18     F      on      up              swl    F       4     --
fc3/3      1      SD     --      up              swl    SD      2     --
fc6/1      22     E      auto    up              swl    E       2     --
```

Related Commands

Command	Description
alias	Displays the default alias command for **show cli alias**.
show cli alias	Displays all configured aliases.

cli var name (configuration)

To define a CLI variable that persists across CLI sessions and switch reloads, use the **cli var name** command in configuration submode. To remove the user-defined persistent CLI variable, use the **no** form of the command.

cli var name *name value*
no cli var name *name value*

Syntax Description

name	Specifies a variable name. The maximum size is 31 characters.
value	Specifies a variable value. The maximum size is 80.

Command Default

None

Command Modes

Configuration submode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

CLI variables can be used as follows:

- Entered directly on the command line.
- Passed to the child script and initiated using the run-script command. The variables defined in the parent shell are available for use in the child run-script command process.
- Passed as command-line arguments to the run-script command.
- Referenced using the syntax $(variable).

CLI variables have the following limitations:

- You cannot reference a variable through another variable using nested references.

Examples

The following example creates a persistent user-defined CLI variable:

```
switch# config t
switch(config)# cli var name mgmtport mgmt 0
```

Related Commands

Command	Description
show cli variables	Displays all CLI variables (persistent, session and system).

cli var name (EXEC)

To define a CLI session variable that persists only for the duration of a CLI session, use the **cli var name** command in either EXEC mode or configuration submode. To remove a user-defined session CLI variable, use the **no** form of the command.

cli var name name value
no cli var name name value

Syntax Description

name	Specifies a variable name. The maximum size is 31 characters.
value	Specifies a variable value. The maximum size is 80.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

CLI session variables can be used as follows:

- Entered directly on the command line.
- Passed to the child script and initiated using the run-script command. The variables defined in the parent shell are available for use in the child run-script command process.
- Passed as command-line arguments to the run-script command.
- Referenced using the syntax $(variable).

CLI variables have the following limitation:

- You cannot reference a variable through another variable using nested references.

Examples

The following example creates a user-defined CLI variable for a session:

```
switch# cli var name testinterface 3/4
```

The following example removes a user-defined CLI variable for a session:

```
switch# cli no var name testinterface 3/4
```

Related Commands

Command	Description
cli no var name	Removes a user-defined session CLI variable.
show cli variables	Displays all CLI variables (persistent, session and system).

clis

To execute Cisco NX-OS commands silently in Tcl, use the **clis** command.

clis *arguments*

Syntax Description

arguments	*arguments* takes the form of a single NX-OS command line to execute in a subprocess. This may include pipes and semicolon separated commands. Normal abbreviations of NX-OS keywords are allowed. Enclosing *arguments* in quotes ("") is optional, but good style that adds clarity to code. The specified NX-OS command line must not cause any prompts for input from the user.

Command Default

None.

Command Modes

Interactive Tcl shell and Tcl script.

Command History

Release	Modification
NX-OS 5.1(1)	This command was introduced.

Usage Guidelines

The **clis** returns the output as a single string. It does not print any output to the terminal. This is usually the desired behavior when running Tcl scripts. This prevents the terminal from getting flooded with the outputs of the executed NX-OS commands.

In a Tcl script, the **cli** or **clis** command is required to execute NX-OS commands.

In the Tcl shell interactive mode, the **cli** and **clis** commands are optional to execute NX-OS commands; commands that are not recognized by the Tcl shell are passed to the NX-OS shell for execution.

Examples

The following example shows enables the locator LED for module 1 in a Tcl script:

```
clis "locator-led module 1"
```

The following example shows how to quote a variable and use the pipe in an interactive Tcl shell. It creates a list of Supervisor-3 modules in the system and assigns it to the variable *sups*. *string trimright* removes the trailing blank line from the variable added by Tcl, but not from the terminal output:

```
switch-tcl# set type "Supervisor Module-3"
Supervisor Module-3
switch-tcl# set sups [split [string trimright [cli "show module | include \"$type\""]] '\n']

switch-tcl#
```

Related Commands

Command	Description
cli	Execute an NX-OS CLI command in Tcl verbosely.
open	Open a file or command pipeline and return a channel identifier.

clock

To configure the time zone or daylight savings time, use the clock command in configuration mode. To disable the daylight saving time adjustment, use the no form of the command.

clock {**summer-time** *summer-time-name start-week start-day start-month start-time end-week end-day end-month end-time offset-minutes*|**timezone** *timezone-name hours-offset minute-offset*}
no clock {**summer-time** *summer-time-name start-week start-day start-month start-time end-week end-day end-month end-time offset-minutes*|**timezone** *timezone-name hours-offset minute-offset*}

Syntax Description

summer-time	Specifies the name of the time zone in summer.
summer-time-name	Specifies the name of the daylight savings time zone, ranging from 1 to 8 characters.
start-week end-week	Specifies the starting week and ending week, ranging from 1 (week 1) to 5 (week 5).
start-dayend-day	Specifies the starting day and ending day, ranging from 1 to 8 characters (Sunday to Saturday).
start-monthend-month	Specifies the starting month and ending month, ranging from 1 to 8 characters (January to December).
start-timeend-time	Specifies the starting time and ending time, ranging from 00:00 to 23:59.
offset-minutes	Specifies the daylight savings time offset, ranging from 1 to 1440 minutes.
timezone	Specifies the name of the time zone.
timezone-name	Specifies the name of the time zone, ranging from 1 to 8 characters.
hours-offset	Specifies the offset time in hours, ranging from 0 to 23. Include a dash before the number; for example, -23.
minutes-offset	Specifies the offset time in minutes, ranging from 0 to 59. Include a dash before the number; for example, -59.

Command Default

Coordinated Universal Time (UTC) is the same as Greenwich Mean Time (GMT).

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.1(1)	Added a new set of arguments for **timezone**.

Usage Guidelines

The appropriate daylight savings time zone name should be specified. If it is not, the default name is used.

Specify the *hours-offset argument* with a dash before the number; for example, **-23** . Specify the *minutes-offset* argument with a dash before the number; for example, **-59**.

Examples

The following example shows how to set Pacific Daylight Time starting on Sunday in the second week of March at 2:00 A.M. and ending on Sunday in the first week of November at 2:00 A.M:

```
switch# configure terminal
switch# clock summer-time PDT 2 sunday march 02:00 1 sunday november 02:00 60
```

The following example shows how to set the time zone to Pacific Standard Time:

```
switch# configure terminal
switch(config)# clock timezone PST 0 0
```

Related Commands

Command	Description
clock set	Changes the time on the switch.
show clock	Displays the current date and time.
show run	Displays changes made to the time zone configuration along with other configuration information.

clock set

To change the system time on a Cisco MDS 9000 Family switch, use the **clock set** command in EXEC mode.

clock set H *H* **:** *MM*:*SS DD Month YYYY*

Syntax Description

HH:	The two-digit time in hours in military format (15 for 3 p.m.).
MM:	The two-digit time in minutes (58).
SS	The two-digit time in seconds (15).
DD	The two-digit date (12).
Month	The month in words (August).
YYYY	The four-digit year (2002).

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Generally, if the system is synchronized by a valid outside timing mechanism, such as an NTP clock source, or if you have a switch with calendar capability, you do not need to set the system clock. Use this command if no other time sources are available. The time specified in this command is relative to the configured time zone.

The **clock set** command changes are saved across system resets.

Examples

The following example shows how to set the system time:

```
switch# clock set 15:58:15 12 August 2002
Mon Aug 12 15:58:00 PDT 2002
```

cloud discover

To initiate manual, on-demand cloud discovery, use the **cloud discover** command.

cloud discovery {**auto**|**fabric distribute**|**message icmp**} **no cloud discovery** {**auto**|**fabric distribute**|**message icmp**}

Syntax Description

interface	(Optional) Specifies an interface for cloud discovery.
gigabitethernet *slot/port*	(Optional) Specifies a Gigabit Ethernet interface.
port-channel *port-channel-number*	(Optional) Specifies a PortChannel interface. The range for the PortChannel number is 1 to 256.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.0(1)	This command was introduced.
3.2(2c)	This command was deprecated.

Usage Guidelines

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 initiates manual, on-demand cloud discovery:

```
switch# cloud discover
```

The following example initiates manual, on-demand cloud discovery on Gigabit Ethernet interface 2/2:

```
switch# cloud discover interface gigabitethernet 2/2
```

Related Commands

Command	Description
cloud discovery	Configures cloud discovery.
cloud-discovery enable	Enables discovery of cloud memberships.
show cloud discovery	Displays discovery information about the cloud.
show cloud membership	Displays information about members of the cloud.

cloud discovery

To configure cloud discovery, use the **cloud discovery** command in configuration mode. To remove the configuration, use the **no** form of the command.

cloud discovery {**auto**|**fabric distribute**|**message icmp**}
no cloud discovery {**auto**|**fabric distribute**|**message icmp**}

Syntax Description

auto	Enables auto fabric discovery.
fabric distribute	Enables cloud discovery fabric distribution.
message icmp	Configures Internet Control Message Protocol (ICMP) as the method for sending a discovery message.

Command Default

Auto.

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.
3.2(2c)	This command was deprecated.

Usage Guidelines

The iSNS server distributes cloud and membership information across all of the switches using CFS. The cloud view is the same on all of the switches in the fabric.

Note If auto discovery is disabled, interface changes result in new members becoming part of an undiscovered cloud. No new clouds are formed.

Note This command is not supported on the Cisco MDS 9124 switch.

Examples

The following example enables auto cloud discovery:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# cloud disovery auto
```

The following example enables auto cloud discovery fabric distribution:

```
switch(config)# cloud disovery fabric distribute
```

The following example disables auto cloud discovery fabric distribution:

```
switch(config)# no
 cloud disovery fabric distribute
```

Related Commands

Command	Description
cloud discover	Initiates manual, on-demand cloud discovery.
cloud-discovery enable	Enables discovery of cloud memberships.
show cloud discovery	Displays cloud discovery information.
show cloud membership	Displays information about members of the cloud.

cloud-discovery enable

To enable discovery of cloud memberships, use the **cloud-discovery** command in configuration mode. To disable discovery of cloud memberships, use the **no** form of the command.

cloud-discovery enable
no cloud-discovery enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.
3.2(2c)	This command was deprecated.

Usage Guidelines

This command is not supported on the Cisco MDS 9124 switch.

Examples

The following example enables discovery of cloud memberships:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# cloud-discovery enable
```

The following example disables discovery of cloud memberships:

```
switch(config)# no
 cloud-discovery enable
```

Related Commands

Command	Description
cloud discover	Initiates manual, on-demand cloud discovery.
cloud discovery	Configures cloud discovery.
show cloud	Displays cloud discovery and membership information.

cluster

To configure a cluster feature, use the cluster command.

cluster enable

Syntax Description

enable	Enables or disables a cluster.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
3.2(2)	This command was introduced.
NX-OS 4.1(1c)	The cluster command is replaced by the feature command.

Usage Guidelines

Starting from Cisco NX-OS 4.x Release, the cluster command is replaced by the feature command.

Examples

The following example enables the Cisco SME clustering:

```
switch# config terminal
switch(config)# cluster enable
switch(config)#
```

code-page

Use the **code-page** command to configure the EBCDIC format. To disable the configuration or to revert to factory defaults, use the **no** form of the command.

{**code-page brazil**|**france**|**international-5**|**italy**|**japan**|**spain-latinamerica**|**uk**|**us-canada**}
{**no code-page brazil**|**france**|**international-5**|**italy**|**japan**|**spain-latinamerica**|**uk**|**us-canada**}

Syntax Description

code-page	Configures code page on a FICON-enabled VSAN
brazil	Configures the brazil EBCDIC format.
france	Configures the france EBCDIC format.
international-5	Configures the international-5 EBCDIC format.
italy	Configures the **italy** EBCDIC format.
japan	Configures the japan EBCDIC format.
spain-latinamerica	Configures the spain-latinamerica EBCDIC format.
uk	Configures the uk EBCDIC format.
us-canada	Configures the us-canada EBCDIC format.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

This is an optional configuration. If you are not sure of the EBCDIC format to be used, we recommend retaining the **us-canada** (default) option.

Examples

The following example configures the **italy** EBCDIC format:

```
switch(config)# ficon vsan 2
switch(config-ficon)# code-page italy
```

The following example reverts to the factory default of using the **us-canada** EBCDIC format:

```
switch(config-ficon)# no code-page
```

Related Commands

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

commit

To apply the pending configuration pertaining to the Call Home configuration session in progress, use the **commit** command in Call Home configuration submode.

commit

Syntax Description

This command has no other arguments or keywords.

Command Default

None

Command Modes

Call Home configuration submode

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(1b)	This command was introduced.

Usage Guidelines

CFS distribution must be enabled before you can commit the Call Home configuration.

Examples

The following example shows how to commit the Call Home configuration commands:

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

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.

commit (DMM job configuration submode)

To commit a DMM job, use the **commit** command in DMM job configuration submode. To remove the DMM job, use the **no** form of the command.

commit
no commit

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

DMM job configuration submode

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

You need to configure server HBA ports, storage ports, and job attributes before you commit the job.

Examples

The following example shows how to commit a data migration job:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# dmm module 3 job 1 destroy
switch(config-dmm-job)#
```

Related Commands

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

configure terminal

To enter the configuration mode, use the **configure terminal** command in EXEC mode.

configure terminal

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None

Examples

The following example enters the configuration mode:

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

The following example enters the configuration mode using an abbreviated format of the command:

```
switch# config terminal
switch(config)#
```

contract-id

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

contract-id *customer-id*
no contract-id *customer-id*

Syntax Description

customer-id	Configures the service contract ID of the customer. Allows up to 64 characters for the contract number.

Command Default

None

Command Modes

Call Home configuration submode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the contract 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)# contract-id Customer1234
```

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.

copy

To save a backup of the system software, use the **copy** command in EXEC mode.

copy source-URL destination-URL

Syntax Description

source-URL	The location URL or alias of the source file or directory to be copied.
destination-URL	The destination URL or alias of the copied file or directory.

The following table lists the aliases for source and destination URLs.

running-config	Specifies the configuration currently running on the switch. The **system:running-config** keyword represents the current running configuration file.
startup-config	Specifies the configuration used during initialization (startup). You can copy the startup configuration from NVRAM. The **nvram:startup-config** keyword represents the configuration file used during initialization.
bootflash:	Specifies the location for internal bootflash memory.
log:	Specifies the location for the log file system.
slot0:	Specifies the location for the CompactFlash memory or PCMCIA card.
volatile:	Specifies the location for the volatile file system.
system:	Specifies the location for system memory, which includes the running configuration.
fabric	Specifies a fabric wide startup configuration update using Cisco Fabric Services (CFS) where all the remote switches in the fabric copy their running configuration (source) file into their startup configuration (destination) file. The syntax for this command is **copy running-config startup-config fabric.**
tftp:	Specifies the location for a Trivial File Transfer Protocol (TFTP) network server. The syntax for this alias is tftp: [[*//location*]*/directory*]*/filename* .
ftp:	Specifies the location for a File Transfer Protocol (FTP) network server. The syntax for this alias is ftp: [[*//location*]*/directory*]*/filename* .
scp:	Specifies the location for a secure copy (scp) network server. The syntax for this alias is scp: [[*//location*]*/directory*]*/filename* .
sftp:	Specifies the location for a Secure Trivial File Transfer Protocol (SFTP) network server. The syntax for this alias is sftp: [[*//location*]*/directory*]*/filename* .
log:	Specifies the location for log files stored in the same directory.
debug:	Specifies the location for the debug files stored in the debug partition.
nvram:	Specifies the switch NVRAM.

core:	Specifies the location of the cores from any switching or supervisor module to an external flash (slot 0) or a TFTP server.
filename	The name of the flash file.
*sup-1***sup-2**	The number of the supervisor module, where sup-1 is the slot 5 supervisor (active) and sup-2 is the slot 6 supervisor (standby).

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.2(1)	Added a note.
1.3(4)	Command modified.
2.1(1a)	Added the **fabric** keyword and functionality.

Usage Guidelines

This command makes the running and the backup copy of the software identical.

A file can only be copied from an active supervisor to a standby supervisor, not from standby to active.

This command does not allow 127.x.x.x IP addresses.

The copy function will not be completed if the required space is not available in the directory. First change to the required directory (for example, **cd bootflash:**) and verify the available space (for example, **dir bootflash:**).

The entire copying process may take several minutes.

Do not copy a file from an external source directly to the standby supervisor. You must copy from the external source to the active supervisor, and then copy the saved file to the standby supervisor.

You can save cores (from the active supervisor module, the standby supervisor module, or any switching module) to an external flash (slot 0) or to a TFTP server in one of two ways:

- On demand—to copy a single file based on the provided process ID.
- Periodically—to copy core files periodically as configured by the user.

You copy the logfile to a different location using the **copy log:messages** command.

The debug partition contains debugging files created by the software for troubleshooting purposes.

The **running-config startup-config fabric** parameters allow you to use CFS to force every switch in the Fibre Channel fabric to copy their running configuration (source) to their startup configuration (destination).

Note If any remote switch fails to complete the **copy running-config startup-config fabric** process, the initiator switch also does not complete saving its startup-configuration. This means that both the remote switch and the initiator switch have failed to save their startup-configuration (the old startup-configuration reverts back). All the other switches in the network would have succeeded.

Examples

The following example saves your configuration to the startup configuration:

```
switch# copy system:running-config nvram:startup-config
```

The following example copies the file called samplefile from the slot0 directory to the mystorage directory:

```
switch# copy slot0:samplefile slot0:mystorage/samplefile
```

The following example copies a file from the current directory level:

```
switch# copy samplefile mystorage/samplefile
```

If the current directory is slot0:mydir, this command copies slot0:mydir/samplefile to slot0:mydir/mystorage/samplefile.

The following example downloads a configuration file from an external CompactFlash to the running configuration:

```
switch copy slot0:dns-config.cfg system:running-config
```

The following example saves a running configuration file to an external CompactFlash:

```
switch# copy system:running-config slot0:dns-config.cfg
```

The following example saves a startup configuration file to an external CompactFlash:

```
switch# copy system:startup-config slot0:dns-config.cfg
```

The following example uses CFS to cause all switches in the fabric to copy their running configuration (source) file to their startup configuration (destination) file:

```
switch# copy running-config startup-config fabric
[########################################] 100%
switch#
```

Note If any remote switch fails to complete the **copy running-config startup-config fabric** process, the initiator switch also does not complete saving its startup-configuration. This means both the remote switch and the initiator switch have failed to save their startup-configuration (the old startup-configuration reverts back). All the other switches in the network would have succeeded.

Note When you copy a file to an ftp server from a Cisco Fabric Switch for IBM BladeCenter, you must enter the full path. For example: switch# copy running-config ftp://172.25.161.201/mnt/hd2/bch6-inagua-bay3_cfg1.txt, If you do not enter the full path, the command will not succeed.

The following example creates a backup copy of the binary configuration:

```
switch# copy nvram:startup-config nvram:snapshot-config
```

The following example copies an image in bootflash on the active supervisor to the bootflash on the standby supervisor:

```
switch# copy bootflash:myimage bootflash://sup-2/myimage
```

The following example creates a running configuration copy in bootflash:

```
switch# copy system:running-config bootflash:my-config
```

The following examples creates a startup configuration copy in bootflash:

```
switch# copy nvram:startup-config bootflash:my-config
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
dir	Displays a list of files on a file system.
reload	Reloads the operating system.
show version	Displays the version of the running configuration file.

copy licenses

To save a backup of the installed license files, use the **copy licenses** command in EXEC mode.

copy licenses source-URL destination-URL

Syntax Description

source-URL	The location URL or alias of the source file or directory to be copied.
destination-URL	The destination URL or alias of the copied file or directory.

The following table lists the aliases for source and destination URLs.

bootflash:	Specifies the location for internal bootflash memory.
slot0:	Specifies the location for the CompactFlash memory or PCMCIA card.
volatile:	Specifies the location for the volatile file system.
filename	Specifies the name of the license file with a.tar extension.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

The copy function will not be completed if the required space is not available in the directory. First change to the required directory (for example, **cd bootflash:**) and verify the available space (for example, **dir bootflash:**).

We recommend backing up your license files immediately after installing them and just before issuing a **write erase** command.

Examples

The following example saves a file called Enterprise.tar to the bootflash: directory:

```
switch# copy licenses bootflash:/Enterprise.tar
Backing up license done
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
dir	Displays a list of files on a file system.
install license	Installs a license file.

copy ssm-nvram standby-sup

To copy the contents of the Storage Services Module (SSM) NVRAM to the standby Supervisor 2 module when migrating from a Supervisor 1 to Supervisor 2 module, use the **copy ssm-nvram** standby-sup command in EXEC mode.

copy ssm-nvram standby-sup

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command should only be used for migrating from a Supervisor 1 to a Supervisor 2 module. When both modules in the switch are the same, you should not use this command; use the **copy** command instead.

Examples

The following example copies the contents of the SSM NVRAM to the standby Supervisor 2 module:

```
switch# copy ssm-nvram standby-sup
```

Related Commands

Command	Description
copy	Saves a backup of the system software.

counter (port-group-monitor configuration mode)

To configure individual counter in a port group monitor policy to use non-default values, use the counter command. To reset the counter to its default values in a Port Group Monitor policy, use the no form of the command.

counter {**rx-performance**|**tx-performance**} **poll-interval** *interval* **delta rising-threshold** *rising threshold* **falling-threshold low** *threshold*
no counter {**rx-performance**|**tx-performance**} **poll-interval** *interval* **delta rising-threshold** *rising threshold* **falling-threshold** *falling-threshold*

Syntax Description

rx-performance	Counfigures RX performance counter.
tx-performance	Configures TX performance counter.
poll-interval	Configures poll interval for counter.
interval	Displays poll interval in seconds. The range is from 0 to 2147483647.
delta	Displays the threshold type.
rising-threshold	Configures the upper threshold value which is the percentage of the polling interval.
rising-threshold	Sets numerical upper threshold limit. The range is from 0 to 100.
falling-threshold	Configures the lower threshold value which is the percentage of the polling interval.
falling-threshold	Sets numerical falling threshold limit. The range is from 0 to 100.

Command Default

None

Command Modes

Configuration Port Group Monitor mode

Command History

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

Usage Guidelines

This command is available in port-group-monitor configuration mode.

Examples

The following example shows how to configure monitoring of a specific counter within a Port Group Monitor policy:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#port-group name pgmon
switch(config-port-group-monitor)# counter rx-performance
switch(config-port-group-monitor)# counter tx-performance
switch(config-port-group-monitor)#
```

The following example shows how to turn off the monitoring of a specific counter in the given policy:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# no port-group-monitor name pgmon
switch(config-port-group-monitor)# no counter rx-performance
switch(config-port-group-monitor)# no counter tx-performance
switch(config-port-group-monitor)#show port-group-monitor
--------------------------------------------------------------------------------
-----------
Port Group Monitor : enabled
--------------------------------------------------------------------------------
-----------
Policy Name : pgmonAdmin status : Not Active
Oper status  : Not Active
Port type    : All Port Groups
--------------------------------------------------------------------------------------------Counter
 Threshold Interval %ge Rising Threshold %ge Falling Threshold In Use------- ---------
-------- ------------------- ---------------------- ------RX Performance Delta 60 80 20
YesTX Performance Delta 60 80 20
No-----------------------------------------------------------------------
```

Related Commands

Command	Description
show port-group-monitor	Displays Port Group Monitor information.

counter (port-monitor configuration mode)

To configure individual counter in a port-monitor policy to use non-default values, use the **counter** command. To reset the counter to its default values in a port-monitor policy, use the **no** form of the command.

counter {**credit-loss-reco** |**err-pkt-from-port** |**err-pkt-from-xbar** |**err-pkt-to-xbar** |**invalid-crc** |**invalid-words** |**link-loss** |**lr-rx** |**lr-tx** |**rx-datarate** |**signal-loss** |**state-change** |**sync-loss** |**timeout-discards** |**tx-credit-not-available** |**tx-datarate** |**tx-discards** |**tx-slowport-count** |**tx-slowport-oper-delay** |**txwait**} **poll-interval** *seconds* {**absolute** |**delta**} **rising-threshold** *count1* **event** *RMON-ID* **warning-threshold** *count2* **falling-threshold** *count3* **event** *RMON-ID* **portguard** {**errordisable** |**flap**}
no counter {**credit-loss-reco** |**err-pkt-from-port** |**err-pkt-from-xbar** |**err-pkt-to-xbar** |**invalid-crc** |**invalid-words** |**link-loss** |**lr-rx** |**lr-tx** |**rx-datarate** |**signal-loss** |**state-change** |**sync-loss** |**timeout-discards** |**tx-credit-not-available** |**tx-datarate** |**tx-discards** |**tx-slowport-count** |**tx-slowport-oper-delay** |**txwait**} **poll-interval** *seconds* {**absolute** |**delta**} **rising-threshold** *count1* **event** *RMON-ID* **warning-threshold** *count2* **falling-threshold** *count3* **event** *RMON-ID* **portguard** {**errordisable** |**flap**}

Syntax Description

credit-loss-reco	Configures the credit loss recovery counter 1.3.6.1.4.1.9.9.289.1.2.1.1.37.
err-pkt-from-port	Configures the err-pkt-from-port counter 1.3.6.1.4.1.9.9.779.1.1.1.1.4.0.1.
err-pkt-from-xbar	Configures the err-pkt-from-xbar counter 1.3.6.1.4.1.9.9.779.1.1.1.1.4.0.2.
err-pkt-to-xbar	Configures the err-pkt-to-xbar counter 1.3.6.1.4.1.9.9.779.1.1.1.1.4.0.3.
invalid-crc	Configures the invalid-crc counter 1.3.6.1.4.1.9.9.289.1.2.1.1.6.
invalid-words	Configures the invalid-words counter 1.3.6.1.4.1.9.9.289.1.2.1.1.5.
link-loss	Configures the link failure counter 1.3.6.1.4.1.9.9.289.1.2.1.1.1.
lr-rx	Configures the number of link reset responses received by the Fibre Channel port 1.3.6.1.4.1.9.9.289.1.2.1.1.9.
lr-tx	Configures link reset responses transmitted by the Fibre Channel port 1.3.6.1.4.1.9.9.289.1.2.1.1.10.
rx-datarate	Configures the receive performance counter 1.3.6.1.2.1.31.1.1.1.6.
signal-loss	Configures the signal-loss counter 1.3.6.1.4.1.9.9.289.1.2.1.1.3.
state-change	Configures the state-change counter. 1.3.6.1.4.1.9.9.289.1.2.1.1.46.
sync-loss	Configures the sync-loss counter 1.3.6.1.4.1.9.9.289.1.2.1.1.2.
timeout-discards	Configures the timeout-discards counter 1.3.6.1.4.1.9.9.289.1.2.1.1.35.
tx-credit-not-available	Configures the transmit credit not available counter 1.3.6.1.4.1.9.9.289.1.2.1.1.38.
tx-datarate	Configures the transmit performance counter 1.3.6.1.2.1.31.1.1.1.10.
tx-discards	Configures the transmit discards counter 1.3.6.1.4.1.9.9.289.1.2.1.1.36.
tx-slowport-count	Configure the tx-slowport-count counter.

tx-slowport-oper-delay	Configure the tx-slowport-oper-delay counter. 1.3.6.1.4.1.9.9.289.1.2.1.1.45.
txwait	Configures the txwait counter. 1.3.6.1.4.1.9.9.289.1.2.1.1.47.
poll-interval *seconds*	Configures poll interval in seconds. The range is from 1 to 700000 seconds.
absolute	Absolute threshold type.
delta	Delta threshold type.
rising-threshold *count1*	Sets numerical upper threshold limit. The range is from 0 to 184467440737095516151.
event-id *RMON-ID*	Event ID. The range is from 0 to 2147483647. **Note** You can also configure the following RMON events: • Event 1: Fatal • Event 3: Error • Event 4: Warning • Event 5: Information
warning-threshold *count2*	Sets numerical warning threshold limit. The range is from 0 to18446744073709551615.
falling-threshold *count3*	Sets numerical lower threshold limit. The range is from 0 to18446744073709551615.
portguard errordisable	Sets the port guard action to disable errors on a port when a given threshold criteria is met.
portguard flap	Sets the port guard action to flap a port when a give threshold criteria is met.

Command Default

None

Command Modes

Port monitor configuration mode.

Command History

Release	Modification
6.2(17)	Added the **state-change** keyword to the syntax description.
6.2(15)	Added the **warning-threshold** keyword to the syntax description.
6.2(13)	Added **tx-slowport-count**, **tx-slowport-oper-delay**, and **txwait** keywords to the syntax description.
5.2(2a)	Added err-pkt-from-port, err-pkt-from-xbar, err-pkt-to-xbar new counters to the syntax description.
4.2(1)	This command was introduced.

Usage Guidelines

The rx-datarate and tx-datarate are calculated using the inoctets and outoctets on an interface. We recommend that you use the delta threshold type for all the counters except the tx-slowport-oper-delay counter which uses absolute threshold type.

Examples

The following example shows how to configure the credit loss recovery counter within a Port Monitor policy:

```
switch# configure
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-monitor name pgmon
switch(config-port-monitor)# counter credit-loss-reco poll-interval 60 delta rising-threshold
 5 event 4 falling-threshold 1 event 4
```

The following example shows how to configure the err-pkt-from-port counter:

```
switch# configure
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-monitor name pgmon
switch(config-port-monitor)# counter err-pkt-from-port poll-interval 30 delta rising-threshold
 50 event 50 falling-threshold 40 event 40
```

Related Commands

Command	Description
show port-monitor	Displays port monitor information.

counter tx-slowport-count

To configure the tx-slowport-count counter, use the counter tx-slowport-count command. To reset the counter use the no form of the command.

counter tx-slowport-count poll-interval seconds {**absolute**|**delta**} **rising-threshold count1 event event-id** [**falling-threshold count2 event event-id**]
no counter tx-slowport-count poll-interval seconds {**absolute**|**delta**} **rising-threshold count1 event event-id** [**falling-threshold count2 event event-id**]

Syntax Description

poll-interval	Configures poll interval for the counter.
seconds	Displays the poll-interval in seconds.
absolute	Displays the threshold type.
delta	Displays the threshold type.
rising-threshold	Configures the upper threshold limit for the counter.
count1	Sets a numerical for the rising threshold limit.
event	Configures rising-threshold event.
event-id	Sets a numerical for the rising threshold event.
falling-threshold	Configures the lower threshold value for the counter.
count2	Sets a numerical for the falling threshold limit.
event	Configures falling-threshold event.
event-id	Sets a numerical for the falling-threshold event.

Command Default

Default values of the different parameters for the counter.

Command Modes

Configuration Port Monitor mode.

Command History

Release	Modification
6.2(13)	This command was introduced.

Examples

The following example shows how to configure the tx-slowport-count counter within a Port Monitor policy:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# port-monitor name pmon
switch(config-port-monitor)# counter tx-slowport-count poll-interval 1 delta rising-threshold
```

```
 1 event 3 falling-threshold 0 event 4
switch(config-port-monitor)#
```

The following example shows how to reset to the default values for the tx-slowport-count counter within a Port Monitor policy:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# port-monitor name pmon
switch(config-port-monitor)# no counter tx-slowport-count poll-interval 1 delta
rising-threshold 1 event 3 falling-threshold 0 event 4
```

Configuration for this counter are reset to use default values.

switch(config-port-monitor)#

Related Commands

Command	Description
show port-monitor	Displays Port Monitor information.

counter tx-slowport-oper-delay

To configure the tx-slowport-oper-delay counter, use the counter tx-slowport-oper-delay command. To reset the counter use the no form of the command.

counter tx-slowport-oper-delay poll-interval seconds absolute rising-threshold value event event-id [**falling-threshold value event event id**]
no counter tx-slowport-oper-delay poll-interval seconds absolute rising-threshold value event event-id [**falling-threshold value event event id**]

Syntax Description

poll-interval	Configures poll interval for counter.
seconds	Displays the poll-interval in seconds.
absolute	Displays the threshold type.
rising-threshold	Configures the upper threshold value for the counter.
value	Sets a numerical value (in milliseconds) for the rising-threshold.
event	Configures rising-threshold event.
event-id	Sets a numerical for the rising threshold event.
falling-threshold	Configures the lower threshold value for the counter.
value	Sets a numerical (in milliseconds) for the falling-threshold.
event	Configures falling-threshold event.
event-id	Sets a numerical for the event.

Command Default

Default values of the different parameters for the counter.

Command Modes

Configuration Port Monitor mode

Command History

Release	Modification
6.2(13)	This command was introduced.

Examples

The following example shows how to configure the tx-slowport-oper-delay counter within a Port Monitor policy:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# port-monitor name pmon
switch(config-port-monitor)# counter tx-slowport-oper-delay poll-interval 1 absolute
rising-threshold 1 event 3 falling-threshold 0 event 4
switch(config-port-monitor)#
```

The following example shows how to reset to the default values for the tx-slowport-oper-delay counter within a Port Monitor policy:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-monitor name pmon
switch(config-port-monitor)# no counter tx-slowport-oper-delay poll-interval 1 absolute
rising-threshold 1 event 3 falling-threshold 0 event 4
Configuration for this counter are reset to use default values.
switch(config-port-monitor)#
```

Related Commands

Command	Description
show port-monitor	Displays Port Monitor information.

counter txwait

To configure the txwait counter, use the counter txwait command. To reset the counter use the no form of the command.

counter txwait poll-interval seconds {**absolute**|**delta**} **rising-threshold percentage1 event event-id** [**falling-threshold percentage2 event event-id**]
no counter txwait poll-interval seconds {**absolute**|**delta**} **rising-threshold percentage1 event event-id** [**falling-threshold percentage2 event event-id**]

Syntax Description

poll-interval	Configures poll interval for counter.
seconds	Displays the poll-interval in seconds.
absolute	Displays the threshold type.
delta	Displays the threshold type.
rising-threshold	Configures the upper threshold value for the counter.
percentage1	Sets a numerical limit (in percentage) for the rising-threshold.
event	Configures a rising-threshold event.
event-id	Sets a numerical limit (in percentage) for the rising-threshold.
falling-threshold	Configures the lower threshold value for the counter.
percentage2	Sets a numerical limit for the falling-threshold.
event	Configures a falling-threshold event.
event-id	Sets a numerical for the event.

Command Default

Default values of the different parameters for the counter..

Command Modes

Configuration Port Monitor mode.

Command History

Release	Modification
6.2(13)	This command was introduced.

Examples

The following example shows how to configure the txwait counter within a Port Monitor policy:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-monitor name pmon
switch(config-port-monitor)# counter txwait poll-interval 1 delta rising-threshold 1 event
 3 falling-threshold 0 event 4
switch(config-port-monitor)#
```

The following example shows how to reset to the default values for the txwait counter within a Port Monitor policy:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-monitor name pmon
switch(config-port-monitor)# no counter txwait poll-interval 1 delta rising-threshold 1
event 3 falling-threshold 0 event 4
Configuration for this counter are reset to use default values.
```

switch(config-port-monitor)#

Related Commands

Command	Description
show port-monitor	Displays Port Monitor information.

crllookup

To set the CRLLookup, use the **crllookup** command. To disable this feature, use the **no** form of the command.

crllookup attribute-name attribute-name search-filter string base-DN string
no crllookup attribute-name attribute-name search-filter string base-DN string

Syntax Description

attribute-name attribute-name	Specifies LDAP attribute name. The maximum size is 128 characters.
search-filter	Specifies LDAP search filter. The maximum length is 128 characters.
string	Specifies search map search filter . The maximum length is 128 characters.
base-DN	Configure base DN to be used for search operation. The Maximum length is 63 characters.
string	Specifies search map base DN name. The Maximum length is 63 characters.

Command Default

None

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None

Examples

```
The following example shows how to set the CRLLookup:
switch(config)#ldap search-map s1
switch(config-ldap-search-map)# CRLLookup attribute-name certificate RevocationList”
search-filter"(&(objectClass=CRLDistributionPoint))" base-DN "CN=CDP,CN=Public Key
Services,CN=Services,CN=Configuration,DC=DCBU-ACS"
GROUP_NAME: map1
CRL
ATTR_NAME: map1
SEARCH_FLTR: map1
BASE_DN: DN1
Sending the SET_REQ
switch(config-ldap-search-map)#end
```

Related Commands

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

crypto ca authenticate

To associate and authenticate a certificate of the certificate authority (CA) and configure its CA certificate (or certificate chain), use the **crypto ca authenticate** command in configuration mode. The CA certificate or certificate chain is assumed to already be available in Privacy Enhanced Mail (PEM) (base-64) encoded format.

crypto ca authenticate trustpoint-label

Syntax Description

trustpoint-label	Specifies the name of the trust point. The maximum size is 64 characters.

Command Default

None

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command authenticates the CA to the switch by obtaining the self-signed certificate of the CA that contains the public key of the CA. Because the CA signs its own certificate, you should manually authenticate the public key of the CA by contacting the CA administrator when you execute this command.

This command is required when you initially configure certificate authority support for the switch. Before you attempt CA authentication, first create the trust point using the **crypto ca trustpoint** command. The CA certificate fingerprint (the MD5 or SHA hash of the certificate) is generally published by the CA. When authenticating the CA, the certificate fingerprint is displayed. The administrator needs to compare it with the one published by the CA and accept the CA certificate only if it matches.

If the CA being authenticated is a subordinate CA (meaning that is is not self-signed), then it is certified by another CA which in turn may be certified by yet another CA and so on until there is a self-signed CA. In this case, the subordinate CA in question is said to have a CA certificate chain certifying it. The entire chain must be input during CA authentication. The maximum length that the CA certificate chain supports is ten.

The trust point CA is the certificate authority configured on the switch as the trusted CA. Any peer certificate obtained will be accepted if it is signed by a locally trusted CA or its subordinates.

Note The trust point configuration (created by the **crypto ca trustpoint** command) is persistent only if saved explicitly using the **copy running-config startup-config** command. The certificates and CRL associated to a trust point are automatically made persistent if the trust point in question was already saved in the startup configuration. Conversely, if the trust point was not saved in the startup configuration, the certificates and CRL associated to it are not made persistent automatically because they do not exist without the corresponding trust point after the switch reboots. To ensure that the configured certificates, CRLs and key pairs are made persistent, always save the running configuration to the startup configuration.

Examples

The following example authenticates a CA certificate called admin-ca:

```
switch# config terminal
switch(config)# crypto ca authenticate myCA
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO
MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----
 END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
Do you accept this certificate? [yes/no]:y
```

Related Commands

Command	Description
crypto ca trustpoint	Configures the trust point.
show crypto ca certificates	Displays configured trust point certificates.
show crypto ca trustpoints	Displays trust point configurations.

crypto ca crl request

To configure a new certificate revocation list (CRL) downloaded from the certificate authority (CA), use the **crypto ca crl request** command in configuration mode.

crypto ca crl request trustpoint-label source-file

Syntax Description

trustpoint-label	Specifies the name of the trust point. The maximum size is 64 characters.
source-file	Specifies the location of the CRL in the form **bootflash**:*filename* . The maximum size is 512.

Command Default

None

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Cisco MDS NX-OS allows you to pre-download CRLs for the trust points and cache the CRLs in the cert store using the **crypto ca crl request** command. During the verification of a peer certificate by IPsec/IKE or SSH, the issuer CA's CRL will be consulted only if it had already been configured locally, and revocation checking is configured to use CRL. Otherwise, CRL checking is not done and a certificate is considered to be not revoked if no other revocation checking methods are configured. This mode of CRL checking is called CRL optional.

The other modes of revocation checking are called CRL best-effort and CRL mandatory. In these modes, if the CRL is not found locally, there is an attempt to fetch it automatically from the CA. These modes are not supported in MDS SAN-OS release 3.0(1).

The CRL file specified should contain the latest CRL in either Privacy Enhanced Mail (PEM) format or Distinguished Encoding Rules (DER) format.

Note The trust point configuration (created by the **crypto ca trustpoint** command) is persistent only if saved explicitly using the **copy running-config startup-config** command. The certificates and CRL associated to a trust point are automatically made persistent if the trust point in question was already saved in the startup configuration. Conversely, if the trust point was not saved in the startup configuration, the certificates and CRL associated to it are not made persistent automatically because they do not exist without the corresponding trust point after the switch reboots. To ensure that the configured certificates, CRLs and key pairs are made persistent, always save the running configuration to the startup configuration.

Examples

The following example configures a CRL for the trust point or replaces the current CRL:

```
switch# config t
switch(config)# crypto ca crl request admin-ca bootflash:admin-ca.crl
```

Related Commands

Command	Description
revocation-check	Configures trust point revocation check methods.
show crypto ca crl	Displays configured certificate revocation lists (CRL).

crypto ca enroll

To request a certificate for the switch's RSA key pair created for this trust point CA, use the **crypto ca enroll** command in configuration mode.

crypto ca enroll trustpoint-label

Syntax Description

trustpoint-label	Specifies the name of the trust point. The maximum size is 64 characters.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

An MDS switch can enroll with the trust point CA to get an identity in the form of a certificate. You can enroll your switch with multiple trust points, thereby getting a separate identity certificate from each.

When enrolling with a trust point, you must specify an RSA key pair to be certified. This key pair must be generated and associated to the trust point before generating the enrollment request. The association between the trust point, key pair, and identity certificate is valid until it is explicitly removed by deleting the identity certificate first, followed by disassociating the key pair, and deleting the CA certificates (in any order), and finally deleting the trust point itself, in that order only.

Use the crypto ca enroll command to generate a request to obtain an identity certificate from each of your trust points corresponding to authenticated CAs. The certificate signing request (CSR) generated is per Public-Key Cryptography Standards (PKCS) #10 standard, and is displayed in PEM format. Cut and paste it and submit it to the corresponding CA through e-mail or the CA website. The CA administrator issues the certificate and makes it available to you either through the website or by sending it in e-mail. You need to import the obtained identity certificate to the corresponding trust point using the **crypto ca import** *trustpoint-label* **certificate** command.

The challenge password is not saved with the configuration. This password is required in the event that your certificate needs to be revoked, so you must remember this password.

Examples

The following example generates a certificate request for an authenticated CA:

```
switch# config t
switch(config)# crypto ca enroll myCA
 Create the certificate request ..
 Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.
  Password:nbv123
 The subject name in the certificate will be: Vegas-1.cisco.com
 Include the switch serial number in the subject name? [yes/no]:no
 Include an IP address in the subject name [yes/no]:yes
```

```
ip address:209.165.200.226
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----
```

Related Commands

Command	Description
crypto ca import trustpoint-label certificate	Imports the identity certificate obtained fromthe CA to the trust point.
crypto key generate rsa	Generates an RSA key pair.
rsakeypair	Configures and associates the RSA key pair details to a trust point.
show crypto key mypubkey rsa	Displays all RSA public key configurations.

crypto ca export

To export the RSA key pair and the associated certificates (identity and CA) of a trust point within a Public-Key Cryptography Standards (PKCS) #12 format file to a specified location, use the **crypto ca export** command in configuration mode.

crypto ca exporttrustpoint-label pkcs12 destination-file-url pkcs12-password

Syntax Description

trustpoint-label	Specifies the name of the trust point. The maximum size is 64 characters.
pkcs12 *destination-file-url*	Specifies a destination file in **bootflash**:*filename* format. The maximum size is 512 characters.
pkcs12-password	Specifies the password to be used to protect the RSA private key inthe exported file. The maximum size is 64 characters.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can export the identity certificate along with the associated RSA key pair and CA certificate (or certificate chain) to a PKCS #12 format file for backup purposes. You can later import the certificate and RSA key pair to recover from a system crash on your switch.

Examples

The following example shows how to export a certificate and key pair in PKCS #12 format:

```
switch# config terminal
switch(config)# crypto ca export admin-ca pkcs12 bootflash:adminid.p12 nbv123
```

Related Commands

Command	Description
crypto ca import trustpoint-label certificate	Imports the identity certificate obtained from the CA to the trust point.
crypto ca import trustpoint-label pkcs12	Imports the identity certificate and associated RSA key pair and CA certificate (chain) to a trust point.
crypto key generate rsa	Generates an RSA key pair.
rsakeypair	Configures and associates the RSA key pair details to a trust point.
show crypto key mypubkey rsa	Displays any RSA public key configurations.

crypto ca import

To import the identity certificate alone in PEM format or the identity certificate and associated RSA key pair and CA certificate (or certificate chain) in Public-Key Cryptography Standards (PKCS) #12 form, use the **crypto ca import** command in configuration mode.

crypto ca import trustpoint-label {**certificate**|**pkcs12 source-file-url pkcs12-password**}

Syntax Description

trustpoint-label	Specifies the name of the trust point. The maximum size is 64 characters.
pkcs12 *source-file-url*	Specifies a source file in **bootflash**:*filename* format. The maximum size is 512 characters.
pkcs12-password	Specifies the password that was used to protect the RSA private key in the imported PKCS#12 file. The maximum size is 64 characters.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The first form of the command, **crypto ca import** *trustpoint-label* **certificate,** is used to import (by cut and paste means) the identity certificate obtained from the CA, corresponding to the enrollment request generated earlier in the trust point and submitted to the CA. The administrator is prompted to cut and paste the certificate.

The second form of the command, **crypto ca import** *trustpoint-label* **pkcs12** *source-file-url pkcs12-password* , is used to import the complete identity information (that is, the identity certficate and associated RSA key pair and CA certificate or certficate chain) into an empty trust point. This command is useful for restoring the configuration after a system goes down.

Note The trust point configuration (created by the **crypto ca trustpoint** command) is persistent only if saved explicitly using the **copy running-config startup-config** command. The certificates and CRL associated to a trust point are automatically made persistent if the trust point in question was already saved in the startup configuration. Conversely, if the trust point was not saved in the startup configuration, the certificates and CRL associated to it are not made persistent automatically because they do not exist without the corresponding trust point after the switch reboots. To ensure that the configured certificates, CRLs and key pairs are made persistent, always save the running configuration to the startup configuration.

Examples

The following example installs an identity certificate obtained from a CA corresponding to an enrollment request made and submitted earlier:

```
switch# config t
```

```
switch(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD
VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz
Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu
Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XENlcnRFbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
```

The following example shows how to import a certificate and key pair in a Public-Key Cryptography Standards (PKCS) #12 format file:

```
switch# config t
witch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123
```

Related Commands

Command	Description
crypto ca enroll	Generates a certificate signing request for a trust point.
crypto ca export trustpoint-label pkcs12	Exports the RSA key pair and associated certificates of a trust point.
crypto key generate rsa	Generates the RSA key pair.
rsakeypair	Configures trust point RSA key pair details.
show crypto ca certificates	Displays the identity and CA certificate details.
show crypto key mypubkey rsa	Displays any RSA public key configurations.

crypto ca lookup

To configure the type of cretstore that PKI will use for authenticatio, use the crypto ca lookup command in configuration mode. The disable this feature, use the no form of the command.

crypto ca lookup {**both**|**local**|**remote**}

Syntax Description

both	Specifies both local and remote certstore.
local	Specifies local certstore.
remote	Specifies remote certstore.

Command Default

None

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None

Examples

The following example shows how to configure both local and remote certstore:

```
switch(config)# crypto ca lookup both
switch(config)#
```

The following example shows how to configure local certstore:

```
switch(config)# crypto ca lookup local
switch(config)#
```

The following example shows how to configure remote certstore:

```
switch(config)# crypto ca lookup remote
switch(config)#
```

Related Commands

Command	Description
show crypto ssh-auth-map	displays mapping filters applied for SSH authentication.

crypto ca remote ldap

To configure Ldap certstore, use the crypto ca remote ldap command in configuration mode. The disable this feature, use the no form of the command.

crypto ca remote ldap {**crl-refresh-time hours**|**server-group group-name**}

Syntax Description

crl-refresh-time	Specifies timer to fetch crl from remote certstore.
hours	Specifies timer value in hours. The range will be from 0 - 744. i.e. The refresh time can be configured at max for one month. So 31 * 24 = 744. And if refresh-time is 0 then the refresh routine will be executed once at the time of configuration.
server-group	Specifies LDAP server group.
group-name	Specifies LDAP server group name. The maximum size is 64 characters.

Command Default

None

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None

Examples

The following example shows how to configure timer to fetch crl from remote certstore:

```
switch(config)# crypto ca remote ldap crl-refresh-time 124
switch(config)#
```

The following example shows how to configure LDAP server group:

```
switch(config)# crypto ca remote ldap server-group admin
switch(config)#
```

Related Commands

Command	Description
show crypto ssh-auth-map	displays mapping filters applied for SSH authentication.

crypto ca test verify

To verify a certificate file, use the **crypto ca test verify** command in configuration mode.

crypto ca test verify certificate-file

Syntax Description

certificate-file	Specifies the certificate filename in the form **bootflash**:*filename* . The maximum size is 512 characters.

Command Default

None

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The **crypto ca test verify** command is only a test command. It verifies the specified certificate in PEM format by using the trusted CAs configured and by consulting the CRL or OCSP if needed, as per the revocation checking configuration.

Examples

The following example shows how to verify a certificate file. Verify status code 0 means the verification is successful.

```
switch(config)# crypto ca test verify bootflash:id1.pem
verify status oode:0
verify error msg:
```

Related Commands

Command	Description
show crypto ca certificates	Displays configured trust point certificates.

crypto ca trustpoint

To create a trust point certificate authority (CA) that the switch should trust, and enter trust point configuration submode (config-trustpoint), use the **crypto ca trustpoint** command in configuration mode. To remove the trust point, use the **no** form of the command.

crypto ca trustpoint trustpoint-label
no crypto ca trustpoint trustpoint-label

Syntax Description

trustpoint-label	Specifies the name of the trust point. The maximum size is 64 characters.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Trust points have the following characteristics:

- A trust point corresponds to a single CA, which an MDS switch trusts for peer certificate verification for any application.
- A CA must be explicitly associated to a trust point using the CA authentication process using the **crypto ca authenticate** command.
- An MDS switch can have many trust points and all applications on the switch can trust a peer certificate issued by any of the trust point CAs.
- A trust point is not restricted to a specific application.
- The MDS switch can optionally enroll with a trust point CA to get an indemnity certificate for itself.

You do not need to designate one or more trust points to an application. Any application should be able to use any certificate issued by any trust point as long as the certificate purpose satisfies application requirement.

You do not need more than one identity certificate from a trust point or more than one key pair to be associated to a trust point. A CA certifies a given identity (name) only once and does not issue multiple certificates with the same subject name. If you need more than one identity certificate for a CA, define another trust point for the same CA, associate another key pair to it, and have it certified, provided CA allows multiple certificates with same subject name.

Note Before using the **no crypto ca trustpoint** command to remove the trust point, first delete the identity certificate and CA certificate (or certificate chain) and then disassociate the RSA key pair from the trust point. The switch enforces this behavior to prevent the accidental removal of the trust point along with the certificates.

Examples

The following example declares a trust point CA that the switch should trust and enters trust point configuration submode:

```
switch#
config terminal

switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)#
```

The following example removes the trust point CA:

```
switch#
config terminal

switch(config)# no crypto ca trustpoint admin-ca
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the certificate of the certificate authority.
crypto ca enroll	Generates a certificate signing request for a trust point.
show crypto ca certificates	Displays the identity and CA certificate details.
show crypto ca trustpoints	Displays trust point configurations.

crypto cert ssh-authorize

To configure mapping filter for SSH, use the crypto cert ssh-authorize command in configuration mode. To disable this feature, use the no form of the command.

crypto cert ssh-authorize name map map name1 mapname2

Syntax Description

name	Specifies issuer name of the certificate. The maximum size is 64 characters.
map	Specifies mapping filter.
map name	Specifies the name of the mapping filter that is already configured. The maximum size is 64 characters.

Command Default

None

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None

Examples

The following example shows how to configure mapping filter for SSH:

```
switch(config)# crypto cert ssh-authorize DCBU map map1 map2
switch(config)#
```

The following example shows how to configure default mapping filter for SSH:

```
switch(config)# crypto cert ssh-authorize default map map1 map2
switch(config)#
```

Related Commands

Command	Description
show crypto ssh-auth-map	displays mapping filters applied for SSH authentication.

crypto certificatemap mapname

To configure the certificate map that will be used for filtering the certificate request, use the **crypto certificatemap mapname** command in configuration mode. To disable this feature, use the no form of the command.

crypto certificatemap mapname mapname

Syntax Description

mapname	Specifies the name of the filter map. The maximum size is 64 characters.

Command Default

None

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None

Examples

The following example shows how to display mapping filters applied for SSH authentication:

```
switch(config)# crypto certificatemap mapname map1
switch(config-certmap-filter)#
```

Related Commands

Command	Description
show crypto ssh-auth-map	displays mapping filters applied for SSH authentication.

crypto global domain ipsec security-association lifetime

To configure global parameters for IPsec, use the **crypto global domain ipsec security-association lifetime** command. To revert to the default, use the **no** form of the command.

crypto global domain ipsec security-association lifetime {**gigabytes** *number*|**kilobytes** *number*|**megabytes** *number*|**seconds** *number*}
no crypto global domain ipsec security-association lifetime {**gigabytes|kilobytes|megabytes|seconds**}

Syntax Description

gigabytes *number*	Specifies a volume-based key duration in gigabytes. The range is 1 to 4095.
kilobytes *number*	Specifies a volume-based key duration in kilobytes. The range is 2560 to 2147483647.
megabytes *number*	Specifies a volume-based key duration in megabytes. The range is 3 to 4193280.
seconds *number*	Specifies a time-based key duration in seconds. The range is 600 to 86400.

Command Default

450 gigabytes and 3600 seconds

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

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

The global security association lifetime value can be overridden for individual IPsec crypto maps using the **set** command in IPsec crypto map configuration submode.

Examples

The following example shows how to configure the system default before the IPsec:

```
switch# config terminal
switch(config)# crypto global domain ipsec security-association lifetime gigabytes 500
```

Related Commands

Command	Description
crypto ipsec enable	Enables IPsec.
set (IPsec crypto map configuration submode)	Configures IPsec crypto map entry parameters.
show crypto global domain ipsec	Displays the global attributes for IPsec.

crypto ike domain ipsec

To enter IKE configuration submode, use the **crypto ike domain ipsec** command.

crypto ike domain ipsec

Syntax Description

This command has no other arguments or keywords.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To configure IKE protocol attributes, IKE must be enabled using the **crypto ike enable** command.

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.

- The crypto ike feature is not supported on the Cisco MDS 9148 and Cisco MDS 9148S, and Cisco MDS 9396S Switches.

Examples

The following example shows how enter IKE configuration mode:

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)#
```

Related Commands

Command	Description
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

crypto ike domain ipsec rekey sa

To rekey an IKE crypto security association (SA) in the IPsec domain, use the **crypto ike domain ipsec rekey sa** command.

crypto ike domain ipsec rekey sa *sa-index*

Syntax Description

sa-index	Specifies the SA index. The range is 1 to 2147483647.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, IKE must be enabled using the **crypto ike enable** command.

Note This command is not supported on the Cisco MDS 9124 switch.

- The crypto ike feature is not supported on the Cisco MDS 9148 and Cisco MDS 9148S, and Cisco MDS 9396S Switches.

Examples

The following example rekeys an IKE crypto SA:

```
switch# crypto ike domain ipsec rekey sa 100
```

Related Commands

Command	Description
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

crypto ike enable

To enable IKE, use the **crypto ike enable** command. To disable IKE, use the **no** form of the command.

crypto ike enable
no crypto ike enable

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

The IKE protocol cannot be disabled unless IPsec is disabled.

The configuration and verification commands for the IKE protocol are only available when the IKE protocol is enabled on the switch. When you disable this feature, all related configurations are automatically discarded.

Note This command is not supported on the Cisco MDS 9124 switch.

- The crypto ike feature is not supported on the Cisco MDS 9148 and Cisco MDS 9148S, and Cisco MDS 9396S Switches.

Examples

The following example shows how to enable the IKE protocol:

```
switch# config terminal
switch(config)# crypto ike enable
```

Related Commands

Command	Description
clear crypto ike domain ipsec sa	Clears IKE protocol information clear IKE SAs.
crypto ipsec enable	Enables IPsec.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

crypto ipsec enable

To enable IPsec, use the **crypto ipsec enable** command. To disable IPsec, use the **no** form of the command.

crypto ipsec enable
no crypto ipsec enable

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To enable the IPsec, the IKE protocol must be enabled using the **crypto ike enable** command.

The configuration and verification commands for IPsec are only available when IPsec is enabled on the switch. When you disable this feature, all related configurations are automatically discarded.

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 IPsec:

```
switch# config terminal
switch(config)# crypto ipsec enable
```

Related Commands

Command	Description
show crypto global domain ipsec	Displays IPsec crypto global information.
show crypto map domain ipsec	Displays IPsec crypto map information.
show crypto transform-set domain ipsec	Displays IPsec crypto transform set information.

crypto key generate rsa

To generate an RSA key pair, use the **crypto key generate rsa** command in configuration mode.

crypto key generate rsa [**label key-pair-label**] **[exportable]** [**modulus key-pair-size**]

Syntax Description

label *key-pair-label*	(Optional) Specifies the name of the key pair. The maximum size is 64 characters.
exportable	(Optional) Configures the key pair to be exportable.
modulus *key-pair-size*	(Optional) Specifies the size of the key pair. The size ranges from 512 to 2048.

Command Default

By default, the **key** is not exportable.The default **label** is switch FQDN.The default **modulus** is 512.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can generate one or more RSA key pairs and associate each RSA key pair with a distinct trust point CA, where the MDS switch enrolls to obtain identity certificates. The MDS switch needs only one identity per CA, which consists of one key pair and one identity certificate.

Cisco MDS NX-OS allows you to generate RSA key pairs with a configurable key size (or modulus). The default key size is 512. Valid modulus values are 512, 768, 1024, 1536, and 2048.

You can also configure an RSA key pair label. The default key pair label is FQDN.

Examples

The following example shows how to configure an RSA key pair called newkeypair:

```
switch# config terminal
switch(config)# crypto key generate rsa label newkeypair
```

The following example shows how to configure an RSA key pair called testkey, of size 768, that is exportable:

```
switch# config terminal
switch(config)# crypto key generate rsa label testkey exportable modulus 768
```

The following example shows how to generate an exportable RSA key with the switch name as the default label and 512 as the default modulus:

```
switch# config terminal
switch(config)# crypto key generate rsa exportable
```

Related Commands

Command	Description
crypto key zeroize rsa	Deletes RSA key pair configurations.

Command	Description
rsakeypair	Configures trust point RSA key pair details.
show crypto key mypubkey rsa	Displays information about configured RSA key pairs.

crypto key zeroize rsa

To delete an RSA key pair from the switch, use the **crypto key zeroize rsa** command in configuration mode.

crypto key zeroize rsa key-pair-label

Syntax Description

key-pair-label	Specifies the RSA key pair to delete. The maximum size is 64 characters.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

If you believe the RSA key pair on your switch was compromised in some way and should no longer be used, you should delete it.

After you delete the RSA key pair on the switch, ask the CA administrator to revoke your switch's certificates at the CA. You must supply the challenge password you created when you originally requested the switch's certificates.

Before deleting a key pair, you should delete the identity certificates corresponding to it in various trust points if the identity certificates exist, and then disassociate the key pair from those trust points. The purpose of this is to prevent accidental deletion of a key pair for which there exists an identity certificate in a trust point.

Note The trust point configuration, certificates, and key pair configurations are made persistent only after saving to the startup configuration. To be consistent with this configuration behavior, the delete behavior is also the same. That is, the deletions are made persistent only after saving to the startup configuration. **Use the copy running-config startup-config** command to make the certificate and key pair deletions persistent.

Examples

The following example shows how to delete an RSA key pair called testkey:

```
switch# config terminal
switch(config)# crypto key zeroize rsa testkey
```

Related Commands

Command	Description
crypto key generate rsa	Configures an RSA key pair.
rsakeypair	Configures trust point RSA key pair details.
show crypto key mypubkey rsa	Displays information about configured RSA key pairs.

crypto map domain ipsec (configuration mode)

To specify an IPsec crypto map and enter IPsec crypto map configuration mode, use the **crypto map domain ipsec** command. To delete an IPsec crypto map or a specific entry in an IPsec crypto map, use the **no** form of the command.

crypto map domain ipsec *map-name* [*seq-number*]
no crypto map domain ipsec *map-name* [*seq-number*]

Syntax Description

map-name	Specifies the map name. Maximum length is 63 characters.
seq-number	(Optional) Specifies the sequence number for the map entry. The range is 1 to 65535.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

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

The sequence number determines the order in which IPsec crypto map entries are applied.

Examples

The following example specifies entry 1 for IPsec crypto map IPsecMap and enters IPsec crypto map configuration mode:

```
switch# config terminal
switch(config)# crypto map domain ipsec IPsecMap 1
switch(config-crypto-map-ip)#
```

The following example deletes an IPsec crypto map entry:

```
switch# config terminal
switch(config)# no crypto map domain ipsec IPsecMap 1
```

The following example deletes the entire IPsec crypto map:

```
switch# config terminal
switch(config)# no crypto map domain ipsec IPsecMap
```

Related Commands

Command	Description
crypto ipsec enable	Enables IPsec.
crypto transform-set domain ipsec	Configures the transform set for an IPsec crypto map.

Command	Description
set (IPsec crypto map configuration submode)	Configures IPsec crypto map entry parameters.
show crypto map domain ipsec	Displays IPsec crypto map information.

crypto map domain ipsec (interface configuration submode)

To configure an IPsec crypto map on a Gigabit Ethernet interface, use the **crypto map domain ipsec** command in interface configuration submode. To remove the IPsec crypto map, use the **no** form of the command.

crypto map domain ipsec *map-name*
no crypto map domain ipsec

Syntax Description

map-name	Specifies the map name. Maximum length is 63 characters.

Command Default

None

Command Modes

Interface configuration submode

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

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

The sequence number determines the order in which crypto maps are applied.

Examples

The following example shows how to specify an IPsec crypto map for a Gigabit Ethernet interface:

```
switch# config terminal
switch(config)# interface gigabitethernet 1/2
switch(config-if)# crypto map domain ipsec IPsecMap
```

Related Commands

Command	Description
crypto ipsec enable	Enables IPsec.
show crypto map domain ipsec	Displays IPsec crypto map information.
show interface	Displays interface information.

crypto transform-set domain ipsec

To create and configure IPsec transform sets, use the **crypto transform-set domain ipsec** command. To delete an IPsec transform set, use the **no** form of the command.

crypto transform-set domain ipsec set-name {**esp-3des**|**esp-des**} [{**esp-aes-xcbc-mac**|**esp-md5-hmac**|**esp-sha1-hmac**}]
crypto transform-set domain ipsec *set-name* **esp-aes** {**128**|**256**} [{**ctr** {**esp-aes-xcbc-mac**|**esp-md5-hmac**|**esp-sha1-hmac**}|**esp-aes-xcbc-mac**|**esp-md5-hmac**|**esp-sha1-hmac**}]
no crypto transform-set domain ipsec set-name {**esp-3des**|**esp-des**} [{**esp-aes-xcbc-mac**|**esp-md5-hmac**|**esp-sha1-hmac**}]
no crypto transform-set domain ipsec *set-name* **esp-aes** {**128**|**256**} [{**ctr** {**esp-aes-xcbc-mac**|**esp-md5-hmac**|**esp-sha1-hmac**}|**esp-aes-xcbc-mac**|**esp-md5-hmac**|**esp-sha1-hmac**}]

Syntax Description

set-name	Specifies the transform set name. Maximum length is 63 characters.
esp-3des	Specifies ESP transform using the 3DES cipher (128 bits).
esp-des	Specifies ESP transform using the DES cipher (56 bits).
esp-aes-xcbc-mac	Specifies ESP transform using AES-XCBC-MAC authentication.
esp-md5-hmac	Specifies ESP transform using MD5-HMAC authentication.
esp-sha1-hmac	Specifies ESP transform using SHA1-HMAC authentication
esp-aes	Specifies ESP transform using the AES cipher (128 or 256 bits).
128	Specifies ESP transform using AES 128-bit cipher.
256	Specifies ESP transform using AES 256-bit cipher.
ctr	Specifies AES in counter mode.

Command Default

None

The default mode of AES is CBC (Cyber Block Chaining).

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.
5.2(2)	The **esp-aes-xcbc-mac** keyword was not supported.

Usage Guidelines

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

You can use this command to modify existing IPsec transform sets. If you change a transform set definition, the change is only applied to crypto map entries that reference the transform set. The change is not applied

to existing security associations, but used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database using the **clear crypto sa domain ipsec** command.

Examples

The following example shows how to configure an IPsec transform set:

```
switch# config terminal
switch(config)# crypto transform-set domain ipsec Set1 esp-aes 128
```

Related Commands

Command	Description
clear crypto sa domain ipsec	Clears security associations.
crypto ipsec enable	Enables IPsec.
show crypto transform-set domain ipsec	Displays IPsec crypto transform set information.

customer-id

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

customer-id *customer-id*
no customer *customer-id*

Syntax Description

customer-id	Specifies the customer ID. The maximum length is 64 alphanumeric characters in free format.

Command Default

None

Command Modes

Call Home configuration submode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

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

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# customer-id Customer1234
```

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.

Caching Services Module Commands

cluster name

To perform operations on a previously-configured cluster, use the **cluster name** command in SVC configuration mode.

cluster name *cluster-name* **flash-copy** *fc-grp-name* [{**prepare**|**start**|**stop**}]
cluster name *cluster-name* **remote-copy** *rc-grp-name* {**failover**|**start** [{**aux**|**clean**|**force**}]|**stop** **aux-enable**}
cluster name *cluster-name* **shutdown** [**node** *node-name*]
cluster name *cluster-name* **start discovery**
cluster name *cluster-name* **upgrade svc-system force**

Syntax Description

cluster	Provides access to cluster commands
name *cluster-name*	Identifies a previously created cluster to perform an operation.
flash-copy *fc-grp-name*	Specifies a previously-configured FlashCopy relationship.
prepare	Prepares the FlashCopy consistency group.
start	Starts the FlashCopy for the specified cluster. Starts the background copy for the specified remote copy group
stop	Stops the FlashCopy for the specified cluster. Stops the remote copy relationships for the specified remote copy group.
remote-copy *rc-grp-name*	Specifies the remote copy consistency group name.
failover	Reverses to using the auxiliary VDisks for the specified relationship.
shutdown	Shuts down the entire cluster (gracefully).
node *node-name*	Specifies a particular node for a graceful shutdown.
start discovery	Starts the background copy for the specified remote copy group.
aux	Makes the auxiliary VDisks as primary.
clean	Marks the intended secondary VDisks as clean.
upgrade svc-system	Upgrades the specified cluster. The new version of the software image is specified to the FTP:, SCP:, SFTP:, TFTP:, bootflash:, or slot0: directories
force	Permits the remote copy operation to start—even if it leads to the loss of data consistency between the primary and secondary.
aux-enable	Enables write access o the secondary (or auxiliary) VDisks.

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example enters the SVC configuration mode and displays all options under the **cluster name** command.

```
switch# svc-config
switch(svc)# cluster name SampleCluster ?
  flash-copy   Flash-copy
  remote-copy  Remote copy
  shutdown     Shutdown
  start        Start discovery
  upgrade      Upgrade uri
switch(svc)# cluster name SampleCluster flash-copy f1 prepare
switch(svc)# cluster name SampleCluster flash-copy f1 start
switch(svc)# cluster name SampleCluster flash-copy f1 stop

switch(svc)# cluster name SampleCluster remote-copy f1 failover
switch(svc)# cluster name SampleCluster remote-copy f1 start
switch(svc)# cluster name SampleCluster remote-copy f1 stop

switch(svc)# cluster name SampleCluster shutdownn
switch(svc)# cluster name SampleCluster shutdown node svc2/1
switch(svc)# cluster name SampleCluster start discovery
switch(svc)# cluster name SampleCluster upgrade svc-system
bootflash:m9000-ek9-csm-svc_mz.1.3.1.bin
```

cluster config

To manage cluster configurations on a specified cluster, use the **cluster config** configuration submode.

cluster config *cluster-name*

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode (switch(svc-cluster)#).

Command Default

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example enters the SVC configuration mode and adds a cluster called SampleCluster.

```
switch(svc)# cluster config SampleCluster
switch(svc-cluster)#
```

Related Commands

Command	Description
show cluster	Displays configured cluster information.

cluster add

To create a cluster with a specified SVC node, use the **cluster add** command in SVC configuration mode.

cluster add *cluster-name* **ip** *ip-address* **node svc** *slot-number/node-number*

Syntax Description

cluster	Provides access to cluster commands
add *cluster-name*	Specifies a new cluster addition. The cluster name must start with an alphabet and is restricted to 15 alphanumeric characters, including dash (-) and underscore (_). The cluster name cannot be Cluster*X*, where *X* is a number.
ip *ip-address*	Specifies the IP address of the specified cluster. The IP address must be in the same subnet as the switch management IP address.
node svc	Specifies the node's SVC interface
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

Enter this command while connected to the switch management IP address of a node at which the cluster is being created.

Examples

The following example enters the SVC configuration mode, verifies the status of previously-configured clusters, and adds a cluster called SampleCluster.

```
switch# svc-config
switch(svc)# show nodes local
--------------------------------------------------------------------------------
Node             cluster          config   cluster      node            sw
                                  node     status       status          version
--------------------------------------------------------------------------------
svc2/1                            No       unconfigured free            1.3(1)
svc2/2                            No       unconfigured free            1.3(1)
switch(svc)# cluster add SampleCluster ip 10.10.0.1 node svc 2/1
cluster creation going on. Please wait....
```

The status of the newly-added cluster can be verified using the **show nodes local** command.

```
switch(svc)# show nodes local
--------------------------------------------------------------------------------
Node    cluster     config  cluster    node    sw
        node  status    status    version
```

```
--------------------------------------------------------------------------------
svc2/1    SampleCluster      Yes  active    active   1.3(1)
svc2/2         No  unconfigured    free   1.3(1)
```

Related Commands

Command	Description
show nodes local	Displays the cluster name and status for all nodes in the switch.

feature enable

To enable a specified feature in a cluster, use the **feature enable** command in the cluster configuration submode.

cluster config *cluster-name*
feature enable {**capacity** *number*|**flash-copy**|**remote-copy**}

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
feature enable	Enables a specified feature on this cluster. Three features can be enabled: **capacity**, flash-copy, or remote-copy
capacity	Configures the virtualization capacity of this cluster.
number	Provides a range from 1- 1677215 Gigabytes.
flash-copy	Enables the flash-copy feature for this cluster.
remote-copy	Enables the remote-copy feature for this cluster.

Command Default

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is (switch(svc-cluster)#).

By default, flash-copy and remote-copy are disabled and 0 (zero) GB of virtualization capacity is enabled.

Examples

The following example enters the cluster configuration submode for the SampleCluster cluster and assigns a size of 4000 Gigabytes. The next two commands enables the flash-copy and remote-copy features for this cluster.

```
switch(svc)# cluster config SampleCluster
switch(svc-cluster)# feature enable ?
  capacity     Cluster enable feature capacity
  flash-copy   Cluster enable feature flash-copy
  remote-copy  Cluster enable feature remote-copy
switch(svc-cluster)# feature enable capacity ?
  <0-2147483647>  Enter the capacity
switch(svc-cluster)# feature enable capacity 4000
switch(svc-cluster)# feature enable flash-copy
switch(svc-cluster)# feature enable remote-copy
```

Related Commands

Command	Description
show cluster *name* **flash-copy**	Displays configured flash-copy information for a specified cluster.
show cluster *name* **remote-copy**	Displays configured remote copy information for a specified cluster.

flash-copy

To create a snapshot (or point-in-time copy) of a specified VDisk or group of VDisks, use the **flash-copy** command in the cluster configuration submode.

cluster config *cluster-name*
flash-copy add *fcopy-name*
{**flash-copy name** *fcopy-name* **map src-vdisk** *vdisk-name* **dst-vdisk** *vdisk-name*|[{**mode copy-on-write**|**full rate** *rate*}]}
flash-copy rename *old-name* **newname** *new-name*

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
flash-copy add *fcopy-name*	Creates a FlashCopy instance.
flash-copy *fcopy-name*	Enters the FlashCopy submode for an existing copy name.
map	Creating a mapping between the source and destination VDisks.
src-vdisk *vdisk-name*	Specifies the source VDisk for the flash copy.
dst-vdisk *vdisk-name*	Specifies the destination VDisk for the flash copy.
mode	Controls the FlashCopy mode.
copy-on-write	Copies to the source VDisk only if new information in written to it after FlashCopy is initiated (default).
full rate *rate*	Specifies the background copy rate (ranges from 1 to 100) at which the source VDisk is copied to the destination VDisk even if no new information is written to the source.

Command Default

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is (switch(svc-cluster)#.

The flash-copy submode prompt is switch(svc-cluster-flash-copy)#.

Examples

The following example enters the enters the cluster configuration mode for the SampleCluster 1 cluster.

```
switch(svc)# cluster config SampleCluster
switch(svc-cluster)# flash-copy f2
switch(svc-cluster-flash-copy)# ?
```

```
Submode Commands:
  exit  Exit from this mode
  map   Flash-copy map
  mode  Flash-copy mode
  no    Negate a command or set its defaults
switch(svc-cluster-flash-copy)# map src-vdisk VDISK1 dst-vdisk DDISK1
switch(svc-cluster-flash-copy)# mode copy-on-write
switch(svc-cluster-flash-copy)# exit
switch(svc-cluster)# flash-copy add FlashC2
switch(svc-cluster)# exit
switch(svc)# show SampleCluster flash-copy
--------------------------------------------------------------------------------
name             status
--------------------------------------------------------------------------------
fccstgrp0        idle_or_copied
f2               idle_or_copied
switch(svc)# show SampleCluster flash-copy f2
Flash-copy mapping 1:
    src vdisk is v2
    dest vdisk is v3
    state is idle_or_copied
    copy rate is 50
    progress 0% done
```

Related Commands

Command	Description
show SampleCluster *name* **flash-copy**	Displays configured flash-copy information for a specified SampleCluster.

host

To create or configure hosts, use the **host** command in the cluster configuration submode.

cluster config *cluster-name*
host add *host-name* **hostport** *port-wwn*
{**host name** *host-name* **hostport** *port-wwn*|**map vdisk** *vdisk-name* [**SCSI-lun** *lun-number*]}

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
host add *host-name*	Creates a host with one port and assigns the host name.
hostport *port-wwn*	Specifies a port using the port WWN
host name *host-name*	Enters the host submode for an existing host name.
map	Maps a previously configured disk to this host.
vdisk *vdisk-name*	Specifies the VDisk to be mapped to the host.
SCSI-lun *lun-number*	Specifies a LUN to map the host port. If the LUN number is not specified, the next available number is assigned automatically.

Command Default

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is (switch(svc-cluster)#).

The host submode prompt is switch (svc-cluster-host)#

Examples

The following example enters the cluster configuration mode for SampleCluster and creates a host called Host 1with one port, adds a second port, and maps the VDisk for Host1, and verifies the configured information for Host1.

```
switch(svc)# cluster config SampleCluster
switch(svc-cluster)# host add Host1 hostport 11:22:33:44:aa:bb:cc:dd
switch(svc-cluster)# host Host1
switch(svc-cluster-host)# ?
Submode Commands:
  exit      Exit from this mode
  hostport  Add pWWN to host
  map       Map vdisk to host
  no        Negate a command or set its defaults
switch(svc-cluster-host)# hostport 22:11:33:55:11:aa:bb:cc
switch(svc-cluster)# host add Host1 hostport 35:66:11:22:aa:bb:22:cc
switch(svc-cluster)# host Host1
```

```
switch(svc-cluster-host)# hostport 35:66:11:22:aa:bb:22:11
switch(svc-cluster-host)# map vdisk Vdisk1
switch(svc-cluster-host)# map vdisk Vdisk1 ssci-lun 10
```

Related Commands

Command	Description
show cluster *name* **host**	Displays configured host information for a specified cluster.

install module node

To install the SVC node image, use the **install module node** command.

install module *module-number* **node** *node-number* **image svc-system** [**bootflash:** | **slot0:** | **ftp:** | **sftp:** | **scp:** | *svc-image*]

Syntax Description

install module	Installs the specified image for the CSM.
module-number	Switching modules:From slot 1 to 4 and 7 to 9 in a Cisco MDS 9500 Series switch.For slot 2 in a Cisco MDS 9200 Series switch. Supervisor modules:Slot 5 or 6—only on the active supervisor module in a Cisco MDS 9500 Series switch.Slot 1—upgrades both the supervisor and switching parts of the module in a Cisco MDS 9200 Series switch.
node	Selects the SVC node to install the image.
node-number	Specifies the node number.
image svc-system	Specifies the file name of an SVC image.
bootflash:	Source location for internal bootflash memory
ftp	URI containing SVC Image.
scp	URI containing SVC Image.
sftp	URI containing SVC Image.
tftp	URI containing SVC Image.
slot0:	Source location for the CompactFlash memory or PCMCIA card.
svc-image	The name of the SAN Volume Controller (SVC) image.

Command Default

None.

Command Modes

EXEC mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.0(3).

Usage Guidelines

The **install module** *module-number* **node** command installs the new image in the specified node on the CSM module. All previous data in that node is lost.

Examples

The following example shows how to install a new image on an SVC node.

```
switch# install module 2 node 1 image svc-system
scp://root@172.22.93.174/auto/isan-src/MAIN_1_3_0_17t/VegasSW/build/gdb.sb-svc/isan/targetfs/sb-svc.bin
SVC reimage going on. Please wait
```

```
root@172.22.93.174's password:
sb-svc.bin        100% |*****************************| 45408 KB    00:53
svc 2/1 software reimage succeeded
```

Related Commands

Command	Description
show version compatibility	Shows the system software that is currently running on the switch

interface svc

To configure a SAN Volume Controller (SVC) interface on the Cisco MDS 9000 Family of switches, use the **interface svc** command.

interface svc *slot_number/node-number*
interface svc *slot_number/node-number* **initiator | mgmt | nwwn** *nwwn-id* **target vsan** *vsan-id*
interface svc *slot_number/node-number* **[switchport description | shutdown]**

Syntax Description

interface	Configures a new interface.
svc	Specifies the new interface to be a SVC interface.
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.
initiator	Configures the initiator or port in the specified VSAN.
mgmt	Configures the management or port in the specified VSAN.
target	Configures the target or port in the specified VSAN.
vsan *vsan-id*	Specifies the VSAN ID ranging from 1 to 4093.
shutdown	Enables or disables an interface.
nwwn *nwwn-id*	Configured a non-system allocated nWWN for SVC Node.
switchport description	Assigns a description to the switchport. Restricted to 80 alphanumeric characters.

Command Default

None.

Command Modes

Configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

By default, all three N-port types (initiator, mgmt, and target) are in VSAN 1. Explicitly remove it from VSAN 1 if this is not required by your network.

The VSAN number can be any number from 1 to 4096. Only 64 VSANs for all initiator/mgmt/target are allowed (meaning, you can have initiator in VSANs 1-30, target in VSANs 31-60, and mgmt in VSANs 61-64). If the target, initiator, and mgmt overlap in VSANs, each overlap is also included in the total VSAN count.

A mgmt N-port can only exist in 4 of these 64 VSANs.

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

interface **svc 1/1** *space* **,** *space* **svc 2/1-2**

This command configures Slot 1 Node 1 as an SVC interface and simultaneously configures Slot 2, Nodes 1and 2 as SVC interfaces.

Place the disk, host, and other SVC nodes in the appropriate VSAN for any configuration to be completely established

Examples

The following example configures the initiator N-port on VSAN 1, the target N-port on VSAN 2, and the management N-port on VSAN 3.

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface svc 2/1
switch(config-if)# ?
Interface configuration commands:
 do          EXEC command
 exit        Exit from this submode
 initiator   Configure Initiator traffic for SVC Node
 mgmt        Configure traffic for communication with other SVC Nodes
 no          Negate a command or set its defaults
 nwwn        Configured a non-system allocated nWWN for SVC Node
 shutdown    Enable/disable an interface
 switchport  Configure switchport parameters
  target      Configure Target traffic for SVC Node
switch(config-if)# initiator vsan 1
switch(config-if)# target vsan 2
switch(config-if)# mgmt vsan 3
```

Related Commands

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

iogroup

To assign a name to I/O groups, use the **iogroup** command in the cluster configuration submode. Use the **no** form of this command to delete the configured I/O group alias.

cluster config *cluster-name*
iogroup *group-id* **alias** *alias-name*

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
iogroup *group-id*	Identifies one of four I/O groups in the specified cluster. The ID ranges from 1 to 4.
alias *alias-name*	Assigns a name to the selected I/O group. The name is restricted to 15 alphanumeric characters.

Command Default

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The **no iogroup** command deletes the alias name, not the I/O group itself.

The cluster configuration submode prompt is (switch(svc-cluster)#).

Examples

The following example enters the cluster configuration mode for SampleCluster and configures a new I/O group. The created group is verified using the **show cluster** *name* **iogroup** command

```
switch(svc)# cluster config SampleCluster
switch(svc-cluster)# iogroup 1 alias SampleIOgroup
switch(svc-cluster)# exit
```

Related Commands

Command	Description
show cluster *name* **iogroup**	Displays configured I/O group information for a specified cluster.

ip

To modify the IP address for a cluster, use the **ip** command in the cluster configuration submode.

cluster config *cluster-name*
ip *ip-address*

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submodes.
ip *ip-address*	Specifies the IP address of the cluster.

Command Default

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The IP address of the cluster can be changed, but not deleted. If you connect using the current cluster IP address, that session is lost when the command completes. You must then reconnect using the new IP address.

The **no** form of this command is not allowed.

The cluster configuration submode prompt is (switch(svc-cluster)#).

Examples

The following example enters the cluster configuration mode for SampleCluster, configures the IP address, and verifies by displaying this information

```
switch(svc)# cluster config SampleCluster
switch(svc-cluster)# ip 209.165.200.226
switch(svc)# show cluster SampleCluster ip
cluster ip address is 209.165.200.226
```

Related Commands

Command	Description
show cluster *name* **ip**	Displays configured -- information for a specified cluster.

mdisk-grp

To create and configure a mdsik group, use the **mdisk-grp** command in the cluster configuration submode.

cluster config *cluster-name*
mdisk-grp add *grp-name* **extent** *size*
mdisk-grp name *grp-name* **--> mdisk id** *mdisk-id*

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
mdisk-grp add*grp-name*	Adds a mdisk group.
extent *size*	Assigns the extent size of the storage allocation for MDisks in this cluster. The extent size can be 16, 32, 64, 128, 256, or 512 MB.
mdisk-grp name *grp-name*	Enters the mdisk submode of an existing MDisk group.
mdisk id *mdisk-id*	Assigns the disk ID ranging from 1 to 4096 to the mdisk in the MDisk group submode.

Command Default

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is (switch(svc-cluster)#).

The submode prompt for the MDisk group is switch (svc-cluster-mdisk-grp)#

Examples

The following example enters the cluster configuration mode for SampleCluster, creates an MDisk group, and adds an MDisk to the group.

```
switch(svc)# cluster config SampleCluster
switch(svc-cluster)# mdisk-grp add Mdisk1 extent 512
switch(svc-cluster)# mdisk-grp name Mdisk1
switch(svc-cluster-mdisk-grp)# mdisk id 3
switch(svc)# show cluster SampleCluster mdisk-grp
-------------------------------------------------------------------------------
name             Capacity      free     extent   number    number    status
                                        size(MB) of mdisks of vdisks
-------------------------------------------------------------------------------
finance          7.56 GB       7.56 GB  16       5
        0         online
marketing        6.48 GB       6.48 GB  16       5
         0         online
```

Related Commands

Command	Description
show cluster *name* **mdisk**	Displays configured MDisk group information for a specified cluster.

migrate vdisk

To configure data migration from a VDisk, use the **migrate vdisk** command in the cluster configuration submode.

cluster config *cluster-name*
migrate vdisk *vdisk-name* **new-mdisk-grp** *grp-name*
migrate vdisk *vdisk-name* **src-mdisk id** *mdisk-id* **num-extents** *number* **tgt-mdisk id** *mdisk-id*

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
migrate vdisk *vdisk-name*	Migrates data from the specified VDisk to a MDisk or MDisk group.
new-mdisk-grp *grp-name*	Migrates data to a newly specified MDisk group.
src-mdisk id *mdisk-id*	Specifies the source MDisk for data migration.
num-extents *number*	Specifies the extents of a VDisk for data migration.
tgt-mdisk id *mdisk-id*	Specifies the target MDisk for data migration.

Command Default

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is (switch(svc-cluster)#).

Examples

The following example enters the cluster configuration mode for SampleCluster, migrates a VDisk to a new MDisk group.

```
switch(svc)# cluster config SampleCluster
switch(svc-cluster)# migrate vdisk Vdisk2 new-mdisk-grp Group5
switch(svc-cluster)# migrate vdisk Vdisk2 src-mdisk id 3 num-extents 2 tgt-mdisk id 4
```

Related Commands

Command	Description
show cluster *name* **status migrate**	Displays configured MDisk migration status information for a specified cluster.

node

To add a node to a cluster or to assign a name to a preconfigured node, use the **node** command in the cluster configuration submode.

cluster config *cluster-name*
node name *node-name*
node nwwn *node-wwn*
node iogroup *group-id* [**alias** *alias-name*]

Syntax Description

cluster config	Provides access to cluster commands
node	Adds a specified node to the cluster being configured.
name *node-name*	Specifies the node using a 15 alphanumeric characters.
nwwn *node-wwn*	Specifies the node using the nWWN with the format hh:hh:hh:hh:hh:hh:hh:hh.
iogroup *group-id*	Identifies one of four I/O groups in the specified cluster. The ID ranges from 1 to 4.
alias *alias-name*	Assigns a name to the selected node. The name is restricted to 156 alphanumeric characters.

Command Default

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is (switch(svc-cluster)#).

The node must first be added before assigning an alias name.

The no form of the command deletes the node from the cluster.

Examples

The following example enters the cluster configuration mode for SampleCluster, adds a node by assigning the nWWN, and associates the node with an alias.

```
switch(svc)# cluster config SampleCluster
switch(svc-cluster)# node nwwn 20:00:00:04:cf:e6:e4:df iogroup 1
switch(svc-cluster)# node nwwn 20:00:00:04:cf:e6:e4:df alias NodeAlias
```

Related Commands

Command	Description
show cluster *name* **nodes**	Displays configured node information for a specified cluster.

node svc delete

To delete all cluster configurations from a specific node, use the **node svc delete** command in SVC configuration mode.

node svc *slot-number/node-number* **delete**

Syntax Description

node svc	Specifies the node's SVC interface
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.
delete	Deletes a cluster information from the specified node.

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

Use this command if the node has lost communication with a configured cluster.

Examples

The following example enters the SVC configuration mode and adds a cluster called SampleCluster.

```
switch# svc-config
switch(svc)# node svc 2/1 delete
```

Related Commands

Command	Description
show nodes local	Displays configured node information.

node svc recover

To initiate cluster recovery on a specified SVC node, use the **recover cluster** command in SVC configuration mode.

node svc *slot-number/node-number* **recover**

Syntax Description

node svc	Specifies the node's SVC interface
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.
recover	Initiates recovery for a specified node.

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

Use this command to initiate cluster recovery after a failure. If the output of the **show nodes local** command displays recovery pause in the node status column.

Examples

The following example initiates recovery for the SVC node 1 in slot 2.

```
switch# svc-config
switch(svc)# node svc 2/1 recover
```

Related Commands

Command	Description
show nodes local	Displays configured node information.

node svc servicemode

To place a node in service mode, use the **servicemode node svc** command in SVC configuration mode. Use the **no** form of the command to remove a node from service mode.

node svc *slot-number/node-number* **servicemode**

Syntax Description

node svc	Specifies the node's SVC interface
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.
servicemode	Places a node in service mode.

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example enters the SVC configuration mode and places the specified node in service mode.

```
switch# svc-config
switch(svc)# node svc 2/2 servicemode
```

Related Commands

Command	Description
show nodes local	Displays configured node information.

node svc upgrade

To upgrade the software on a specified SVC node, use the upgrade node svc command in SVC configuration mode.

node svc *slot-number/node-number url* **upgrade svc-system** *url*

Syntax Description

node svc	Specifies the node's SVC interface
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.
upgrade	Upgrades the image on the specified node.
svc-system *url*	Specifies the SVC image to be used. The new version of the software image is specified to the FTP:, SCP:, SFTP:, TFTP:, bootflash:, or slot0: directories

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

This command is valid only if the node is in service mode or the node has been shutdown.

Examples

The following example enters the SVC configuration mode and displays all options in this mode.

```
switch# svc-config
switch(svc)# node svc 2/1 upgrade svc-system ?
  bootflash:  URI containing the system image for SVC
  ftp:        URI containing the system image for SVC
  scp:        URI containing the system image for SVC
  sftp:       URI containing the system image for SVC
  slot0:      URI containing the system image for SVC
  tftp:       URI containing the system image for SVC
```

quorum

To set the quorum disk for a cluster, use the **quorum** command in the cluster configuration submode.

cluster config *cluster-name*
quorum disk [{**1**|**2**|**3**}] **mdisk** *disk-id*

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
quorum disk *id*	Configures one of three quorum disks for the specified cluster. The quorum ID ranges from 1 to 3.
mdisk *mdisk-id*	Specifies the MDisk ID (ranges form 1 to 4096).

Command Default

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is (switch(svc-cluster)#).

You can assign one of 3 possible quorum IDs in any desired order.

Examples

The following example enters the cluster configuration mode for SampleCluster and sets the quorum disk ID.

```
switch(svc)# cluster config SampleCluster
switch(svc-cluster)# quorum disk 2 mdisk 1
```

remote-copy

To create a synchronous copy of a specified VDisk or group of VDisks, use the **remote-copy** command in the cluster configuration submode.

cluster config *cluster-name*
remote-copy add *rcopy-name* [**cluster** *rcluster-name*]
remote-copy *rcopy-name* **map src-vdisk** *vdisk-name* **aux-vdisk** *vdisk-name*

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
remote-copy add *rcopy-name*	Creates a remote copy instance and assigns a name.
remote-copy cluster *rcluster-name*	Specifies the remote cluster name for the consistency group.
remote-copy *rcopy-name*	Enters the remote-copy submode for an existing copy object.
map	Establishes a relationship between the source and destination VDisks.
src-vdisk *vdisk-name*	Specifies the source VDisk for the copy creation.
aux-vdisk *vdisk-name*	Specifies a VDisk in the remote copy cluster.

Command Default

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is (switch(svc-cluster)#).

The remote-copy submode prompt is switch(svc-cluster-remote-copy)#

Examples

The following example enters the cluster configuration mode for SampleCluster and creates a synchronous copy of a specified disk.

```
switch(svc)# cluster config SampleCluster
switch(svc-cluster)# remote-copy add Rcopy1
switch(svc-cluster)# remote-copy r1
switch(svc-cluster-remote-copy)# ?
Submode Commands:
  exit  Exit from this mode
  map   Remote-copy map
  no    Negate a command or set its defaults
switch(svc-cluster-remote-copy)# map src-vdisk SrcVdisk1 aux-vdisk AuxVdisk1
switch(svc-cluster)# remote-copy add Rcopy1 cluster remote-cluster
switch(svc-cluster)# remote-copy name Rcopy1
```

Related Commands

Command	Description
show cluster *name* **remote-copy**	Displays configured remote-copy information for a specified cluster.

show cluster flash-copy

To display configured FlashCopy information for a specified cluster, use the **show cluster** *cluster-name* **flash-copy** command.

show cluster *cluster-name* **flash-copy** [*fcopy-name*]

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
flash-copy *fcopy-name*	Displays FlashCopy relationships configured for the specified FlashCopy object.

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured cluster information.

```
switch(svc)# show cluster SampleCluster flash-copy
--------------------------------------------------------------------------------
name             status
--------------------------------------------------------------------------------
fccstgrp0        idle_or_copied
f2               idle_or_copied
switch(svc)# show cluster SampleCluster flash-copy f2
Flash-copy mapping 1:
    src vdisk is v2
    dest vdisk is v3
    state is idle_or_copied
    copy rate is 50
    progress 0% done
```

show cluster host

To display configured host information for a specific cluster, use the **show cluster** *cluster-name* **host** command.

show cluster *cluster-name* **host** [{*host-name*|**candidate**}]

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
host	Displays information about hosts and host ports.
candidate	Lists all candidates that are not part of this entity but are visible to the cluster.
host-name	Displays information about the specified host.

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured cluster host information.

```
switch(svc)# show SampleCluster host
--------------------------------------------------------------------------------
name             number of ports
--------------------------------------------------------------------------------
oasis15          1
Host1            2
switch(svc)# show SampleCluster host Host1
host Host1:
    Number of port is 2
    Port WWN is 11:22:33:44:aa:bb:cc:dd
    Port WWN is 22:11:33:55:11:aa:bb:cc
 LUN 0:   vdisk V1
 LUN 10: vdisk V2
switch(svc)# show cluster SampleCluster host candidate
--------------------------------------------------------------------------------
id       pwwn
--------------------------------------------------------------------------------
1        21:00:00:e0:8b:09:e7:04
```

show cluster iogroup

To display configured I/O group information for a specified cluster, use the **show cluster** *cluster-name* **iogroup** command.

show cluster *cluster-name* **iogroup** [*group-id*]

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
iogroup	Identifies one of four I/O groups in the specified cluster.
group-id	Specifies the iogroup ID (ranges from 1 to 4).

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured cluster iogroup information.

```
switch(svc)# show SampleCluster iogroup
-------------------------------------------------------------------------------
ID   NAME                              NODE-COUNT       VLUN_COUNT
-------------------------------------------------------------------------------
1    Sampleio1                         2                3
2    io_grp1                           0                0
3    io_grp2                           0                0
4    io_grp3                           0                0
5    recovery_io_grp                   0                0
```

Note Only four IDs can be used, the fifth I/O group is internally created and is only used for cluster recovery.

```
switch(svc)# show SampleCluster iogroup id 2
Io group id 2:
    Node count is 0
    Host LUN count is 0
    Contains no nodes
```

show cluster ip

To displays configured ip information for a specified cluster, use the **show** *cluster-name* **ip** command.

show cluster *cluster-name* **ip**

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
ip	Displays the IP address of the specified cluster.

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example displays configured cluster ip information.

```
switch(svc)# show SampleCluster ip
cluster ip address is 209.165.200.226
```

show cluster mdisk

To display configured MDisk information for a specified cluster, use the **show cluster** *cluster-name* **mdisk** command.

show cluster *cluster-name* **mdisk** {**candidate**|**id** *mdisk-id* **[extent]**}

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
mdisk	Displays MDisk specific information.
candidate	Displays all MDisks that are not assigned to a group.
id *mdisk-id*	Displays details of the specified MDisk ID.
extent	Displays information about the specified MDisk's extent.

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured cluster MDisk information.

```
switch(svc)# show SampleCluster mdisk
------------------------------------------------------------------------------
id       nwwn                   mdisk-grp       capacity      status
------------------------------------------------------------------------------
1        20:00:00:04:cf:e6:1b:5b mg1             68.37 GB      online
2        20:00:00:04:cf:e6:e5:32 mg1             68.37 GB      online
3        20:00:00:04:cf:e6:21:a2 mg1             68.37 GB      online
4        20:00:00:04:cf:e6:e1:81 mg1             68.37 GB      online
5        20:00:00:04:cf:e6:e4:df                 68.37 GB      online
6        20:00:00:04:cf:e6:1c:fb                 68.37 GB      online
7        20:00:00:04:cf:e6:1a:4c                 68.37 GB      online
8        20:00:00:04:cf:e6:e4:6b                 68.37 GB      online
switch(svc)# show SampleCluster mdisk candidate
------------------------------------------------------------------------------
id       nwwn                   capacity
------------------------------------------------------------------------------
5        20:00:00:04:cf:e6:e4:df 68.37 GB
6        20:00:00:04:cf:e6:1c:fb 68.37 GB
7        20:00:00:04:cf:e6:1a:4c 68.37 GB
8        20:00:00:04:cf:e6:e4:6b 68.37 GB
switch(svc)# show cluster SampleCluster mdisk id 1
mdisk id 1 is online
   Is member of mdisk-grp mg1
   Controller node WWN is 20:00:00:04:cf:e6:e4:6b
   Controller port WWN is 22:00:00:04:cf:e6:e4:6b, LUN 00:00:00:00:00:00:00:00
   Controller serial number is 3HZ0KZ8W
```

```
   Capacity is 68.37 GB
   Number of free extents is 2231
switch(svc)# show cluster SampleCluster mdisk id 1 extent
--------------------------------------------------------------------------------
vdisk            number of extents
--------------------------------------------------------------------------------
v1              2144
```

show cluster mdsik-grp

To display configured MDisk group information for a specified cluster, use the **show cluster** *cluster-name* **mdisk-grp** command.

show cluster *cluster-name* **mdisk-grp** [*grp-name*]

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
mdisk-grp *grp-name*	Displays information about a specified MDisk group.

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured cluster information for a MDisk group.

```
switch(svc)# show cluster SampleCluster mdisk-grp
-------------------------------------------------------------------------------------
name    Capacity    free   extent      number       number       status
                                                   size(MB)    of mdisks    of vdisks
-------------------------------------------------------------------------------------
mg1     410.16 GB    309.16 GB   16   6   1    online
switch(svc)# show cluster SampleCluster mdisk-grp mg1
mdisk-grp mg1 is online
   Total capacity is 410.16 GB
   Free capacity is 309.16 GB
   Extent size is 16 MB
   Number of mdisks is 6
   Number of vdisks using this group is 1
```

show cluster nodes

To display configured node information for a specified cluster, use the **show cluster** *cluster-name* **nodes** command.

show cluster *cluster-name* **nodes [candidate]**

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
nodes	Displays information about nodes in this cluster.
candidate	Lists all candidates that are not part of this entity but are visible to the cluster.

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example displays configured cluster information for a specified node.

```
switch(svc)# show cluster SampleCluster nodes
Node node1 is online(3)
    Node WWN is 20:06:00:0b:be:57:73:42
    Serial number is JAB072705JH
    Unique id is 01:00:07:27:30:35:4a:48
    Node is in config mode
    Node is part of iogroup id 1 name io_grp0
Node node2 is online(3)
    Node WWN is 20:08:00:0b:be:57:73:42
    Serial number is JAB076605JH
    Unique id is 01:00:07:66:30:35:4a:48
    Node is in non config mode
    Node is part of iogroup id 1 name io_grp0
switch1(svc)# show cluster SampleCluster nodes candidate
--------------------------------------------------------------------------------
NODE                              NWWN
--------------------------------------------------------------------------------
switch1.2.1                  20:06:00:05:30:00:8d:e0
```

show cluster remote-copy

To display configured remote-copy information for a specified cluster, use the **show cluster** *cluster-name* **remote-copy** command.

show cluster *cluster-name* **remote-copy** [*rcopy-name*]

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
remote-copy	Displays remote copy relationships configured for a specified cluster.
rcopy-name	Displays the specified remote copy object.

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example displays configured cluster information for the specified copy instance.

```
switch(svc)# show cluster SampleCluster remote-copy r1
Remote-copy mapping 1:
    master cluster is SampleCluster
    master vdisk is v6
    aux cluster is c1
    aux vdisk is v7
    status is inconsistent_stopped
    progress 0% done
Remote-copy mapping 2:
    master cluster is SampleCluster
    master vdisk is v8
    aux cluster is c1
    aux vdisk is v9
    status is inconsistent_stopped
    progress 0% done
```

show cluster remote-copy-cluster

To display configured remote-copy partnership information for a specified cluster, use the **show cluster** *cluster-name* **remote-copy-cluster** command.

show cluster *cluster-name* **remote-copy-cluster** [*rcopy-name*]

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
remote-copy-cluster	Displays remote copy relationships configured for a specified cluster.
rcopy-name	Displays the specified remote copy object.

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example displays configured cluster information for the specified copy instance.

```
switch(svc)# show cluster SampleCluster remote-copy-cluster
-------------------------------------------------
Cluster          Local/remote     Bandwidth
-------------------------------------------------
local-cluster    local             10
remote-cluster   remote            50
```

show cluster status

To displays progress information for a specified cluster, use the **show cluster** *cluster-name* **status** command.

show cluster *cluster-name* **status** [{**flash-copy** *fcopy-name*|**remote-copy** *rcopy-name*}]

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
status	Displays the status of a upgrade or copy process.
flash-copy	Displays FlashCopy relationships configured for the specified cluster.
fcopy-name	Displays the specified FlashCopy object.
remote-copy	Displays remote copy relationships configured for a specified cluster.
rcopy-name	Displays the specified remote copy object.

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured cluster information.

```
switch(svc)# show cluster SampleCluster status flash-copy fc1
--------------------------------------------------------------------------------
src vdisk        dest vdisk       progress
--------------------------------------------------------------------------------
v1               v2               100% done
v3               v4               100% done
switch(svc)# show cluster SampleCluster status remote-copy rc1
--------------------------------------------------------------------------------
src vdisk        aux vdisk        progress
--------------------------------------------------------------------------------
v5               v6               100% done
v7               v8               100% done
```

show cluster vdisk

To display configured VDisk information for a specified cluster, use the **show cluster** *cluster-name* **vdisk** command.

show cluster *cluster-name* **vdisk** *vdisk-id* [{**extent**|**mapped_hosts**}]

Syntax Description

show cluster *cluster-name*	Specifies a previously created cluster name.
vdisk	Displays configured VDisks in the cluster
vdisk-id	Displays details of the specified VDisk ID.
extent	Displays information about the specified MDisk's extent.
mapped_hosts	Displays information about which hosts are mapped to the specified VDisk.

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured cluster information for VDisks.

```
switch(svc)# show cluster SampleCluster vdisk v1 extent
--------------------------------------------------------------------------------
mdisk id  number of extents
--------------------------------------------------------------------------------
1         2144
2         2144
3         2144
5         11
6         11
7         10
switch(svc)# show cluster SampleCluster vdisk v1 mapped_hosts
--------------------------------------------------------------------------------
host             LUN
--------------------------------------------------------------------------------
oasis15          0
```

show environment battery

To display status of a battery module for the Caching Services Module (CSM), use the **show environment battery** command.

show environment battery module *slot-number* **[detail]**

Syntax Description

show environment	Displays the hardware environment in any Cisco MDS 9000 Family switch.
battery	Displays the status of the battery in a CSM.
module *slot-number*	Specifies the slot number of the CSM.
detail	Provides detailed information about the CSM battery status.

Command Default

None.

Command Modes

EXEC mode.

Command History

This command was modified in Release 1.3(1).

Usage Guidelines

None.

Examples

The following example displays the current contents of the boot variable.

```
switch# show environment battery module 2
Battery 1:
----------
Voltage             : 10.343 V
Current             : 0.000 A
Temperature         : 23.7 C
Current Capacity    : 1571 mAHr
Full Capacity       : 2057 mAHr
CySampleClustere Count         : 3
Last conditioned in : Week 22 2003
Serial Num          : AMB0722009C
Battery 2:
----------
Voltage             : 10.596 V
Current             : 0.000 A
Temperature         : 26.6 C
Current Capacity    : 1701 mAHr
Full Capacity       : 2032 mAHr
CySampleClustere Count         : 6
Last conditioned in : Week 22 2003
Serial Num          : AMB0722009R
switch## show environment battery module 2 detail
Battery 1:
----------
Voltage             : 10.338 V
Current             : 0.000 A
Temperature         : 23.7 C
Current Capacity    : 1571 mAHr
```

```
Full Capacity       : 2057 mAHr
Caching Capacity    : 6463 MB
CySampleClustere Count         : 3
Last conditioned in : Week 22 2003
Serial Num          : AMB0722009C
EEPROM version      : 1
Manufacturer Access            : 0x0
Remaining Capacity Alarm       : 0xc8
Remaining Time Alarm           : 0xa
Battery Mode                   : 0x6000
AtRate                         : 0x0
AtRate Time To Full            : 0xffff
AtRate Time To Empty           : 0xffff
AtRate OK                      : 0x1
Temperature                    : 0xb97
Voltage                        : 0x2862
Current                        : 0xd
Average Current                : 0x6
Max Error                      : 0x2
Relative State of Charge       : 0x4c
Absolute State of Charge       : 0x4f
Remaining Capacity             : 0x623
Full Charge Capacity           : 0x809
Run Time To Empty              : 0xffff
Average Time To Empty          : 0xffff
Average Time To Full           : 0x13f2
Charging Current               : 0x44c
Charging Voltage               : 0x3840
Battery Status                 : 0xc0
CySampleClustere Count                    : 0x3
Design Capacity                : 0x7d0
Design Voltage                 : 0x2580
Specification Info             : 0x21
Manufacture Date               : 0x3037
Serial Number                  : 0x0
Manufacturer Name              : 0x430a
Device Name                    : 0x4207
Device Chemistry               : 0x4e04
Manufacturer Data              : 0x7507
Pack Status & Configuration    : 0x2020
VCELL4                         : 0x0
VCELL3                         : 0x0
VCELL2                         : 0x0
VCELL1                         : 0x0
...
```

show interface svc

You can check the status of a SVC interface at any time by using the show interface svc command.

show interface svc *slot-number/node-number* [**brief | counters | description**]

Syntax Description

interface range	Displays the interfaces in the specified range.
brief	Displays brief info of interface.
counters	Displays the interface counter information.
description	Displays a description of interface.
svc	Displays the SAN Volume Controller (SVC) interface.
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.

Command Default

None

Command Modes

EXEC

Command History

This command was modified in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured SVC interface information.

```
switch# show interface svc 2/1
svc2/1 is up
    Node WWN is 10:00:00:00:00:00:00:00
    Fabric WWN is 20:41:00:05:30:00:33:1e
    Target N-port WWN is 27:39:00:05:30:00:33:2a, vsan is 1, FCID is 0x010006
    Initiator N-port WWN is 27:3a:00:05:30:00:33:2a, vsan is 1, FCID is 0x010007
    Mgmt N-port WWN is 27:3b:00:05:30:00:33:2a, vsan is 1, FCID is 0x010008
    5 minutes input rate 16 bits/sec, 2 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      7 frames input, 736 bytes
        0 discards, 0 errors
      3 frames output, 276 bytes
        0 discards, 0 errors
switch# show interface svc 8/1-2
svc8/1 is down (Administratively down)
    Node WWN is 23:34:00:05:30:00:00:02
    Fabric WWN is 21:c1:00:05:30:00:00:00
    Target N-port WWN is 23:2e:00:05:30:00:00:02, vsan is 1, FCID is 0x000000
    Initiator N-port WWN is 23:2f:00:05:30:00:00:02, vsan is 1, FCID is 0x000000
    Mgmt N-port WWN is 23:30:00:05:30:00:00:02, vsan is 1, FCID is 0x000000
```

```
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      0 frames input, 0 bytes
        0 discards, 0 errors
      0 frames output, 0 bytes
        0 discards, 0 errors
svc8/2 is up
    Node WWN is 23:35:00:05:30:00:00:02
    Fabric WWN is 21:c2:00:05:30:00:00:00
    Target N-port WWN is 23:31:00:05:30:00:00:02, vsan is 1, FCID is 0x650003
    Initiator N-port WWN is 23:32:00:05:30:00:00:02, vsan is 1, FCID is 0x650004
    Mgmt N-port WWN is 23:33:00:05:30:00:00:02, vsan is 1, FCID is 0x650005
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      3268061 frames input, 6602103068 bytes
        0 discards, 2 errors
      3208131 frames output, 6598470800 bytes
        0 discards, 0 errors
switch# show interface brief
--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          FCOT   Oper  Oper   Port
                  Mode   Trunk                         Mode  Speed  Channel
                         Mode                                (Gbps)
--------------------------------------------------------------------------------
fc8/1      1      FX     --      fcotAbsent       --     --           --
...
fc8/32     1      FX     --      fcotAbsent       --     --           --
--------------------------------------------------------------------------------
Interface          Status                          Speed
                                                   (Gbps)
--------------------------------------------------------------------------------
sup-fc0            up                              1
--------------------------------------------------------------------------------
Interface               Status     IP Address        Speed        MTU
--------------------------------------------------------------------------------
mgmt0                   up         172.22.90.21/24   100 Mbps     1500
--------------------------------------------------------------------------------
Interface          Status
--------------------------------------------------------------------------------
svc2/1             down
svc2/2             up
svc4/1             up
svc4/2             up
switch# show interface svc 2/1 counters
svc2/1
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec 0 ios/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec 0 ios/sec
    272 frames input, 89764 bytes
      39 input session management frames
        19 plogi, 1 plogi_acc, 13 prli, 1 prli_acc
        2 logo, 0 logo_acc, 0 prlo, 0 prlo_acc
        3 abts, 0 ba_acc, 0 ls_rjt
      28 input I/Os, 28 cmd complete, 0 cmd fail
        24 reads, 4 writes
        0 input errors
        0 input discards
          FCP cmd errors
            0 sess not up, 0 no resources, 0 bad frames
            0 up layer rjt, 0 out of order, 0 proc unexp exch st
            0 drop unexp exch st, 0 no exch match
          FCP Xrdy errors
            0 sess not up, 0 no resources, 0 bad frames
            0 up layer rjt, 0 out of order, 0 proc unexp exch st
            0 drop unexp exch st, 0 no exch match
```

```
          FCP status errors
            0 sess not up, 0 no resources, 0 bad frames
            0 up layer rjt, 0 out of order, 0 proc unexp exch st
            0 drop unexp exch st, 0 no exch match
          FCP Data errors
            0 sess not up, 0 no resources, 0 bad frames
            0 up layer rjt, 0 out of order, 0 proc unexp exch st
            0 drop unexp exch st, 0 no exch match
          0 Incoming Aborts
    232 frames output, 84176 bytes
      35 output session management frames
        6 plogi, 13 plogi_acc, 1 prli, 12 prli_acc
        0 logo, 0 logo_acc, 0 prlo, 0 prlo_acc
        1 abts, 2 ba_acc, 0 ls_rjt
      103 out I/Os, 103 cmd complete, 0 cmd fail
        63 reads, 4 writes
      0 output errors
      0 output discards
        0 out ls aborts
           LS requests while sess not up
             0 cmds 0 data xfers 0 status xfers 0 ds xfers
switch# show interface svc 4/2 description
--------------------------------------------------------------------------------
Interface          Description
--------------------------------------------------------------------------------
svc4/2             SampleInt1
```

show nodes

To displays configured information for the CSM, use the **show svc** command.

show nodes {**local [detail]** | **svc** *slot_number/node-number* | **version**}

Syntax Description

nodes show nodes	Displays information about the specified nodes.
local	Displays SVC nodes in the switch.
detail	Displays detailed node information.
svc	Displays node information specific to the SVC interface.
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.
version	Displays software version information for each node.

Command Default

None.

Command Modes

SVC configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example display configured SVC information and statistics.

```
switch(svc)# show nodes local detail
svc2/1:
  Is a config node for cluster SampleCluster
  cluster Status is active
  Node Status is active
svc2/2:
  Is member of cluster SampleCluster
  cluster Status is active
  Node Status is active
switch(svc)# show nodes ?
  local    Show nodes in the switch
  svc      SVC Interface
  version  Show node sw versions in the switch
  <cr>     Carriage Return
switch(svc)# show nodes svc 2/2
svc2/2:
  Is not a member of any cluster
  Cluster Status is unconfigured
  Node Status is free
switch(svc)# show nodes version
-------------------------------------------------------
```

```
Node              sw version       state
----------------------------------------------------------
svc2/1            1.3(1)       Runtime code    (5)
svc2/2            1.3(1)       Runtime code    (5)
```

Related Commands

Command	Description
svc config	Configures SVC nodes.

show svc

To displays configured information for the CSM, use the **show svc** command.

show svc port svc *slot_number/node-number* [**detail** | **initiator** | **mgmt** | **target** [**detail** | **vsan** *vsan-id*]] | **session** [**detail** | **initiator** | **mgmt** | **peer-wwn** *pwwn-id* | **target** [**detail** | **vsan** *vsan-id*]] | **stats xipc**[**interface svc** *slot_number/node-number*]| [**module** *slot-number*]

Syntax Description

show svc	Displays configured SVC information.
port	Displays N-port specific SVC information.
svc	Specifies the new interface to be a SVC interface.
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.
detail	Displays detailed information for all N ports
initiator	Displays a SVC node as an initiator in the specified VSAN.
mgmt	Displays a SVC node as a management node in the specified VSAN.
target	Displays a SVC node as a target in the specified VSAN.
vsan*vsan-id*	Specifies the VSAN ID ranging from 1 to 4093.
session	Displays information specific to the SVC session.
peer-pwwn pwwn-id	Specifies the port WWN of the target or host, with the format hh:hh:hh:hh:hh:hh:hh:hh.
stats	Displays SVC statistical information generally used for debugging.
module *slot-number*	Specifies the slot number containing the CSM.

Command Default

None.

Command Modes

EXEC mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following examples display configured SVC information and statistics.

```
switch# show svc session svc 2/1
svc2/1:
   Target N-port WWN is 21:00:00:05:30:00:8d:e0, vsan is 2, FCID is 0x610100
```

```
    pWWN 21:00:00:e0:8b:09:f0:04, nWWN 20:00:00:e0:8b:09:f0:04, FCID 0x610000
  Initiator N-port WWN is 20:01:00:05:30:00:8d:e0, vsan is 1, FCID is 0xec0100
    pWWN 22:00:00:04:cf:e6:e4:6b, nWWN 20:00:00:04:cf:e6:e4:6b, FCID 0xec00d4
    pWWN 22:00:00:04:cf:e6:1a:4c, nWWN 20:00:00:04:cf:e6:1a:4c, FCID 0xec00d5
    pWWN 22:00:00:04:cf:e6:1c:fb, nWWN 20:00:00:04:cf:e6:1c:fb, FCID 0xec00d6
    pWWN 22:00:00:04:cf:e6:e1:81, nWWN 20:00:00:04:cf:e6:e1:81, FCID 0xec00d9
    pWWN 22:00:00:04:cf:e6:e4:df, nWWN 20:00:00:04:cf:e6:e4:df, FCID 0xec00da
    pWWN 22:00:00:04:cf:e6:21:a2, nWWN 20:00:00:04:cf:e6:21:a2, FCID 0xec00dc
    pWWN 22:00:00:04:cf:e6:e5:32, nWWN 20:00:00:04:cf:e6:e5:32, FCID 0xec00e0
    pWWN 22:00:00:04:cf:e6:1b:5b, nWWN 20:00:00:04:cf:e6:1b:5b, FCID 0xec00e1
  Mgmt N-port WWN is 21:02:00:05:30:00:8d:e0, vsan is 3, FCID is 0x7a0000
    pWWN 21:03:00:05:30:00:8d:e0, nWWN 20:07:00:05:30:00:8d:e0, FCID 0x7a0001
switch# show svc session svc 2/1 peer-pwwn 22:00:00:04:cf:e6:e4:6b detail
svc2/1:
   Initiator N-port WWN is 20:01:00:05:30:00:8d:e0, vsan is 1, FCID is 0xec0102
     pWWN 22:00:00:04:cf:e6:e4:6b, nWWN 20:00:00:04:cf:e6:e4:6b, FCID 0xec00d4
       47 frames input, 920 data bytes
         2 ELS pkts, 0 BLS pkts
         0 FCP commands, 0 FCP xfer ready
         20 FCP data frames, 25 FCP status
         0 FCP overrun, 15 FCP underrun
         0 aborts, 0 bad FC2 drops
         0 data excess
       27 frames output, 0 data bytes
         2 ELS pkts, 0 BLS pkts
         25 FCP commands, 0 FCP xfer ready
         0 FCP data frames, 0 FCP status
         0 aborts
       0 open exchanges
switch#  show svc port svc 2/1
svc2/1:
   Target N-port in vsan 2 is up
     Port WWN is 21:00:00:05:30:00:8d:e0, FCID is 0x610101
   Initiator N-port in vsan 1 is up
     Port WWN is 20:01:00:05:30:00:8d:e0, FCID is 0xec0102
   Mgmt N-port in vsan 1 is up
     Port WWN is 20:02:00:05:30:00:8d:e0, FCID is 0xec0103
switch# show svc port svc 2/1 target detail
svc2/1:
   Target N-port in vsan 1 is up
     Port WWN is 27:39:00:05:30:00:33:2a, FCID is 0x010006
     0 sessions, 0 closed, 0 in transition
       5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec 0 ios/sec
       5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec 0 ios/sec
     9 frames input, 1064 bytes
       0 input session management frames
         0 plogi, 0 prli
         0 logo, 0 logo_acc
         0 prlo, 0 prlo_acc
         0 abts, 0 ls_rjt
       0 input I/Os, 0 cmd complete, 0 cmd fail
         0 reads, 0 writes
       0 input errors
       0 input discards
     5 frames output, 388 bytes
       0 output session management frames
         0 plogi_acc, 0 prli_acc
         0 logo, 0 logo_acc
         0 prlo, 0 prlo_acc
         0 ba_acc, 0 ls_rjt
       0 output I/Os, 0 cmd complete, 0 cmd fail
       0 output errors
       0 output discards
switch# show svc session svc 2/1 peer-pwwn 27:46:00:05:30:00:33:2a detail
```

```
svc2/1:
    Mgmt N-port WWN is 27:3b:00:05:30:00:33:2a, vsan is 1, FCID is 0x010008
      pWWN 27:46:00:05:30:00:33:2a, nWWN 27:48:00:05:30:00:33:2a, FCID 0x010011
        19 frames input, 16517 data bytes
          2 ELS pkts, 0 BLS pkts
          3 FCP commands, 1 FCP xfer ready
          10 FCP data frames, 3 FCP status
          0 FCP overrun, 2 FCP underrun
          0 aborts, 0 bad FC2 drops
          0 data excess
        19 frames output, 16520 data bytes
          2 ELS pkts, 0 BLS pkts
          3 FCP commands, 1 FCP xfer ready
          10 FCP data frames, 3 FCP status
          0 aborts
        0 open exchanges
        FCP Error Stats
          FCP cmd errors
            0 sess not up, 0 no resources, 0 bad frames
            0 up layer rjt, 0 out of order, 0 proc unexp exch st
            0 drop unexp exch st, 0 no exch match
          FCP Xfer Rdy errors
            0 sess not up, 0 no resources, 0 bad frames
            0 up layer rjt, 0 out of order, 0 proc unexp exch st
            0 drop unexp exch st, 0 no exch match
          FCP Status errors
            0 sess not up, 0 no resources, 0 bad frames
            0 up layer rjt, 0 out of order, 0 proc unexp exch st
            0 drop unexp exch st, 0 no exch match
          FCP Data errors
            0 sess not up, 0 no resources, 0 bad frames
            0 up layer rjt, 0 out of order, 0 proc unexp exch st
            0 drop unexp exch st, 0 no exch match
```

svc-config

To perform SAN Volume Controller (SVC) configurations, use the **svc-config** command.

svc-config

Syntax Description

svc-config	Enters the SVC configuration mode.
cluster	Provides access to cluster commands.
node	Provides access to node commands.
show	Displays configured SVC information for the specified node.

Command Default

None.

Command Modes

EXEC mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

None.

Examples

The following example enters the SVC configuration mode and displays all options in this mode.

```
switch# svc-config
switch-sw6(svc)# ?
Submode Commands:
  cluster  Cluster commands
  exit     Exit from this mode
  no       Negate a command or set its defaults
  node     Node commands
  show     Show
```

svc-ibmcli

To perform SAN Volume Controller (SVC) configurations by using IBM's CLI, use the **svc-ibmcli** command.

svc-ibmcli { **cluster-name** *cluster-name* [*IBM-CLI-command*] | **node svc** *slot-number/node-number* [*IBM-CLI-command*] }

Syntax Description

svc-ibmcli	Enters the IBM CLI configuration mode.
cluster-name	Specifies a new cluster.
cluster-name	Specifies a cluster name.
node svc	Specifies a node in the SVC interface.
slot-number	Specifies the slot number of the Caching Service Module (CSM).
node-number	Specifies the node number of the SVC instance running on the CSM. This number ranges from 1 to 2 nodes per module.
IBM-CLI-command	Specifies the IBM TotalStorage command to be executed

Command Default

None.

Command Modes

EXEC mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

When you enter the IBM TotalStorage shell, all future commands are interpreted directly by this shell. Type **exit** to return to the Cisco MDS switch prompt.

Examples

The following example enters the SVC configuration mode and displays all options in this mode.

```
switch# svc-ibmcli cluster-name SampleCluster
Attaching to config node for cluster SampleCluster
To exit type 'exit', to abort type '$.'
IBM_svc:admin>
switch# svc-ibmcli node svc 2/1
Attaching to node 2/1
To exit type 'exit', to abort type '$.'
IBM_svc:admin>
```

svc-purge-wwn module

To remove all configured WWNs for the CSM from the running configuration, use the **svc-purge-wwn module** command.

svc-purge-wwn module *module-number*

Syntax Description

svc-purge-wwn	Purges the WWN for the CSM.
module *module-number*	Specifies the slot number for the CSM.

Command Default

None.

Command Modes

EXEC mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

This command also purges all system allocated pWWNs and nWWNs from the system and will never be used again (by the system or by SVC interfaces). New system values will be allocated for all pWWN/nWWNs for the module.

Examples

The following example enters the SVC configuration mode and displays all options in this mode.

```
switch# svc purge-wwn module 2
!!!WARNING!  This command will purge all SVC system allocated
    WWNs for the specified module.  These WWNs will be lost.
    All user configured WWNs will be removed from the
    running-config, but not from the startup-config.
This operation can take a long time.  Other CLI commands
    on the system may be stopped while this operation is
    in progress.
Are you sure you want to do this? [Y/N] [N] y
switch#
```

vdisk

To create a new VDisk or access a new VDisk, use the **vdisk** command in the cluster configuration submode.

cluster config *cluster-name*
{**vdisk add** *vdisk-name* **iogroup** *group-id* **mdisk-grp** *grp-name* **capacity** *number*|**import** [{**clean**|**mdisk-list**|**preferred-node**|**sequential**}]}
vdisk name *vdisk-name* **-> expand** [**capacity | extent mdisk** *disk-id* **offset** *number*] | **io-throttle** *number* [**MB**] | **iogroup | shrink**

Syntax Description

cluster	Provides access to cluster commands
config *cluster-name*	Places a previously created cluster in the cluster configuration submode.
vdisk add *vdisk-name*	Creates a VDisk of the specified name.
iogroup *group-id*	Identifies one of four I/O groups in the specified cluster. The ID ranges from 1 to 4. The I/O for the VDisk is serviced by node belonging to that I/O group.
mdisk-grp*grp-name*	Specifies an existing MDisk group from which the VDisk storage originates.
capacity	Configures the size of this VDisk.
number	Provides a range from 0- 1677215 Gigabytes.
import	Imports a previously unmanaged disk that contains SVC virtualization data.
clean	Clears all data in the VDisk.
mdisk-list	Specifies a list of MDisks. All disks in this list must be part of the MDisk group
preferred-node	specifies the preferred node within the two nodes in this group to send I/Os for this VDisk
sequential	Specifies a sequential virtualization policy. If this option is not specified, the striped (default) virtualization policy is used.
vdisk *vdisk-name*	Enters the VDisk submode of an existing VDisk.
expand capacity	Expands the MDisk capacity.
extent	Expands the MDisk by a single extent.
offset*number*	Offsets the extent.
io-throttle	Limits the amount of I/Os allowed for this VDisk. If MB is not specified, the unit is calculated in I/Os per second.
MB	Specifies the I/O throttling in Megabytes.
shrink	Shrinks the capacity of the VDisk as specified.

Command Default

None.

Command Modes

SVC configuration mode—cluster configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

The cluster configuration submode prompt is (switch(svc-cluster)#).

The VDisk submode prompt is switch (svc-cluster-vdisk)#

Extents are allowed from all MDisks in the list

Examples

The following example enters the cluster configuration mode for SampleCluster and ---

```
switch(svc)# cluster config SampleCluster
switch(svc-cluster)# vdisk add Vdisk1 iogroup 1 mdisk-grp Mdisk1 ?
  capacity  Vdisk add name iogroup mdisk-grp
  import    Vdisk add import
switch(svc-cluster)# vdisk add Vdisk1 iogroup 1 mdisk-grp Mdisk1 capacity ?
  <0-2147483647>  Enter the capacity
switch(svc-cluster)# vdisk add Vdisk1 iogroup 1 mdisk-grp Mdisk1 capacity 5000 ?
  gb  Vdisk add name iogroup mdisk-grp capacity
  mb  Vdisk add name iogroup mdisk-grp capacity
  pb  Vdisk add name iogroup mdisk-grp capacity
  tb  Vdisk add name iogroup mdisk-grp capacity
switch(svc-cluster)# vdisk add Vdisk1 iogroup 1 mdisk-grp Mdisk1 capacity 5000 gb ?
  clean           Vdisk add clean
  mdisk-list      Vdisk add mdisk-list
  preferred-node  Vdisk add sequential mdisk
  sequential      Vdisk add sequential
  <cr>            Carriage Return
switch(svc-cluster)# vdisk add VDISK1 iogroup 1 mdisk-grp Mdisk1 capacity 0 gb
switch(svc-cluster)# vdisk VDISK1
switch(svc-cluster-vdisk)# ?
Submode Commands:
  exit         Exit from this mode
  expand       Expand
  io-throttle  Io throttle
  iogroup      Move vdisk to iogroup
  no           Negate a command or set its defaults
  shrink       Shrink capacity
switch(svc-cluster-vdisk)# expand ?
  capacity  Expand capacity
  extent    Expand extent
switch(svc-cluster-vdisk)# io-throttle 0
switch(svc-cluster-vdisk)# shrink capacity 1 ?
  gb  Expand capacity
  mb  Expand capacity
  pb  Expand capacity
  tb  Expand capacity
switch(svc-cluster-vdisk)# exit
switch(svc)# show cluster SampleCluster vdisk
--------------------------------------------------------------------------------
name             capacity     iogroup mdisk-grp name    policy      status
--------------------------------------------------------------------------------
Vdisk1           100.00 GB    1       Group1            striped     online
Vdisk2           50.00 GB     1       Group2            striped     online
switch(svc)# show cluster SampleCluster vdisk Vdisk1
vdisk Vdisk1 is online
```

```
    Capacity is 100.00 GB
    Using storage from mdisk-grp Group1
    Processed by io group 1
    Virtualization policy is striped
    Preferred node is 2
switch(svc)# show cluster SampleCluster vdisk Vdisk1 extent
------------------------------------------------------------------------------
mdisk id  number of extents
------------------------------------------------------------------------------
1         2134
2         2133
3         2133
switch(svc)# show cluster SampleCluster vdisk Vdisk1 mapped_hosts
------------------------------------------------------------------------------
host             LUN
------------------------------------------------------------------------------
Host1            0
```

Related Commands

Command	Description
show cluster *name* **vdisk**	Displays configured vdisk information for a specified cluster.

D Commands

data-pattern-file

To configure data pattern file for a SAN tuner extension N port, use the **data-pattern-file** command in interface configuration submode. To remove data pattern file, use the **no** form of the command.

data-pattern-file *filename*
no data-pattern-file

Syntax Description

filename	Specifies the data pattern file name.

Command Default

All zero pattern.

Command Modes

SAN extension N port configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

By default, an all-zero pattern is used as the pattern for data generated by the virtual N ports. You can optionally specify a file as the data pattern to be generated by selecting a data pattern file from one of three locations: the bootflash: directory, the volatile: directory, or the slot0: directory. This option is especially useful when testing compression over FCIP links. You can also use Canterbury corpus or artificial corpus files for benchmarking purposes.

Examples

The following example configures the data pattern file for an 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)# data-pattern-file bootflash://DataPatternFile
```

Related Commands

Command	Description
nport pwwn	Configures SAN extension tuner N port pWWNs.
san-ext-tuner	Enters SAN extension tuner configuration mode.
show san-ext-tuner	Displays SAN extension tuner information.

deadtime (radius group configuration)

To configure a periodic time interval where a nonreachable (non-responsive) RADIUS server is monitored for responsiveness, use the **deadtime** command in RADIUS group configuration submode. To disable the monitoring of the non-responsive server, use the **no** form of the command.

deadtime *time*
no deadtime *time*

Syntax Description

time	Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.

Command Default

Zero.

Command Modes

RADIUS group configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

If the dead time interval for an individual RADIUS server is greater than zero (0), that value takes precedence over the value set for the server group.

When the dead time interval is 0 minutes, RADIUS server monitoring is not performed unless the RADIUS server is part of a server group and the dead time interval for the group is greater than 0 minutes.

Examples

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

```
switch# config terminal
switch(config)# aaa group server radius testgroup
switch(config-radius)# deadtime 10
```

Related Commands

Command	Description
radius-server deadtime	Sets a time interval for monitoring a nonresponsive RADIUS server.
show radius-server	Displays RADIUS server information.

deadtime (tacacs+ group configuration)

To configure a periodic time interval where a non-reachable (non responsive) TACACS+ server is monitored for responsiveness, use the **deadtime** command in TACACS+ group configuration submode. To disable the monitoring of the non responsive server, use the **no** form of the command.

deadtime *time*
no deadtime *time*

Syntax Description

time	Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.

Command Default

Zero.

Command Modes

TACACS+ group configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

If the dead time interval for an individual TACACS+ server is greater than zero (0), that value takes precedence over the value set for the server group.

When the dead time interval is 0 minutes, TACACS+ server monitoring is not performed unless the TACACS+ server is part of a server group and the dead time interval for the group is greater than 0 minutes.

Examples

The following example shows the **deadtime** command in TACACS+ group configuration submode:

```
switch# config terminal
switch(config)# aaa group server tacacs mygroup
switch(config-tacacs)# deadtime 5
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
tacacs-server deadtime	Sets a time interval for monitoring a nonresponsive TACACS+ server.

deadtime (server group configuration mode)

To configure deadtime within the context of LDAP server groups, use the **deadtime** command in server group configuration mode. To disable this feature, use the no form of the command.

deadtime *minutes*
no deadtime *minutes*

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Server group configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure deadtime within the context of LDAP server groups:

```
switch(config-ldap)# deadtime minutes
switch(config-ldap)#
```

Related Commands

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

delete

To delete a specified file or directory on a flash memory device, use the **delete** command in EXEC mode.

delete
{**bootflash :** *filename*|**debug :** *filename*|**log :** *filename*|**modflash :** *filename*|**slot0 :** *filename*|**volatile :** *filename*}

Syntax Description

bootflash:	Flash image that resides on the supervisor module.
filename	The name of the file to be deleted.
debug:	Contains the debug files.
log:	Contains the two default logfiles. The file dmesg contains the kernel log-messages and the file messages contains the system application log-messages.
modflash:	Flash image that resides on a module.
slot0:	Flash image that resides on another module.
volatile:	Flash image that resides on the volatile file system.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2	This command was introduced.
2.1(1a)	Added debug, log, and modflash keywords.

Usage Guidelines

When you delete a file, the software erases the file.

If you attempt to delete the configuration file or image specified by the CONFIG_FILE or BOOTLDR environment variable, the system prompts you to confirm the deletion. Also, if you attempt to delete the last valid system image specified in the BOOT environment variable, the system prompts you to confirm the deletion.

Caution If you specify a directory, the **delete** command deletes the entire directory and all its contents.

Examples

The following example deletes the file named test from the flash card inserted in slot 0:

```
switch# delete slot0:test
Delete slot0:test? [confirm]
```

The following example deletes a file from a directory:

```
switch# delete dns_config.cfg
```

The following example deletes a file from an external CompactFlash (slot0):

```
switch# delete slot0:dns_config.cfg
```

The following example deletes the entire m y-dir directory and all its contents:

```
switch# delete bootflash:my-dir
```

The following example deletes the entire user created d k log file on the active supervisor:

```
switch# delete log://sup-active/
log://sup-active/dk        log://sup-active/dmesg     log://sup-active/messages
switch# delete log://sup-active/dk
switch# dir log:
         31     Feb 04 18:22:03 2005  dmesg
      14223     Feb 04 18:25:30 2005  messages
Usage for log://sup-local
   35393536 bytes used
  174321664 bytes free
  209715200 bytes total
switch#
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
dir	Displays a list of files on a file system.
show boot	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.

delete ca-certificate

To delete certificate authority certificates, use the **delete ca-certificate** command in trust point configuration submode.

delete ca-certificate

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Trust point configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command deletes the CA certificate or certificate chain corresponding to the trust point CA. As a result, the trust point CA is no longer trusted. If there is an identity certificate form the CA, you should delete it before attempting to delete the CA certificate. Doing so prevents the accidental deletion of a CA certificate when you have not yet deleted the identity certificate from that CA. This action may be necessary when you do not want to trust the CA any more for a reason such as the CA is compromised or the CA certificate is already expired, with the latter being a very rare event.

Note The trust point configuration, certificates, and key pair configurations are made persistent only after saving to the startup configuration. To be consistent with this configuration behavior, the delete behavior is also the same. That is, the deletions are made persistent only after saving to the startup configuration. Use the **copy running-config startup-config** command to make the certificate and key pair deletions persistent.

Examples

The following example shows how to delete a certificate authority certificate:

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete ca-certificate
```

Related Commands

Command	Description
delete certificate	Deletes the identity certificate.
delete crl	Deletes the crl from the trustpoint.

delete certificate

To delete the identity certificate, use the **delete certificate** command in trust point configuration submode.

delete certificate [force]

Syntax Description

force	(Optional) Forces the deletion of the identity certificate.

Command Default

None.

Command Modes

Trust point configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Use this command to delete the identity certificate from the trust point CA. This action may be necessary when the identity certificate expires or the corresponding key pair is compromised. Applications will be left without any identity certificate to use after the deletion of the last or the only identity certificate present. Accordingly, an error message is generated if the certificate being deleted is the last or only identity certificate present. If needed, the deletion can still be accomplished by forcing it using the force option.

Note The trust point configuration, certificates, and key pair configurations are made persistent only after saving to the startup configuration. To be consistent with this configuration behavior, the delete behavior is also the same. That is, the deletions are made persistent only after saving to the startup configuration. Use the **copy running-config startup-config** command to make the certificate and key pair deletions persistent.

Examples

The following example shows how to delete the identity certificate:

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete certificate
```

The following example shows how to force the deletion of the identity certificate:

```
switch(config-trustpoint)# delete certificate force
```

Related Commands

Command	Description
delete ca-certificate	Deletes the certificate authority certificate.
delete crl	Deletes the crl from the trustpoint.

delete crl

To delete the crl from the trustpoint, use the **delete crl** command in trust point configuration submode.

delete crl

Syntax Description

This command has no argument or keywords.

Command Default

None.

Command Modes

Trust point configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to delete the crl from the trustpoint:

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete crl
```

Related Commands

Command	Description
delete ca-certificate	Deletes the certificate authority certificate.
delete certificate	Deletes the identity certificate.

deny (IPv6-ACL configuration)

To configure deny conditions for an IPv6 access control list (ACL), use the deny command in IPv6-ACL configuration submode. To remove the conditions, use the **no** form of the command.

deny {*ipv6-protocol-number*|**ipv6**} {*source-ipv6-prefix/prefix-length*|**any**|**host** *source-ipv6-address*} {*dest-ipv6-prefix/prefix-length*|**any**|**host** *dest-ipv6-address*} **[log-deny]**
deny icmp {*source-ipv6-prefix/prefix-length*|**any**|**host** *source-ipv6-address*} {*dest-ipv6-prefix/prefix-length*|**any**|**host** *dest-ipv6-address*} [*icmp-type* [*icmp-code*]] **[log-deny]**
deny tcp {*source-ipv6-prefix/prefix-length*|**any**|**host** *source-ipv6-address*} [{*source-port-operator source-port-number*|**range** *source-port-number source-port-number*}] {*dest-ipv6-prefix/prefix-length*|**any**|**host** *dest-ipv6-address*} [{*dest-port-operator dest-port-number*|**range** *dest-port-number dest-port-number*}] **[established] [log-deny]**
deny udp {*source-ipv6-prefixprefix-length*|**any**|**host** *source-ipv6-address*} [{*source-port-operator source-port-number*|**range** *source-port-number source-port-number*}] {*dest-ipv6-prefixprefix-length*|**any**|**host** *dest-ipv6-address*} [{*dest-port-operator dest-port-number*|**range** *dest-port-number dest-port-number*}] **[log-deny]**
no deny {*ipv6-protocol-number*|**ipv6**|**icmp**|**tcp**|**udp**}

Syntax Description

i*pv6-protocol-number*	Specifies an IPv6 protocol number. The range is 0 to 255.
ipv6	Applies the ACL to any IPv6 packet.
source-ipv6-prefix/prefix-length	Specifies a source IPv6 network or class of networks. The format is *X:X:X::X/n* .
any	Applies the ACL to any source or destination prefix.
host *source-ipv6-address*	Applies the ACL to the specified source IPv6 host address. The format is *X:X:X::X* .
dest-ipv6-prefix/prefix-length	Specifies a destination IPv6 network or class of networks. The format is *X:X:X::X/n* .
host *dest-ipv6-address*	Applies the ACL to the specified destination IPv6 host address. The format is *X:X:X::X* .
log-deny	(Optional) For packets that are dropped, creates an informational log message about the packet that matches the entry. The message includes the input interface.
icmp	Applies the ACL to any Internet Control Message Protocol (ICMP) packet.
icmp-type	Specifies an ICMP message type. The range is 0 to 255.
icmp-code	Specifies an ICMP message code. The range is 0 255.
tcp	Applies the ACL to any TCP packet.
source-port-operator	Specifies an operand that compares the source ports of the specified protocol. The operands are **lt** (less than), **gt** (greater than), and **eq** (equals).

source-port-number	Specifies the port number of a TCP or UDP port. The number can be from 0 to 65535. A range requires two port numbers.
udp	Applies the ACL to any UDP packet.
dest-port-operator	Specifies an operand that compares the destination ports of the specified protocol. The operands are **lt** (less than), **gt** (greater than), and **eq** (equals).
dest-port-operator	Specifies the port number of a TCP or UDP port. The number can be from 0 to 65535. A range requires two port numbers.
range	Specifies a range of ports to compare for the specified protocol.
established	(Optional) Indicates an established connection, which is defined as a packet whole SYN flag is not set.

Command Default

None.

Command Modes

IPv6-ACL configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The following guidelines can assist you in configuring an IPv6-ACL.

You can apply IPv6-ACLs to VSAN interfaces, the management interface, Gigabit Ethernet interfaces on IPS modules and MPS-14/2 modules, and Ethernet PortChannel interfaces. However, if IPv6-ACLs are already configured in a Gigabit Ethernet interface, you cannot add this interface to a Ethernet PortChannel group.

Caution Do not apply IPv6-ACLs to just one member of a PortChannel group. Apply IPv6-ACLs to the entire channel group.

- Use only the TCP or ICMP options when configuring IPv6-ACLs on Gigabit Ethernet interfaces.
- Configure the order of conditions accurately. Because the IPv6-ACL filters are applied sequentially to the IP flows, the first match determines the action taken. Subsequent matches are not considered. Be sure to configure the most important condition first. If no conditions match, the software drops the packet.

Examples

The following example configures an IPv6-ACL called List1, enters IPv6-ACL submode, and adds an entry to deny TCP traffic from any source address to any destination address:

```
switch# config terminal
switch(config)# ipv6 access-list List1
switch(config-ipv6-acl)# deny tcp any any
```

The following example removes a deny condition set for any destination prefix on a specified UDP host:

```
switch# config terminal
```

```
switch(config)# ipv6 access-list List1
switch(config-ipv6-acl)# no deny udp host 2001:db8:200d::4000 any
```

The following example removes the IPv6-ACL called List1 and all its entries:

```
switch# config terminal
switch(config)#  no ipv6 access-list List1
```

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6 ACL and enters IPv6-ACL configuration submode.
permit	Configures permit conditions for an IPv6 ACL.

description

To configure a description for the Event Manager policy, use the description command.

description *policy-description*

Syntax Description

policy-description	Configures a descriptive string for the policy. The string can be any alphanumeric string up to 80 characters. Enclose the string in quotation marks.

Command Default

None.

Command Modes

Embedded Event Manager.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure a descriptive string for the policy:

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

Related Commands

Command	Description
show interface	Displays an interface configuration for a specified interface.
shutdown	Disables and enables an interface.

destination interface

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

destination interface {**fc** *slot/port*|**fc-tunnel** *tunnel-id*}
no destination interface {**fc** *slot/port*|**fc-tunnel** *tunnel-id*}

Syntax Description

fc *slot/port*	Specifies the Fibre Channel interface ID at a slot and port.
fc-tunnel *tunnel-id*	Specifies the Fibre Channel tunnel interface ID.

Command Default

Disabled.

Command Modes

SPAN session configuration submode.

Command History

Release	Modification
6.2(5)	SPAN is supported and RSPAN is not supported in Cisco MDS 9250i Multiservice Fabric Switch.
1.0(2)	This command was introduced.
1.2(1)	Added the fc-tunnel parameter.

Usage Guidelines

The SPAN destination interface must be configured as SPAN destination port (SD port) mode using the **switchport** command before the interface can be associated with SPAN session as a destination interface.

Examples

The following example shows how to configure an interface as a SPAN destination port (SD port), create a SPAN session, and then configure the interface fc3/13 as the SPAN destination interface:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# interface fc3/13
switch(config-if)# switchport mode

switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface fc3/13
switch(config-if)# switchport mode sd
switch(config-if)# exit
switch(config)# span session 1
switch(config-span)# destination interface fc3/13
switch(config-span)# do show span session 1
switch(config-span)# show span session 1
Session 1 (inactive as destination is down)
   Destination is fc3/13
   No session filters configured
   No ingress (rx) sources
   No egress (tx) sources
switch(config-span)#
```

Related Commands

Command	Description
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.

destination-profile

To configure the attributes of the destination such as the e-mail address or the message level with the Call Home function, use the **destination-profile** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

{**destination-profile** {*profile-name*|**XML-destination**|**full-txt-destination**|**short-txt-destination**} **alert-group** {**all**|**cisco-Tac**|**environmental**|**inventory**|**license**|**linecard-hardware**|**rmon**|**supervisor-hardware**|**syslog-group-port**|**system**|**test**}|**email-addr** *email-address*|**http** *https-or-http url*|**message-level** *message-level*|**message-size** *message-size*|**transport-method** {**email**|**http**}}
{**no destination-profile** {*profile-name*|**XML-destination**|**full-txt-destination**|**short-txt-destination**} **alert-group** {**all**|**cisco-Tac**|**environmental**|**inventory**|**license**|**linecard-hardware**|**rmon**|**supervisor-hardware**|**syslog-group-port**|**system**|**test**}|**email-addr** *email-address*|**http** *https-or-http url*|**message-level** *message-level*|**message-size** *message-size*|**transport-method** {**email**|**http**}}

Syntax Description

profile-name	Specifies a user-defined user profile with a maximum of 32 alphanumeric characters.
XML-destination	Configures the destination profile for XML messages.
full-txt-destination	Configures the destination profile for plain text messages.
short-txt-destination	Configures the destination for short text messages.
alert-group	Specifies one or more of the alert groups.
all	Specifies an alert group consisting of all Call Home messages.
cisco-Tac	Specifies an alert group consisting of events that are meant only for Cisco TAC.
environmental	Specifies an alert group consisting of power, fan, and temperature-related events.
inventory	Specifies an alert group consisting of inventory status events.
license	Specifies an alert group consisting of license status events.
linecard-hardware	Specifies an alert group consisting of module related events.
rmon	Specifies an alert group consisting of RMON status events.
supervisor-hardware	Specifies an alert group consisting of supervisor-related events.
syslog-port-group	Specifies an alert group consisting of syslog port group status events.
system	Specifies an alert group consisting of software-related events.
test	Specifies an alert group consisting of user-generated test events.

email-addr	E-mail transport method.
email-address	Specifies the E-mail address.
http	HTTP transport method.
https-or-http url	Specifies the HTTP or HTTPs URL.
message-level *message-level*	Specifies Call Home message level (0 is the lowest urgency, 9 is the highest urgency).
message-size *message-size*	Configures the maximum message size (default 2500000).
transport-method	Specifies Call Home message-sending transport method.
email	Specifies the e-mail transport method.
http	Specifies the HTTP transport method.

Command Default

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
NX-OS 4.2(1)	Deleted Avanti keyword from the syntax description. Added the Usage guideline.
NX-OS 4.1(3)	Added the HTTPs URL and transport method for syntax description.
1.0(2)	This command was introduced.

Usage Guidelines

The transport method as well as the HTTP URL is distributed only to the switches in the fabric running images for 4.2(1) and later. The switches running in the lower version images will simply ignore the HTTP configuration.

The HTTP configuration also will not be distributed to switches that support the HTTP configuration but do not distribute it.

Examples

The following example shows how to configure XML destination profiles for the HTTP URL:

```
switch(config-callhome)# destination-profile XML-destination http http://site.service.com
switch(config-callhome)# no destination-profile XML-destination http http://site.service.com
```

The following example enables the transport method for destination profile:

```
switch(config-callhome)# destination-profile XML-destination transport-method http
switch(config-callhome)# no destination-profile XML-destination transport-method http
switch(config-callhome)#
switch(config-callhome)# destination-profile XML-destination transport-method email
switch(config-callhome)# no destination-profile XML-destination transport-method email
```

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

The following example shows how to configure full-text destination profiles:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# destination-profile full-txt-destination email-addr person@place.com
switch(config-callhome)# destination-profile full-txt-destination message-size 1000000
```

The following example shows how to configure short-text destination profiles:

```
switch(config-callhome)# destination-profile short-txt-destination email-addr person@place.com
switch(config-callhome)# destination-profile short-txt-destination message-size 100000
```

Related Commands

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

device-alias (IVR fcdomain database configuration submode)

To map a device alias to a persistent FC ID for IVR, use the **device-alias** command in IVR fcdomain database configuration submode. To remove the mapping for the device alias, use the **no** form of the command.

device-alias *device-name fc-id*
no device-alias *device-name*

Syntax Description

device-name	Specifies the device name. Maximum length is 64 characters.
fc-id	Specifies the FC ID for the device.

Command Default

None.

Command Modes

IVR fcdomain database configuration submode.

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

Only one FC ID can be mapped to a device alias.

Examples

The following example shows how to map the device alias to the persistent FC ID:

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# native-autonomous-fabric-num 20 native-vsan 30 domain 15
switch(config-fcdomain-fcid)# device-alias SampleName 0x123456
```

The following example shows how to remove the mapping between the device alias and the FC ID:

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# native-autonomous-fabric-num 20 native-vsan 30 domain 15
switch(config-fcdomain-fcid)# no device-alias SampleName
```

Related Commands

Command	Description
ivr fcdomain database autonomous-fabric-num	Creates IVR persistent FC IDs.
native-autonomous-fabric-num	Creates an IVR persistent FC ID database entry.
show ivr fcdomain database	Displays IVR fcdomain database entry information.

device-alias (SDV virtual device configuration submode)

To add a device alias to a virtual device, use the **device-alias** command in SDV virtual device configuration submode. To remove a device alias, use the **no** form of the command.

device-alias *device-name* **[primary]**
no device-alias *device-name* **[primary]**

Syntax Description

device-name	Specifies the device name. Maximum length is 64 characters.
primary	(Optional) Specifies the device as a primary device.

Command Default

None.

Command Modes

SDV virtual device configuration submode.

Command History

Release	Modification
3.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure a virtual target alias name:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# sdv virtual-device name sqa1 vsan 1
switch(config-sdv-virt-dev)# device-alias group1 primary
```

Related Commands

Command	Description
sdv enable	Enables or disables SAN device virtualization.
show sdv statistics	Displays SAN device virtualization statistics.

device-alias abort

To discard a Distributed Device Alias Services (device alias) Cisco Fabric Services (CFS) distribution session in progress, use the **device-alias abort** command **in configuration mode.**

device-alias abort

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to discard a device alias CFS distribution session in progress:

```
switch# config terminal
switch(config)# device-alias abort
```

Related Commands

Command	Description
device-alias database	Configures and activates the device alias database.
device-alias distribute	Enables CFS distribution for device aliases.
show device-alias	Displays device alias information.

device-alias commit

To apply the pending configuration pertaining to the Distributed Device Alias Services (device alias) Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **device-alias commit** command in configuration mode.

device-alias commit

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None

Note Once the **device-alias commit** is done the running configuration has been modified on all switches participating in device-alias distribution. You can then use the **copy running-config startup-config fabric** command to save the running-config to the startup-config on all the switches in the fabric.

Note When the **device-alias commit** is in progress, you must not issue the **clear device-alias** command, until the device-alias commit is successful.

Examples

The following example shows how to commit pending changes to the active DPVM database:

```
switch# config terminal
switch(config)# device-alias commit
```

Related Commands

Command	Description
device-alias database	Configures and activates the device alias database.
device-alias distribute	Enables CFS distribution for device aliases.
show device-alias	Displays device alias information.

device-alias confirm-commit enable

To enable the display of the device-alias pending-diff and subsequent confirmation of pending-diff on issuing a device-alias commit, use the **device-alias confirm-commit enable** command in configuration mode. To disable this feature command, use the **no** form of this command.

device-alias confirm-commit enable
no device-alias confirm-commit enable

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(9)	This command was introduced.

Usage Guidelines

If the **device-alias confirm-commit** command is enabled, on committing the pending database, the pending-diff is displayed on the console and the user is prompted for Yes or No. If the **device-alias confirm-commit** command is disabled, the pending-diff is not displayed and the user is not prompted for Yes or No.

Note If this feature is enabled, downgrade is blocked by a configuration check. To resume downgrade correctly, confirm-commit has to be disabled.

Examples

The following example shows how to enable the confirm-commit mode for device-alias:

```
switch# config terminal
switch(config)# device-alias confirm-commit enable
switch(config)#
```

The following example shows how to disable the confirm-commit mode for device-alias:

```
switch# config terminal
switch(config)# no device-alias confirm-commit enable
switch(config)#
```

device-alias database

To initiate a Distributed Device Alias Services (device alias) session and configure device alias database, use the **device-alias database** command.

device-alias database

Syntax Description

This command has no other arguments or keywords.

Command Default

Deactivated.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

The **device-alias database** command starts a device alias session that locks all the databases on all the switches in this fabrics. When you exit device alias database configuration submode, the device alias session ends and the locks are released.

You can only perform all modifications in the temporary device alias database. To make the changes permanent, use the **device-alias commit** command.

Examples

The following example shows how to activate a device alias session and enter device alias database configuration submode:

```
switch# config terminal
switch(config)# device-alias database
switch(config-device-alias-db)#
```

Related Commands

Command	Description
device-alias commit	Commits changes to the temporary device alias database to the active device alias database.
show device-alias	Displays device alias database information.

device-alias distribute

To enable Cisco Fabric Services (CFS) distribution for Distributed Device Alias Services (device alias), use the **device-alias distribute** command. To disable this feature, use the **no** form of the command.

device-alias distribute
no device-alias distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

Use the **device-alias commit** command to apply pending changes to the CFS distribution session.

Examples

The following example shows how to enable distribution for device alias information:

```
switch# config terminal
switch(config)# device-alias distribute
```

Related Commands

Command	Description
device-alias commit	Commits changes to the active device alias database.
device-alias database	Configures and activates the device alias database.
show device-alias	Displays device alias information.

device-alias import fcalias

To import device alias database information from another VSAN, use the **device-alias import fcalias** command. To revert to the default configuration or factory defaults, use the **no** form of the command.

device-alias import fcalias vsan *vsan-id*
no device-alias import fcalias vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

You can import legacy device name configurations using this feature without losing data, if they satisfy the following restrictions:

- Each fcalias has only one member.
- The member type is supported by the device name implementation.

If any name conflict exists, the fcaliases are not imported. The device name database is completely independent from the VSAN dependent fcalias database.

When the import operation is complete, the modified global fcalias table can distributed to all other switches in the physical fabric using the **device-alias distribute** command so that new definitions are available everywhere.

Examples

The following example shows how to import device alias information:

```
switch# config terminal
switch(config)# device-alias import fcalias vsan 10
```

Related Commands

Command	Description
device-alias database	Configures and activates the device alias database.
device-alias distribute	Distributes fcalias database changes to the fabric.
show device-alias	Displays device alias database information.

device-alias mode enhanced

To configure device aliases to operate in enhanced mode, use the device-alias mode enhanced command. To disable this feature, use the **no** form of the command.

device-alias mode enhanced
no device-alias mode enhanced

Syntax Description

This command has no arguments or keywords.

Command Default

Basic mode.

Command Modes

Configuration mode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When a device alias is configured in basic mode, which is the default mode, all the applications operate like 3.0 switches. For example, when you attempt to configure the device aliases, immediately the device alias are expanded to a PWWN. This operation continues until the mode is changed to enhanced.

When a device alias is configured in enhanced mode, all the applications accept a device alias name in its native format, instead of expanding the device alias to a PWWN, the device alias name is stored in the configuration and distributed in its native device alias format.

To use enhanced mode, all switches in the fabric must be running in the Cisco SAN-OS Release 3.1(1) or later, or NX-OS 4.1(1b) later.

Note Enhanced mode, or native device alias based configurations are not accepted in interop mode. VSANs. IVR zoneset activation will fail in interop mode VSANs if the corresponding zones have native device alias-based members

Examples

The following example shows how to configure the device alias in enhanced mode:

```
switch# config terminal
switch(config)# device-alias mode enhanced
switch(config)#
```

Related Commands

Command	Description
device-alias commit	Commits changes to the active device alias database.
device-alias database	Configures and activates the device alias database.
show device-alias	Displays device alias information.

debug ldap

To configure debugging for LDAP, use the **debug ldap** command. To disable this feature, use the **no** form of the command.

debug ldap {**aaa-request**|**aaa-request-lowlevel**|**all**|**config**|**config-lowlevel**}
no debug ldap {**aaa-request**|**aaa-request-lowlevel**|**all**|**config**|**config-lowlevel**}

Syntax Description

aaa-request	Enables LDAP AAA request debug.
aaa-request-lowlevel	Enables LDAP AAA request low level debugging.
config	Enables LDAP configuration debugging.
config-lowlevel	Enables LDAP configuring low level debugging.
all	Enables all the debug flags.

Command Default

None.

Command Modes

EXEC mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure LDAP AAA request debug:

```
switch# debug ldap aaa-request
switch#
```

The following example shows how to configure LDAP AAA request low level debugging:

```
switch# debug ldap aaa-request-lowlevel
switch#
```

Related Commands

Command	Description
show debug	Displays all Cisco SME related debug commands configured on the switch.

device-alias name

To configure device names in the device alias database, use the **device-alias name** command. To remove device names from the device alias database, use the **no** form of the command.

device-alias name *device-name* **pwwn** *pwwn-id*
no device-alias name *device-name*

Syntax Description

device-name	Specifies the device name. Maximum length is 64 characters.
pwwn *pwwn-id*	Specifies the pWWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.

Command Default

None.

Command Modes

Device alias database configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure a device name alias entry in the device name database:

```
switch# config terminal
switch(config)# device-alias database
switch(config-device-alias-db)# device-alias name Device1 pwwn 21:00:00:20:37:6f:db:bb
```

Related Commands

Command	Description
device-alias database	Enters device alias database configuration submode.
show device-alias	Displays device alias database information.

diagnostic bootup level

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

{**diagnostic bootup level bypass|complete**}
{**no diagnostic bootup level bypass|complete**}

Syntax Description

bypass	Specifies the skip all bootup test. Do not perform any bootup diagnostics.
complete	Specifies all bootup diagnostics. The default is complete.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure all bootup diagnostics level:

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

Related Commands

Command	Description
show diagnostic bootup level	Displays the bootup diagnostic level (bypass or complete) that is currently in place on the device.
show diagnostic events	Displays diagnostic events by error and information event type.

diagnostic isl latency-test

To configure a generator switch to start and display the results for a latency test, use the **diagnostic isl latency-test interface fc** *slot/port* command.

diagnostic isl latency-test interface fc *slot/port*

Syntax Description

interface fc *slot/port*	Fibre Channel port.

Command Default

None

Command Modes

User EXEC (#)
Privileged EXEC (#)

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Examples

This example displays how to start and display results for the latency test on the interface fc4/9:

```
switch# diagnostic isl latency-test interface fc4/9
waiting for link to be in sync ...
------------------------------------------------------------
Latency test Result for port: fc4/9
Latency in the switch(In nano-seconds):396
Latency in the cable(In nano-seconds):36
Length of the cable approximately (+/-2m)):2 metres
```

Related Commands

Command	Description
diagnostic isl multi_hop generator	Configures an interface on a generator switch to run the Multihop Traffic Test for a given VSAN, destination domain (domain ID of the reflector switch), frame count, link speed, and frame size parameters.
diagnostic isl multi_hop reflector	Enables or disables a test interface on a reflector switch by setting it to loopback mode for a given VSAN and domain ID of a generator switch for Multihop Traffic Test.
diagnostic isl show status	Displays the status of configured Inter-Switch Link (ISL) diagnostic tests per port.

diagnostic isl multi_hop generator

To configure an interface on a generator switch to run the Multihop Traffic Test for a given VSAN, destination domain (domain ID of the reflector switch), frame count, link speed, and frame size parameters, use the **diagnostic isl multi_hop generator** command.

diagnostic isl multi_hop generator interface fc *slot/port* **vsan** *id* **dest_domain** *id* {**start** {**duration** *seconds* |**frame_count** *number*} |**stop**} [**rate** {**6.25%** |**12.5%** |**25%** |**50%** |**100%**}] [**frame_size min** *size* **max** *size* **step** *size*]

Syntax Description

interface fc *slot/port*	Fibre Channel port.
vsan *id*	Specifies entries based on a VSAN ID. Range is from 1 to 4096.
dest_domain *id*	Domain ID of a reflector switch. Range is from 0 to 255.
start	Specifies to start traffic generation.
duration *seconds*	Duration of the traffic test.
frame_count *number*	Frame count to transmit. Range is 1 to 2000000000.
stop	Specifies to stop traffic generation.
rate	Specifies a speed value to generate traffic.
6.25%	Generate traffic at 6.25% of the line rate.
12.5%	Generate traffic at 12.5% of the line rate.
25%	Generate traffic at 25% of the line rate.
50%	Generate traffic at 50% of the line rate.
100%	Generate traffic at 100% of the line rate.
frame_size	Specifies packet size range for traffic generation.
min *size*	Minimum packet size for packet generation. Range is from 16 to 517.
max *size*	Maximum packet size for packet generation. Range is from 16 to 517.
step *size*	Step size, in the range between minimum and maximum frame size, for traffic generation. Range is from 1 to 100.

Command Default

None

Command Modes

User EXEC (#)
Privileged EXEC (#)

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Examples

This example displays how to start traffic generation on the interface fc4/11 of a generator switch for a duration of 5 seconds:

```
switch# diagnostic isl multi_hop generator interface fc4/11 vsan 1 dest_domain 36 start
duration 5
```

This example displays how to stop traffic generation on the interface fc4/11 of a generator switch:

```
switch# diagnostic isl multi_hop generator interface fc4/11 vsan 1 dest_domain 36 stop

Generator is stopped.  Clean-up in progress.
Please wait....

------------------------------------------------------------
Traffic test Result for port: fc4/11
Packets Transmitted:111734
Packets Recieved in ISL :111734
ISL traffic Efficiency(in percentage):100.000000
------------------------------------------------------------
```

Related Commands

Command	Description
diagnostic isl multi_hop reflector	Enables or disables a test interface on a reflector switch by setting it to loopback mode for a given VSAN and domain ID of a generator switch for Multihop Traffic Test.
diagnostic isl show status	Displays the status of configured Inter-Switch Link (ISL) diagnostic tests per port.

diagnostic isl multi_hop reflector

To enable or disable a test interface on a reflector switch by setting it to loopback mode for a given VSAN and domain ID of a generator switch for Multihop Traffic Test, use the **diagnostic isl multi_hop reflector** command.

diagnostic isl multi_hop reflector loop-back interface fc *slot/port* **vsan** *id* **source_domain** *id* {**enable** |**disable**}

Syntax Description

loop-back	Specifies loopback.
interface fc *slot/port*	Fibre Channel port.
vsan *id*	Specifies entries based on a VSAN ID. Range is from 1 to 4096.
source_domain *id*	Source ID of a generator switch. Range is from 0 to 255.
enable	Enable loopback.
disable	Disable loopback.

Command Default

Loopback for an interface is disabled by default.

Command Modes

User EXEC (#)
Privileged EXEC (#)

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Examples

This example displays how to enable Multihop Traffic Test on the interface fc1/39 of a reflector switch:

```
switch# diagnostic isl multi_hop reflector loop-back interface fc1/39 vsan 1 source_domain
 2 enable
```

This example displays how to disable Multihop Traffic Test on the interface fc1/39 of a reflector switch:

```
switch# diagnostic isl multi_hop reflector loop-back interface fc1/39 vsan 1 source_domain
 2 disable
```

Related Commands

Command	Description
diagnostic isl multi_hop generator	Configures an interface on a generator switch to run the Multihop Traffic Test for a given VSAN, destination domain (domain ID of the reflector switch), frame count, link speed, and frame size parameters.
diagnostic isl show status	Displays the status of configured Inter-Switch Link (ISL) diagnostic tests per port.

diagnostic isl show status

To display the status of configured Inter-Switch Link (ISL) diagnostic tests per port, use the **diagnostic isl show status** command.

diagnostic isl show status index start *index* **num** *number*

Syntax Description

index	Index of the ISL diagnostic port status.
start *index*	Index number of the ISL diagnostic port status.
num *number*	Number of entries of the ISL diagnostic port status array.

Command Default

None

Command Modes

User EXEC (#)
Privileged EXEC (#)

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Examples

This example displays the ISL diagnostic tests for the port fc2/2:

```
switch# diagnostic isl show status index start 1 num 1
Status of isl_daig tests in progress:
------------------------------------------------------------
Index  Interface        Mode <Gen/Ref>          Test
------------------------------------------------------------

 1      fc2/2           Generator        MH Traffic Test
------------------------------------------------------------
```

Related Commands

Command	Description
diagnostic isl multi_hop generator	Configures an interface on a generator switch to run the Multihop Traffic Test for a given VSAN.
diagnostic isl multi_hop reflector	Enables or disables a test interface on a reflector switch by setting it to loopback mode for a given VSAN and domain ID of the generator switch for Multihop Traffic Test.

diagnostic monitor interval module

To configure diagnostic monitoring tests interval for a module, use the **diagnostic monitor interval module** command. To remove this diagnostic monitor interval module, use the **no** form of the command.

diagnostic monitor interval module *module-number* **test** [{*test-id*|**name**|**all**}] **hour** *hour* **min** *minutes* **second** *sec*
no diagnostic monitor interval module *module-number* **test** [{*test-id*|**name**|**all**}] **hour** *hour* **min** *minutes* **second** *sec*

Syntax Description

module-number	Specifies the module number. The range is from 1 to 10.
test	Specifies the diagnostic test selection.
test-id	Specifies test IDs. The range is from 1to 10.
name	Specifies the test name. Can be any case-sensitive alphanumeric string up to 32 characters.
all	Specifies all test ID.
hour	Specifies hour of the day.
hour	Specifies interval in hours. The range is from 0 to 23.
min	Specifies minute of an hour.
minutes	Specifies interval in minutes. The range is from 0 to 59.
second	Specifies second of a minute.
sec	Specifies inteval in seconds. The range is from 0 to 59.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure diagnostic monitoring tests interval for a module:

```
switch# config terminal
switch(config)# diagnostic monitor interval module 6 test 3 hour 1 min 0 sec 0
switch(config)#
```

Related Commands

Command	Description
diagnostic monitor module	Activates the specified test.
show diagnostic content module	Displays information about the diagnostics and their attributes.

diagnostic monitor module

To configure diagnostic monitoring tests for a module, use the **diagnostic monitor module** command. To remove this diagnostic monitor module, use the **no** form of the command.

diagnostic monitor module *module-number* **test** [{*test-id*|**name**|**all**}]
no diagnostic monitor module *module-number* **test** [{*test-id*|**name**|**all**}]

Syntax Description

module-number	Specifies the module number. The range is from 1 to 10.
test	Specifies the diagnostic test selection.
test-id	Specifies test IDs. The range is from 1to 10.
name	Specifies the test name. Can be any case-sensitive alphanumeric string up to 32 characters.
all	Specifies all test ID.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure diagnostic monitoring tests for a module:

```
switch# config terminal
switch(config)# diagnostic monitor module 6 test 3
switch(config)#
```

Related Commands

Command	Description
diagnostic monitor interval module	Configures the interval at which the specified test is run.
show diagnostic content module	Displays information about the diagnostics and their attributes.

diagnostic ondemand iteration

To configure the number of times that the on demand test runs, use the **diagnostic ondemand iteration** command. To remove this diagnostic ondemand iteration, use the **no** form of the command.

diagnostic ondemand iteration *number*
no diagnostic ondemand iteration *number*

Syntax Description

number	Specifies number of times to repeat ondemand test list. The range is from 1 to 999.

Command Default

1.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the number of times that the on demand test runs:

```
switch# diagnostic ondemand iteration 4
switch(config)#
```

Related Commands

Command	Description
diagnostic ondemand action-on-failure	Configures the action to take if the on-demand test fails.
show diagnostic ondemand setting	Displays information about on-demand diagnostics.

diagnostic ondemand action-on-failure

To configure the action to take if the on demand test fails, use the **diagnostic ondemand action-on-failure** command. To remove this feature command, use the **no** form of the command.

diagnostic ondemand action-on-failure {**continue failure-count** *num-fails*|**stop**}
no diagnostic ondemand action-on-failure {**continue failure-count** *num-fails*|**stop**}

Syntax Description

continue	Specifies the continue ondemand test until test failure limit is reached.
failure-count	Specifies the continue failing tests these many times.
num-fails	The num-fails range is from 1 to 999.
stop	Stop ondemand tests immediately if a test fails.

Command Default

1.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the action to take if the on demand test fails:

```
switch# diagnostic ondemand action-on-failure stop
switch#
```

Related Commands

Command	Description
diagnostic ondemand iteration	Configures the number of times that the on-demand test runs.
show diagnostic ondemand setting	Displays information about on-demand diagnostics.

diagnostic start module

To start one or more diagnostic tests on a module, use the **diagnostic start module** command. To remove this feature command, use the **no** form of the command.

diagnostic start module *module-number* **test** [{*test-id*|**name**|**all**|**non-disruptive**}] [{**port** *port-number*|**all**}]
no diagnostic start module *module-number* **test** [{*test-id*|**name**|**all**|**non-disruptive**}] [{**port** *port-number*|**all**}]

Syntax Description

module-number	Specifies the module number. The range is from 1 to 10.
test	Specifies the diagnostic test selection.
test-id	Specifies test IDs. The range is from 1 to 10.
name	Specifies the test name. Can be any case-sensitive alphanumeric string up to 32 characters.
`all`	Specifies all test ID.
non-disruptive	Specifies non disruptive diagnostics.
port	Specifies the port.
port-number	Specfies the port number. The port range is from 1 to 48.

Command Default

1.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to start one or more diagnostic tests on a module:

```
switch# diagnostic start module 6 test all
switch#
switch#
```

Related Commands

Command	Description
diagnostic run module	Starts the selected test on a module and displays the result on the completion of the test.
diagnostic stop module	Stops one or more diagnostic tests on a module.

diagnostic stop module

To stop one or more diagnostic tests on a module, use the **diagnostic stop module** command. To remove this feature command, use the **no** form of the command.

diagnostic stop module slot test [{**test-id**|**name**|**all**}]
no diagnostic stop module slot test [{**test-id**|**name**|**all**}]

Syntax Description

module-number	Specifies the module number. The range is from 1 to 10.
test	Specifies the diagnostic test selection.
test-id	Specifies test IDs. The range is from 1to 10.
name	Specifies the test name. Can be any case-sensitive alphanumeric string up to 32 characters.
all	Specifies all test ID.

Command Default

1.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to stop one or more diagnostic tests on a module:

```
switch# diagnostic stop module 6 test all
switch#
switch#
```

Related Commands

Command	Description
diagnostic run module	Starts the selected test on a module and displays the result on the completion of the test.
diagnostic start module	Starts one or more diagnostic tests on a module.

dir

To display the contents of the current directory or the specified directory, use the **dir** command in EXEC mode.

dir [{ **bootflash** **:** *module directory-or-filename* | **debug** **:** *directory-or-filename* | **log** **:** *module directory-or-filename* | **modflash** **:** *module directory-or-filename* | **slot0** **:** *directory-or-filename* | **volatile** **:** *module directory-or-filename* }]

Syntax Description

bootflash:	(Optional) Flash image that resides on the supervisor module.
debug:	(Optional) Provides information about the debug capture directory.
log:	(Optional) Provides information about the two default log files. The file dmesg contains the kernel log messages and the file messages contains the system application log messages.
modflash:	(Optional) Provides information about the flash image that resides in a module flash file directory.
slot0:	(Optional) Flash image that resides on another module.
module	(Optional) Module name and number.
directory-or-filename	(Optional) Name of the file or directory to display on a specified device. The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.
volatile:	(Optional) Flash image on the volatile file system.

Command Default

The default file system is specified by the **cd** command.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.
2.1(1a)	Added debug, log, and modflash keywords.

Usage Guidelines

None.

Examples

The following example shows how to list the files on the bootflash directory:

```
switch# dir bootflash:
40295206     Aug 05 15:23:51 1980  ilc1.bin
12456448     Jul 30 23:05:28 1980  kickstart-image1
12288         Jun 23 14:58:44 1980  lost+found/
27602159     Jul 30 23:05:16 1980  system-image1
```

```
12447232     Aug 05 15:08:30 1980  kickstart-image2
28364853     Aug 05 15:11:57 1980  system-image2
Usage for bootflash://sup-local
  135404544 bytes used
   49155072 bytes free
  184559616 bytes total
```

The following example shows how to list the files in the debug directory:

```
switch# dir debug:
Usage for debug://sup-local
          0 bytes used
    2097152 bytes free
    2097152 bytes total
switch#
switch# dir ?
  bootflash:  Directory or filename
  debug:      Directory or filename
  log:        Directory or filename
  modflash:   Directory or filename
  slot0:      Directory or filename
  volatile:   Directory or filename
  <cr>        Carriage Return
```

The following example shows how to list the files in the log file directory:

```
switch# dir log:
         31     Feb 05 05:00:57 2005  dmesg
       8445     Feb 06 10:34:35 2005  messages
Usage for log://sup-local
   35196928 bytes used
  174518272 bytes free
  209715200 bytes total
switch#
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
delete	Deletes a file on a flash memory device.

disable

To disable the Call Home function, use the **disable** command in Call Home configuration submode.

disable

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

To enable the Call Home function, use the **enable** command.

Examples

The following example shows how to disable the Call Home function:

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

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.

discover

To initiate the discovery of hosts, use the **discovery** command. To disable this feature, use the **no** form of the command.

discover host *host port* **target** *target port* **vsan** *vsan id* **fabric** *fabric name*
no discover

Syntax Description

host *host port*	Identifies the host port WWN. The format is hh:hh:hh:hh:hh:hh:hh:hh.
target *target port*	Identifies the target port WWN. The format is hh:hh:hh:hh:hh:hh:hh:hh.
vsan *vsan id*	Selects the VSAN identifier. The range is 1 to 4093.
fabric *fabric name*	Specifies the fabric for discovery. The maximum length is 32 characters.

Command Default

None.

Command Modes

Cisco SME cluster configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example discovers a host and specifies a target, a VSAN, and a fabric for discovery:

```
switch# config t
switch(config)# sme cluster clustername1
switch(config-sme-cl)# discover host 20:00:00:00:c9:49:28:47 target 21:01:00:e0:8b:29:7e:0c
 vsan 2345 fabric sw-xyz
```

The following example disables the discovery feature:

```
switch# config t
switch(config)# sme cluster clustername1
switch(config-sme-cl)# no discover
```

Related Commands

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

discover custom-list

To selectively initiate discovery for specified domain IDs in a VSAN, use the discover custom-list command in EXEC mode.

discover custom-list {**add**|**delete**} **vsan** *vsan-id* **fcid** *fc-id*

Syntax Description

add	Add a targets to the customized list.
delete	Deletes a target from the customized list.
vsan *vsan-id*	Discovers SCSI targets for the specified VSAN ID. The range is 1 to 4093.
fcip *fc-id*	Discovers SCSI targets for the specified FCID. The format is *0xhhhhhhh*, where *h* is a hexadecimal digit.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example selectively initiates discovery for the specified VSAN and FCID:

```
switch# discover custom-list add vsan 1 fcid 0X123456
```

The following example deletes the specified VSAN and FCID from the customized list:

```
switch# discover custom-list delete vsan 1 fcid 0X123456
```

discover scsi-target

To discover SCSI targets on local storage to the switch or remote storage across the fabric, use the **discover scsi-target** command in EXEC mode.

discover scsi-target {**custom-list**|**local**|**remote**|**vsan** *vsan-id* **fcid** *fc-id*} **os** {**aix**|**all**|**hpux**|**linux**|**solaris**|**windows**} [{**lun**|**target**}]

Syntax Description

custom-list	Discovers SCSI targets from the customized list.
local	Discovers local SCSI targets.
remote	Discovers remote SCSI targets.
vsan *vsan-id*	Discovers SCSI targets for the specified VSAN ID. The range is 1 to 4093.
fcip *fc-id*	Discovers SCSI targets for the specified FCID. The format is *0xhhhhhhh*, where *h* is a hexadecimal digit.
os	Discovers the specified operating system.
aix	Discovers the AIX operating system.
all	Discovers all operating systems.
hpux	Discovers the HPUX operating system.
linux	Discovers the Linux operating system.
solaris	Discovers the Solaris operating system.
windows	Discovers the Windows operating system.
lun	(Optional) Discovers SCSI targets and LUNs.
target	(Optional) Discovers SCSI targets.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(2a)	This command was introduced.

Usage Guidelines

On-demand discovery only discovers Nx ports present in the name server database that have registered a FC4 Type = SCSI_FCP.

Examples

The following example shows how to discover local targets assigned to all OSs:

```
switch# discover scsi-target local os all
discovery started
```

The following example shows how to discover remote targets assigned to the Windows OS:

```
switch# discover scsi-target remote os windows
discovery started
```

The following example shows how to discover SCSI targets for the specified VSAN (1) and FCID (0x9c03d6):

```
switch# discover scsi-target vsan 1 fcid 0x9c03d6
discover scsi-target vsan 1 fcid 0x9c03d6
VSAN:    1 FCID: 0x9c03d6 PWWN: 00:00:00:00:00:00:00:00
  PRLI RSP: 0x01 SPARM: 0x0012...
```

The following example begins discovering targets from a customized list assigned to the Linux operating system:

```
switch# discover scsi-target custom-list os linux
discovery started
```

distribute

To enable distribution of the Call Home function using CFS, use the **distribute** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

distribute
no distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Call Home configuration submode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to enable distribution of the Call Home function using CFS:

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

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.

dmm module

To specify default DMM values for migration block size, number of migration blocks and fast migration speed, use the **dmm module** command in configuration mode.

dmm module *mod-id* **rate-of-migration fast** *migration-rate* **medium** *migration-rate* **slow** *migration-rate*

Syntax Description

mod-id	Specifies the module ID.
rate-of-migration	Migration rate can be configured as slow, medium or fast.
fast *migration-rate*	Specifies the rate for fast migration. Units are megabytes per second (MB/s).
medium *migration-rate*	Specifies the rate for medium migration. Units are MB/s.
slow *migration-rate*	Specifies the rate for slow migration. Units are MB/s.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to set the fast migration rate to 100 MB/s, the medium migration rate to 50 MB/s, and slow migration rate to 10 MB/s:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config) dmm module 3 rate_of_migration fast 100 medium 50 slow 10
```

Related Commands

Command	Description
show dmm ip-peer	Displays a DMM port's IP peer.
show dmm job	Displays job information.

dmm module job

To configure a data migration job, use the **dmm module** *mod-id* **job** command in configuration mode.

dmm module *mod-id* **job** *job-id* {**create**|**destroy**|**finish**|**get-vi vsan** *vsan-id*|**modify rate**|**schedule** {**hour** *hour* **min** *minute* **day** *day* **month** *month* **year** *year*|**now**|**reset**}|**session**|**set-vi** *portwwn nodewwn* **vsan** *vsan-id*|**start**|**stop**|**validate**|**verify**}

Syntax Description

module *mod-id*	Specifies the module ID.
job *job-id*	Specifies the job ID. The range is 0 to18446744073709551615.
create	Creates the job and enters DMM job configuration submode.
destroy	Deletes the DMM job.
finish	Moves the Method 2 data migration job to completed state.
get-vi	Retrieves the virtual initiator (VI) for the DMM job.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
modify	Modifies the DMM job attributes.
rate	Specifies the rate of the job attribute. The range is from 1 to 4. Specify 1 for a default value, 2 for slow, 3 for medium and 4 for fast rates.
schedule	Schedules the DMM job.
hour *hour*	Specifies the hour the DMM job starts. The range is 0 to 23.
min *minute*	Specifies the minute the DMM job starts. The range is 0 to 59.
day *day*	Specifies the day the DMM job starts. The range is 1 to 31.
month *month*	Specifies the month the DMM job starts. The range is 1 to 12.
year*year*	Specifies the year the DMM job starts. The range is 2000 to 2030.
now	Resets the schedule to start the DMM job immediately.
reset	Resets the DMM job to unscheduled.
session	Enables the Session Configuration submode.
set-vi	Sets the VI for the storage based job.
portwwn	Specifies the port WWN. The format is *hh:hh:hh:hh:hh:hh:hh:hh* , where *h* is a hexadecimal number.
nodewwn	Specifies the node WWN. The format is *hh:hh:hh:hh:hh:hh:hh:hh* , where *h* is a hexadecimal number.

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
start	Starts the DMM job session.
stop	Stops the DMM job.
validate	Validates the DMM job data.
verify	Verifies the data migration for the specified job.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.3(1a)	The **finish** keyword is introduced.
4.1(1b)	The set-**vi** and modify rate keywords were introduced.

Usage Guidelines

DMM must be enabled before you can create DMM jobs. Use the **ssm enable feature dmm** command to enable DMM.

The data migration job stops executing if it encounters any errors. To restart the migration, enter the **validate** command to validate the job configuration, then enter the **restart** command to restart the job.

Before creating a storage based data migration job, use the show dmm module vi-list command to choose the VI for migrating the data and then use the set-vi command to specify the VI.

When the job is in the failed state, you can restart the job using the start command. This command will start the job from point of last failure.

Examples

The following example shows how to restart the job in failed stated.

```
switch(config)# dmm module 3 job 4 start
switch#
```

The following example shows how to create a job with a schedule. The job is scheduled to start on Sunday, January 6, 2008 at 11:00 P.M.

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# dmm module 3 job 1 schedule hour 23 min 0 day 6 month 1 year 2008
```

Command	Description
show dmm ip-peer	Displays the IP peers that the DMM port is connected to.
show dmm job	Displays DMM job information.
show dmm module vi-list	Displays the list of VIs.

do

Use the **do** command to execute an EXEC-level command from any configuration mode or submode.

do *command*

Syntax Description

command	Specifies the EXEC command to be executed.

Command Default

None.

Command Modes

All configuration modes.

Command History

Release	Modification
1.1(1)	This command was introduced.
NX-OS 4.1(1b)	Added the command output for extended bbcredit interface.
NX-OS 4.1(1b)	Added a note.

Usage Guidelines

Use this command to execute EXEC commands while configuring your switch. After the EXEC command is executed, the system returns to the mode from which you issued the do command.

Note The receive bbcredit value reflects the extended bbcredit configuration. Extended bbcredit range for Vegas and ISOLA cards is 256-3500.

Examples

The following example shows how to execute the EXEC commands:

```
switch(config)# port-monitor name cisco
switch(config-port-monitor)# do
switch(config-port-monitor)#
```

The following example disables the **terminal session-timeout** command using the **do** command in configuration mode:

```
switch(config)# do terminal session-timeout 0
switch(config)#
```

The following example creates and enables the interface from configuration mode:

```
switch(config)# int fc 3/1
switch(config-if)# no shut
```

The following example shows how to receive the extended bbcredit interface:

```
switch(config-if)# do show interface fc3/2
fc3/2 is trunking
Hardware is Fiber Channel, SFP is short wave laser w/o OFC (SN)
Port WWN is 20:82:00:05:30:00:2a:1e
Peer port WWN is 20:42:00:0b:46:79:f1:80
Admin port mode is auto, trunk mode is on
Port mode is TE
Port vsan is 1
Speed is 2 Gbps
Transmit B2B Credit is 255
Receive B2B Credit is 1500
Receive data field Size is 2112
Beacon is turned off
    Trunk vsans (admin allowed and active) (1-10)
    Trunk vsans (up)                       (1-10)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()
    5 minutes input rate 504 bits/sec, 63 bytes/sec, 0 frames/sec
    5 minutes output rate 344 bits/sec, 43 bytes/sec, 0 frames/sec
      69390 frames input, 4458680 bytes
        0 discards, 0 errors
        0 CRC,  0 unknown class
        0 too long, 0 too short
      69458 frames output, 3086812 bytes
        0 discards, 0 errors
      2 input OLS, 1 LRR, 0 NOS, 2 loop inits
      1 output OLS, 1 LRR, 1 NOS, 1 loop inits
```

dpvm abort

To discard a dynamic port VSAN membership (DPVM) Cisco Fabric Services (CFS) distribution session in progress, use the **dpvm abort** command in configuration mode.

dpvm abort

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Examples

The following example shows how to discard a DPVM CFS distribution session in progress:

```
switch# config terminal
switch(config)# dpvm abort
```

Related Commands

Command	Description
dpvm database	Configures the DPVM database.
dpvm distribute	Enables CFS distribution for DPVM.
dpvm enable	Enables DPVM.
show dpvm	Displays DPVM information.

dpvm activate

To activate the dynamic port VSAN membership (DPVM) configuration database, use the **dpvm activate** command. To deactivate the DPVM configuration database, use the **no** form of the command.

dpvm activate [force]
no dpvm activate [force]

Syntax Description

force	(Optional) Forces the activation or deactivation if conflicts exist between the configured DPVM database and the active DPVM database.

Command Default

Deactivated.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Activation might fail if conflicting entries are found between the configured DPVM database and the currently activated DPVM database. You can ignore the conflicts using the **force** option.

Examples

The following example shows how to activate the DPVM database:

```
switch# config terminal
switch(config)# dpvm activate
```

The following example shows how to deactivate the DPVM database:

```
switch# config terminal
switch(config)# no dpvm activate
```

Related Commands

Command	Description
dpvm database	Configures the DPVM database.
dpvm enable	Enables DPVM.
show dpvm	Displays DPVM database information.

dpvm auto-learn

To enable the automatic learning feature (autolearn) for the active dynamic port VSAN membership (DPVM) database, use the **dpvm auto-learn** command. To disable this feature, use the **no** form of the command.

dpvm auto-learn
no dpvm auto-learn

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

When autolearn is enabled, the system automatically creates the DPVM database by learning about devices currently logged or newly logged devices with a VSAN. This is a quick way to create the DPVM which can later be edited. Autolearn features include the following:

- An autolearned entry is created by adding the device PWWN and VSAN to the active DPVM database.
- The active DPVM database must be present when autolearning is enabled.
- Autolearned entries can be deleted from the active DPVM database by the user until autolearning is disabled. Autolearned entries are not permanent in the active DPVM database until autolearning is disabled.
- If a device logs out when autolearning is enabled, the device entry is deleted from the active DPVM database.
- If a particular device logs into the switch multiple times through different ports, then only the VSAN corresponding to last login is associated with the device.
- Autolearn entries do not override previously configured activate entries.

Examples

The following example shows how to enable autolearning for the DPVM database:

```
switch# config terminal
switch(config)# dpvm auto-learn
```

The following example shows how to disable autolearning for the DPVM database:

```
switch# config terminal
switch(config)# no dpvm auto-learn
```

Related Commands

Command	Description
dpvm enable	Enables DPVM.
show dpvm	Displays DPVM database information.

dpvm commit

To apply the pending configuration pertaining to the dynamic port VSAN membership (DPVM) Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **dpvm commit** command.

dpvm commit

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Examples

The following example shows how to commit changes to the DPVM database:

```
switch# config terminal
switch(config)# dpvm commit
```

Related Commands

Command	Description
dpvm distribute	Enables CFS distribution for DPVM.
dpvm enable	Enables DPVM.
show dpvm	Displays DPVM information.

dpvm database

To activate and configure the dynamic port VSAN membership (DPVM) database, use the **dpvm database** command. To deactivate the database, use the **no** form of the command.

dpvm database
no dpvm database

Syntax Description

This command has no other arguments or keywords.

Command Default

Deactivated.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

The DPVM database consists of a series of device mapping entries. Each entry consists of device pWWN or nWWN along with the dynamic VSAN to be assigned. Use the **nwwn** command or **pwwn** command to add the entries to the DPVM database. This database is global to the whole switch (and fabric) and is not maintained for each VSAN.

Examples

The following example shows how to activate the DPVM database and enter DPVM database configuration submode:

```
switch# config terminal
switch(config)# dpvm database
switch#(config-dpvm-db)#
```

The following example shows how to activate the DPVM database and enter nWWN device:

```
switch#(config-dpvm-db)# nwwn 14:21:30:12:63:39:72:81 vsan 101
Successful. Commit should follow for command to take effect.
excal-178(config-dpvm-db)#
```

The following example shows how to activate the DPVM database and enter pWWN device:

```
switch#(config-dpvm-db)# pwwn 14:21:30:12:63:39:72:81 vsan 101
Successful. Commit should follow for command to take effect.
switch#(config-dpvm-db)#
```

Related Commands

Command	Description
dpvm enable	Enables DPVM.
nwwn (DPVM database configuration submode)	Adds entries to the DPVM database using the nWWN.

Command	Description
pwwn (DPVM database configuration submode)	Adds entries to the DPVM database using the pWWN.
show dpvm	Displays DPVM database information.

dpvm database copy active

To copy the active dynamic port VSAN membership (DPVM) database to the config DPVM database, use the **dpvm database copy active** command.

dpvm database copy active

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

The following circumstances may require the active database to be copied to the config database:

- When the autolearned entries are only added to the active database.
- When the config database or entries in the config database are accidently deleted.

Note If you want to copy the DPVM database and fabric distribution is enabled, you must first commit the changes.

Examples

The following example shows how to copy the active DPVM database to the config DPVM database:

```
switch# dpvm database copy active
```

Related Commands

Command	Description
dpvm enable	Enables DPVM.
show dpvm	Displays DPVM database information.

dpvm database diff

To display the active dynamic port VSAN membership (DPVM) database, use the **dpvm database diff** command.

dpvm database diff {**active**|**config**}

Syntax Description

active	Displays differences in the DPVM active database compared to the DPVM config database.
config	Displays differences in the DPVM config database compared to the DPVM active database.

Command Default

Deactivated.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Examples

The following example displays the differences in the DPVM active database when compared with the DPVM config database:

```
switch# dpvm database diff active
Legend: "+" New Entry, "-" Missing Entry, "*" Possible Conflict Entry
------------------------------------------------------------------
- pwwn 44:22:33:44:55:66:77:88 vsan 44
* pwwn 11:22:33:44:55:66:77:88 vsan 11
```

The following example displays the differences in the DPVM config database when compared with the DPVM active database:

```
switch# dpvm database diff config
Legend: "+" New Entry, "-" Missing Entry, "*" Possible Conflict Entry
------------------------------------------------------------------
- pwwn 44:22:33:44:55:66:77:88 vsan 44
* pwwn 11:22:33:44:55:66:77:88 vsan 11
```

Related Commands

Command	Description
dpvm enable	Enables DPVM.
show dpvm	Displays DPVM database information.

dpvm distribute

To enable Cisco Fabric Services (CFS) distribution for dynamic port VSAN membership (DPVM), use the **dpvm distribute** command. To disable this feature, use the **no** form of the command.

dpvm distribute
no dpvm distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Temporary changes to the DPVM database must be committed to the active DPVM database using the **dpvm commit** command before being distributed to the fabric.

Examples

The following example shows how to disable distribution for the DPVM database:

```
switch# config terminal
switch(config)# no dpvm distribute
```

The following example shows how to enable distribution for the DPVM database:

```
switch# config terminal
switch(config)# dpvm distribute
```

Related Commands

Command	Description
dpvm enable	Enables DPVM.
show dpvm	Displays DPVM information.

dpvm enable

To enable dynamic port VSAN membership (DPVM), use to **dpvm enable** command. To disable DPVM, use the **no** form of the command.

dpvm enable
no dpvm enable

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

The configuration and verification commands for DPVM are only available when DPVM is enabled on the switch. When you disable this feature, all related configurations are automatically discarded.

Examples

The following example shows how to enable DPVM:

```
switch# config terminal
switch(config)# dpvm enable
```

Related Commands

Command	Description
dpvm activate	Activates the DPVM database.
dpvm database	Configures the DPVM database.
show dpvm	Displays DPVM database information.

dpvm overwrite-duplicate-pwwn

To overwrite the first login information with the duplicate PWWN login, use the **dpvm overwrite-duplicate-pwwn** command.

dpvm overwrite-duplicate-pwwn

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to overwrite the DPVM duplicate PWWN login:

```
switch#(config)# dpvm overwrite-duplicate-pwwn
switch#(config)#
```

dscp

To configure a differentiated services code point (DSCP) in a QoS policy map class, use the **dscp** command in EXEC mode. To disable this feature, use the **no** form of the command.

dscp *value*
no dscp *value*

Syntax Description

value	Configures the DSCP value. The range is 0 to 63. DSCP value 46 is reserved.

Command Default

The default DSCP value is 0.

Command Modes

QoS policy map class configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Before you can configure a QoS policy map class you must complete the following:

- Enable the QoS data traffic feature using the **qos Enable** command.
- Configure a QoS class map using the **qos Class-map** command.
- Configure a QoS policy map using the **qos Policy-map** command.
- Configure a QoS policy map class using the **class** command.

Examples

The following example configures a DSCP value of 56 in QoS policy classMap1:

```
switch(config-pmap)# class classMap1
switch(config-pmap-c)# ?
Configure class-map set params:
  do        EXEC command
  dscp      DSCP for frames matching class-map.
  exit      Exit from this submode
  no        Negate a command or set its defaults
  priority  Priority to be used for frames matching class-map
switch(config-pmap-c)#
switch(config-pmap-c)# ?
Configure class-map set params:
  do        EXEC command
  dscp      DSCP for frames matching class-map.
  exit      Exit from this submode
  no        Negate a command or set its defaults
  priority  Priority to be used for frames matching class-map
switch(config-pmap-c)# dscp ?
  <0-63>  DSCP value. DSCP of 46 is disallowed.
switch(config-pmap-c)# dscp 56 ?
  <cr>  Carriage Return
switch(config-pmap-c)# dscp 56
Operation in progress. Please check class-map parameters
switch(config-pmap-c)# priority ?
  high    Frames matching class-map get high priority
```

```
  low     Frames matching class-map get low priority
  medium  Frames matching class-map get medium priority
switch(config-pmap-c)# priority low ?
  <cr>  Carriage Return
switch(config-pmap-c)# priority low
Operation in progress. Please check class-map parameters
switch(config-pmap-c)#
```

Related Commands

Command	Description
class	Configure a QoS policy map class.
qos class-map	Configures a QoS class map.
qos enable	Enables the QoS data traffic feature on the switch.
qos policy-map	Configure a QoS policy map.
show qos	Displays the current QoS settings.

duplicate-message throttle

To enable throttling of duplicate Call Home alert messages, use the **duplicate-message throttle** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

duplicate-message throttle
no duplicate-message throttle

Syntax Description

This command has no other arguments or keywords.

Command Default

Enabled.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

The rate of throttling is a maximum of thirty messages in 2 hours.

Examples

The following example shows how to enable throttling of duplicate Call Home alert messages:

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

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.

E Commands

egress-sa

To configure the Security Association (SA) to the egress hardware, use the **engress-sa** command. To delete the SA from the egress hardware, use the no form of the command.

engress-sa *spi-number*
no engress-sa *spi-number*

Syntax Description

spi-number	The range is from 256 to 4294967295.

Command Default

None.

Command Modes

Configuration submode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure the SA to the egress hardware:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface fc 2/1 - 3
switch(config-if)# fcsp esp manual
switch(config-if-esp)# egress-sa 258
switch(config-if-esp)#
```

Related Commands

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

email-contact

To configure an e-mail contact with the Call Home function, use the **email-addr** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

email-addr *email-address*
no email-addr *email-address*

Syntax Description

email-address	Configures an e-mail address. Uses a standard e-mail address that does not have any text size restrictions.

Command Default

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure e-mail contact in the Call Home configuration:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# email-contact username@company.com
```

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.

empty

To remove all steps of the user-configured algorithm, use the **empty** command in configuration mode.

empty

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration Secure Erase algorithm submode

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to remove all steps of the user-configured algorithm:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 algorithm 0
switch (config-se-algo)# empty
```

Related Commands

Command	Description
add-step dynamic	Adds a dynamic pattern step to a specific algorithm.
add-step static	Adds static pattern step to a specific algorithm.

enable

To turn on the privileged commands, use the **enable** command. To disable this feature, use the **disable** command.

enable *privilege-level*

Syntax Description

privilege-level	Specifies privilege level. Default value is 15.

Command Default

Enabled.

Command Modes

EXEC mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to turn on the privileged commands:

```
switch# enable 15
switch#
```

Related Commands

Command	Description
enable secret	Displays the secret for privilege escalation.

enable (Call Home configuration submode)

To enable the Call Home function, use the **enable** command in Call Home configuration submode. To disable this feature, use the **disable** command.

enable

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

To disable the Call Home function, use the **disable** command:

Examples

The following example shows how to enable the Call Home function.

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

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.

enable user-server-group

To enable or disable group validation, use the **enable user-server-group** command. To disable this feature, use the **no** form of the command.

enable user-server-group
no enable user-server-group

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration submode.

Command History

Release	Modification
NX-OS 5.0	This command was introduced.

Usage Guidelines

None.

Examples

```
The following example shows how to enable group validation:
switch(config-ldap)# enable user-server-group
switch(config-ldap)#
```

Related Commands

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

enable secret

To create secret for privilege escalation, use the **enable secret** command. To disable this feature, use the no form of the command.

enable secret {**0**|**5**} *password* [**priv-lvl** *privilege-level*]
no enable secret {**0**|**5**} *password* [**priv-lvl** *privilege-level*]

Syntax Description

0	Specifies that the secret that follows should be in clear text.
5	Specifies that the secret that follows should be encrypted.
password	Specifies that the secret for user privilege escalation.
priv-lvl	(Optional) Specifies the privilege level to which the secret belongs.
privilege-level	(Optional) Specifies the privilege level. Default value is 15.

Command Default

Enabled.

Command Modes

Global Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to specify the secret that follows should be in clear text:

```
switch(config)# enable secret 0 admin priv-lvl 4
switch(config)#
```

The following example shows how to specify the secret that follows should be encrypted:

```
switch(config)# enable secret 5 admin priv-lvl 4
switch(config)#
```

enable cert-DN-match

To enable or disable cert DN matching, use the **enable cert-DN-match** command. To disable this feature, use the **no** form of the command.

enable cert-DN-match
no enable cert-DN-match

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration submode.

Command History

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

Usage Guidelines

If Cert-DN match is configured, user will be allowed to login only if the user profile lists the subject-DN of the user certificate as authorized for logging in.

Examples

```
The following example shows how to enable cert DN match:
switch(config-ldap)# enable cert-dn-match
switch(config-ldap)#
```

Related Commands

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

encryption

To configure an encryption algorithm for an IKE protocol policy, use the **encryption** command. To revert to the default, use the **no** form of the command.

encryption {**3des**|**aes**|**des**}
no encryption

Syntax Description

3des	Specifies 168-bit DES (3DES).
aes	Specifies 128-bit AES-CBC.
des	Specifies 56-bit DES-CBS.

Command Default

3des

Command Modes

IKE policy configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Examples

The following example shows how to configure the encryption algorithm for the IKE protocol:

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# policy 1
switch(config-ike-ipsec-policy)# encryption 3des
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
policy	Configures IKE policy parameters.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

end

To exit any of the configuration modes and return to EXEC mode, use the **end** command in configuration mode.

end

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
4.1(1b)	Modified the command output.
1.0(2)	This command was introduced.

Usage Guidelines

You can also press **Ctrl-Z** to exit configuration mode.

Examples

The following example shows how to exit from configure mode:

```
switch(config-port-monitor)# end
switch#
```

Related Commands

Command	Description
exit	Exits configuration mode, or any of the configuration modes.

enrollment terminal

To enable manual cut-and-paste certificate enrollment through the switch console, use the **enrollment terminal** command in trust point configuration submode. To revert to the default certificate enrollment process, use the **no** form of the command.

enrollment terminal
no enrollment terminal

Syntax Description

This command has no arguments or keywords.

Command Default

The default enrollment method is manual cut-and-paste, which is the only enrollment method that the MDS switch currently supports.

Command Modes

Trust point configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure trust point enrollment through the switch console:

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# enrollment terminal
```

The following example shows how to discard a trust point enrollment through the switch console:

```
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# no enrollment terminal
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the certificate of the certificate authority.

errdisable detect cause link-down

To error-disable and bring down a port on a link failure, use the **errdisable detect cause link-down** command in the interface configuration submode. To disable this feature, use the **no** form of the command.

errdisable detect cause link-down num-times *count* **duration** *sec*
no errdisable detect cause link-down num-times *count* **duration** *sec*

Syntax Description

num-times	Specifies the flap number.
count	Specifies the count. The range is from 1 to 1023.
duration	Specifies the time in seconds.
sec	The range is from 45 to 2000000. The duration must be equal to or greater than **num-times** multiplied by 45. For example, to configure a port to move to the error disabled state when five bit-errors were detected, the duration must be set to 225 or more seconds.

Command Default

None.

Command Modes

Interface Configuration submode.

Command History

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

Usage Guidelines

The port guard feature is used in environments where the system and application does not adapt quickly and efficiently to a port going down and back up or to a port rapidly cycling up and down which can happen in some failure modes. For example, if the port is going up and down once a second, and the system takes five seconds to stabilize after the port goes down, this situation might cause a more severe failure in the fabric.

The port guard feature gives the SAN administrator the ability to prevent this issue from occurring in environments that are vulnerable to these problems. The port can be configured to stay down after the first failure, or after a specified number of failures in a specified time period. This allows the SAN administration to intervene and control the recovery and avoiding any problems caused by the cycling.

Examples

The following example shows how to configure the port as down when the link flaps once:

```
Switch# configure terminal
Switch (config)# interface fc1/1
Switch (config-if)# errdisable detect cause link-down
```

The following example shows how to configure the port as down when the link flaps 5 times in 225 seconds:

```
Switch# configure terminal
Switch (config)# interface fc1/1
Switch (config-if)# errdisable detect cause link-down num-times 5 duration 225
```

The following example shows how to remove the port guard feature on the interface:

```
Switch# config t
Switch (config)# interface fc1/1
Switch (config-if)# no errdisable detect cause link-down
switch(config)#
```

Related Commands

Command	Description
show interface	Displays the interface status information.
show running-config interface	Displays the running configuration on the interface.
show interface status err-disabled	Displays the Ethernet interface error status information.

errdisable detect cause bit-errors

To enable error-disable detection on bit errors, use the **errdisable detect cause bit-errors** command in the interface configuration submode. To disable this feature, use the **no** form of the command.

errdisable detect cause bit-errors num-times *count* **duration** *seconds*
no errdisable detect cause bit-errors num-times *count* **duration** *seconds*

Syntax Description

num-times	Specifies the number of flaps.
count	Specifies the count. The range is from 1 to 1023.
duration	Specifies the time in seconds.
seconds	The range is from 45 to 2000000. The duration must be equal to or greater than **num-times** multiplied by 45. For example, to configure a port to move to the error disabled state when five bit-errors were detected, the duration must be set to 225 or more seconds.

Command Default

None.

Command Modes

Interface Configuration submode.

Command History

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

Usage Guidelines

The port guard feature is used in environments where the system and application does not adapt quickly and efficiently to a port going down and backup or to a port rapidly cycling up and down which can happen in some failure modes. For example, if the port is going up and down once a second, and the system takes five seconds to stabilize after the port goes down, this situation might cause a more severe failure in the fabric.

The port guard feature gives the SAN administrator the ability to prevent this issue from occurring in environments that are vulnerable to these problems. The port can be configured to stay down after the first failure, or after a specified number of failures in a specified time period. This allows the SAN administration to intervene and control the recovery and avoiding any problems caused by the cycling.

Examples

The following example shows how to enable error-disable detection on bit errors:

```
switch# configure terminal
switch(config)# interface fc1/1
switch(config-if)# errdisable detect cause bit-errors num-times 5 duration 225
```

Related Commands

Command	Description
show interface	Displays the interface status information.
show running-config interface	Displays the running configuration on the interface.
show interface status err-disabled	Displays the Ethernet interface error status information.

errdisable detect cause credit-loss

To enable error-disable detection on a credit loss, use the **errdisable detect cause credit-loss** command in the interface configuration submode. To disable this feature, use the **no** form of the command.

errdisable detect cause credit-loss num-times *count* **duration** *sec*
no errdisable detect cause credit-loss num-times *count* **duration** *sec*

Syntax Description

num-times	Specifies the flap number.
count	Specifies the count. The range is from 1 to 1023.
duration	Specifies the time in seconds.
sec	The range is from 45 to 2000000. The duration must be equal to or greater than **num-times** multiplied by 45. For example, to configure a port to move to the error disabled state when five bit-errors were detected, the duration must be set to 225 or more seconds.

Command Default

None.

Command Modes

Interface Configuration submode.

Command History

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

Usage Guidelines

The port guard feature is used in the environments where the system and application does not adapt quickly and efficiently to a port going down and back up or to a port rapidly cycling up and down which can happen in some failure modes. For example, if the port is going up and down once a second, and the system takes five seconds to stabilize after the port goes down, this situation might cause a more severe failure in the fabric.

The port guard feature gives the SAN administrator the ability to prevent this issue from occurring in environments that are vulnerable to these problems. The port can be configured to stay down after the first failure, or after a specified number of failures in a specified time period. This allows the SAN administration to intervene and control the recovery and avoiding any problems caused by the cycling.

Examples

The following example shows how to enable error-disable detection on a credit loss:

```
Switch# configure terminal
Switch (config)# interface fc1/1
Switch (config-if)# errdisable detect cause credit-loss num-times 5 duration 225
Switch (config-if)#
```

Related Commands

Command	Description
show interface	Displays the interface status information.
show running-config interface	Displays the running configuration on the interface.

Command	Description
show interface status err-disabled	Displays the Ethernet interface error status information.

errdisable detect cause link-reset

To enable error-disable detection on a link reset, use the **errdisable detect cause link-reset** command in the interface configuration submode. To disable this feature, use the **no** form of the command.

errdisable detect cause link-reset num-times *count* **duration** *sec*
no errdisable detect cause link-reset num-times *count* **duration** *sec*

Syntax Description

num-times	Specifies the flap number.
count	Specifies the count. The range is from 1 to 1023.
duration	Specifies the time in seconds.
sec	The range is from 1 to 2000000.

Command Default

None.

Command Modes

Interface Configuration submode.

Command History

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

Usage Guidelines

The port guard feature is used in environments where the system and application does not adapt quickly and efficiently to a port going down and back up or to a port rapidly cycling up and down which can happen in some failure modes. For example, if the port is going up and down once a second, and the system takes five seconds to stabilize after the port goes down, this situation might cause a more severe failure in the fabric.

The port guard feature gives the SAN administrator the ability to prevent this issue from occurring in environments that are vulnerable to these problems. The port can be configured to stay down after the first failure, or after a specified number of failures in a specified time period. This allows the SAN administration to intervene and control the recovery and avoiding any problems caused by the cycling.

Examples

The following example shows how to enable error-disable detection on a link reset:

```
Switch# configure terminal
Switch (config)# interface fc1/1
Switch (config-if)# errdisable detect cause link-reset num-times 5 duration 30
Switch (config-if)#
```

Related Commands

Command	Description
show interface	Displays the interface status information.
show running-config interface	Displays the running configuration on the interface.
show interface status err-disabled	Displays the Ethernet interface error status information.

errdisable detect cause signal-loss

To enable error-disable detection on a signal loss, use the **errdiable detect cause signal-loss** command in the interface configuration submode. To disable this feature, use the **no** form of the command.

errdisable detect cause signal-loss num-times *count* **duration** *sec*
no errdisable detect cause signal-loss num-times *count* **duration** *sec*

Syntax Description

num-times	Specifies the flap number.
count	Specifies the count. The range is from 1 to 1023.
duration	Specifies the time in seconds.
sec	The range is from 1 to 2000000.

Command Default

None.

Command Modes

Interface Configuration submode.

Command History

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

Usage Guidelines

The port guard feature is used in the environments where the system and application does not adapt quickly and efficiently to a port going down and back up or to a port rapidly cycling up and down which can happen in some failure modes. For example, if the port is going up and down once a second, and the system takes five seconds to stabilize after the port goes down, this situation might cause a more severe failure in the fabric.

The port guard feature gives the SAN administrator the ability to prevent this issue from occurring in environments that are vulnerable to these problems. The port can be configured to stay down after the first failure, or after a specified number of failures in a specified time period. This allows the SAN administration to intervene and control the recovery and avoiding any problems caused by the cycling.

Examples

The following example shows how to enable error-disable on a signal loss:

```
Switch# configure terminal
Switch (config)# interface fc1/1
Switch (config-if)# errdisable detect cause signal-loss num-times 5 duration 30
Switch (config-if)#
```

Related Commands

Command	Description
show interface	Displays the interface status information.
show running-config interface	Displays the running configuration on the interface.
show interface status err-disabled	Displays the Ethernet interface error status information.

errdisable detect cause sync-loss

To enable error-disable detection on a sync loss, use the **errdisable detect cause sync-loss** command in the interface configuration submode. To disable this feature, use the **no** form of the command.

errdisable detect cause sync-loss num-times *count* **duration** *sec*
no errdisable detect cause sync-loss num-times *count* **duration** *sec*

Syntax Description

num-times	Specifies the flap number.
count	Specifies the count. The range is from 1 to 1023.
duration	Specifies the time in seconds.
sec	The range is from 1 to 2000000.

Command Default

None.

Command Modes

Interface Configuration submode.

Command History

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

Usage Guidelines

The port guard feature is used in environments where the system and application does not adapt quickly and efficiently to a port going down and back up or to a port rapidly cycling up and down which can happen in some failure modes. For example, if the port is going up and down once a second, and the system takes five seconds to stabilize after the port goes down, this situation might cause a more severe failure in the fabric.

The port guard feature gives the SAN administrator the ability to prevent this issue from occurring in environments that are vulnerable to these problems. The port can be configured to stay down after the first failure, or after a specified number of failures in a specified time period. This allows the SAN administration to intervene and control the recovery and avoiding any problems caused by the cycling.

Examples

The following example shows how to enable error-disable detection on a synchronized loss:

```
Switch# configure terminal
Switch (config)# interface fc1/1
Switch (config-if)# errdisable detect cause sync-loss num-times 5 duration 30
Switch (config-if)#
```

Related Commands

Command	Description
show interface	Displays the interface status information.
show running-config interface	Displays the running configuration on the interface.
show interface status err-disabled	Displays the Ethernet interface error status information.

errdisable detect cause trustsec-violation

To enable error-disable detection on a trustsec violation, use the **errdisable detect cause trustsec-violation** command in the interface configuration submode. To disable this feature, use the **no** form of the command.

errdisable detect cause trustsec-violation num-times *count* **duration** *sec*
no errdisable detect cause trustsec-violation num-times *count* **duration** *sec*

Syntax Description

num-times	Specifies the flap number.
count	Specifies the count. The range is from 1 to 1023.
duration	Specifies the time in seconds.
sec	The range is from 1 to 2000000.

Command Default

None.

Command Modes

Interface Configuration submode.

Command History

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

Usage Guidelines

The port guard feature is used in environments where the system and application does not adapt quickly and efficiently to a port going down and back up or to a port rapidly cycling up and down which can happen in some failure modes. For example, if the port is going up and down once a second, and the system takes five seconds to stabilize after the port goes down, this situation might cause a more severe failure in the fabric.

The port guard feature gives the SAN administrator the ability to prevent this issue from occurring in environments that are vulnerable to these problems. The port can be configured to stay down after the first failure, or after a specified number of failures in a specified time period. This allows the SAN administration to intervene and control the recovery and avoiding any problems caused by the cycling.

Examples

The following example shows how to enable error-disable detection on a trustsec violation:

```
switch#(config-if)# errdisable detect cause trustsec-violation num-times 1 duration 1
switch#(config-if)#
```

Related Commands

Command	Description
show interface	Displays the interface status information.
show running-config interface	Displays the running configuration on the interface.
show interface status err-disabled	Displays the Ethernet interface error status information.

event cli

To configure a CLI command as an EEM applet trigger, use the **event cli** command. To delete the applet trigger, use the **no** form of the command.

event cli [**tag** *tagname*] **match** *expression* [**count** *countnum* [**time** *seconds*]]
no event cli [**tag** *tagname*] **match** *expression* [**count** *countnum* [**time** *seconds*]]

Syntax Description

tag *tagname*	(Optional) Configures an event tag identifier. *tagname* specifies a handle for combining multiple events and this handle can be any string value of 1 to 29 characters.
match *expression*	Specifies the regular expression (regexp) used to match the CLI command. The command must have been successfully parsed before a match is attempted. The expression is compared to the fully expanded command and must match exactly, not just part of the command. When the expression contains embedded spaces enclose it in double quotes.
count *countnum*	(Optional) Specifies the number of matching occurrences before an Embedded Event Manager event is triggered. When a number is not specified, an Embedded Event Manager event is triggered after the first match. This number must be an integer greater than 0.
time *seconds*	(Optional) Specifies the time interval during which one or more occurrences must take place. When the keyword is not specified, no time period check is applied.

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

Release	Modification
NX-OS 4.1(2)	This command was introduced.

Usage Guidelines

A cli event trigger allows control over CLI commands. By default, the triggering command is not executed. This allows an applet to take action before or after a command runs, or even prevent it from running. To run the triggering command, configure an event-default action at the stage in the applet where the command should run.

Examples

The following example shows how to match the **shutdown** command as an applet trigger:

```
switch# configure terminal
switch(config)# event manager applet blockShutdownCmd
switch(config-applet)# event cli match "shutdown"
switch(config-applet)# end
```

The following example shows how to use spaces and regular expressions. Action 10 logs a syslog message and action 20 allows the matching command to complete normally.

```
switch# configure terminal
switch(config)# event manager applet fcanalyserCheck
switch(config-applet)# event cli match "fcanalyzer * mgmt*"
switch(config-applet)# action 10 syslog priority emergencies msg fcanalyser command used
for mgmt interface
switch(config-applet)# action 20 event-default
switch(config-applet)# end
```

Related Commands

Command	Description
action	Configure EEM applet actions.
show event manager event-types	Displays information about EEM event triggers.
show event manager history events	Displays the history of EEM events.
show running-config eem	Displays all EEM applets.
tag	Correlate multiple events in an EEM applet. Correlate multiple events in an EEM applet.

event counter

To configure a counter as an EEM applet trigger, use the **event counter** command. To delete the applet trigger, use the **no** form of the command.

event counter [**tag** *tagname*] **name** *name* **entry-val** *value* **entry-op** *operator* [**exit-val** *value* **exit-op** *operator*]
no event counter [**tag** *tagname*] **name** *name* **entry-val** *value* **entry-op** *operator* [**exit-val** *value* **exit-op** *operator*]

Syntax Description

tag *tagname*	(Optional) Configures an event tag identifier. *tagname* specifies a handle for combining multiple events and this handle can be any string value of 1 to 29 characters.
name *name*	Configures the name of the counter to monitor. *name* can be any string value of 1 to 28 characters.
entry-val *value*	Configures a value to compare the named counter against. The event resets immediately unless an exit-val is specified. *value* is an integer in the range from 0 to 2147483647.
entry-op *operator*	Specifies how to compare the current value of the named counter with the specified value. The operator can be one of the following: • **eq**—Equal to • **ge**—Greater than or equal to • **gt**—Greater than • **le**—Less than or equal to • **lt**—Less than • **ne**—Not equal to
exit-val *value*	(Optional) Configures a value that the named counter must reach before resetting the event. *value* is an integer in the range from 0 to 2147483647.
exit-op *operator*	(Optional) Specifies how to compare the current value of the named counter with the specified value. The operator can be one of the following: • **eq** —Equal to • **ge**—Greater than or equal to • **gt**—Greater than • **le**—Less than or equal to • **lt**—Less than • **ne**—Not equal to

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

Release	Modification
NX-OS 4.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to trigger an EEM applet when a counter named 'test' has a value of 0:

```
switch# configure terminal
switch(config)# event manager applet testCtrIsZero
switch(config-applet)# event counter name test entry-val 0 entry-op eq
switch(config-applet)# end
```

Related Commands

Command	Description
show event manager event-types	Displays information about EEM event triggers.
show event manager history events	Displays the history of EEM events.
show running-config eem	Displays all EEM applets.
tag	Correlate multiple events in an EEM applet. Correlate multiple events in an EEM applet.

event fanabsent

To configure a fan absence as an EEM applet trigger, use the **event fanabsent** command. To delete the applet trigger, use the **no** form of the command.

fanabsent [**fan** *fannumber*] **time** *seconds*
no fanabsent [**fan** *fannumber*] **time** *seconds*

Syntax Description

fan *number*	(Optional) Configures a chassis fan. *fannumber* range is platform specific.
time *seconds*	Configures a time period. *seconds* range is 10 to 64000.

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

Release	Modification
NX-OS 4.1(2)	This command was introduced.

Usage Guidelines

This event specification monitors if a fan is removed from the chassis for a particular period of time. Embedded Event Manager takes an action based on the actions configured on the applet.

Examples

This example shows how to configure a an EEM applet to trigger after a fan absence of 300 seconds (5 minutes):

```
switch# configure terminal
switch(config)# event manager applet fanGoneForFiveMins
switch(config-applet)# event fanabsent fan 300
switch(config-applet)# end
```

Related Commands

Command	Description
show event manager event-types	Displays information about EEM event triggers.
show event manager history events	Displays the history of EEM events.
show running-config eem	Displays all EEM applets.

event fanbad

To configure fanbad event specification, use the **event fanbad** command. To remove the fanbad event, use the **no** form of the command.

event fanbad [**fan** *fannumber*] **time** *seconds*
no event fanbad [**fan** *fannumber*] **time** *seconds*

Syntax Description

fan *fannumber*	(Optional) Configures a chassis fan. *fannumber* range is platform specific.
time *seconds*	Configures a time period. *seconds* range is 10 to 64000.

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

Release	Modification
NX-OS 4.1(2)	This command was introduced.

Usage Guidelines

This event specification monitors for the failure of any chassis cooling fan and Embedded Event Manager takes an action based on the actions configured on the applet.

Examples

This example shows how to configure an EEM applet to trigger after a fan failure of 10 seconds:

```
switch# configure terminal
switch(config)# event manager applet applet1
switch(config-applet)# event fanbad time 10
switch(config-applet)# end
```

Related Commands

Command	Description
show event manager event-types	Displays information about EEM event triggers.
show event manager history events	Displays the history of EEM events.
show running-config eem	Displays all EEM applets.

event fcns

To change the maximum number of FC Name Server (FCNS) entries allowed on a switch, use the **event fcns** command. You must override the default system policy **__fcns_entries_max_per_switch** with a new policy to do this. To remove the FCNS event, use the **no** form of the command.

event fcns entries max-per-switch *count*
no event fcns entries max-per-switch *count*

Syntax Description

entries	Specifies FCNS Database entries.
max-per-switch *count*	Specifies an event to configure maximum FCNS database count per switch. *count* specifies the maximum number of FCNS entries the switch will register. *count* range is platform specific.

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

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

Usage Guidelines

The maximum number of name server entries that a switch can support is dependent on the platform. Refer to the *Cisco MDS NX-OS Release 6.2(13) Configuration Limits* document for platform specific limits.

Examples

This example shows how to configure an Embedded Event Manager event when the FCNS database count per switch reaches a maximum:

```
switch# configure terminal
switch(config)# event manager applet fcns_policy override __fcns_entries_max_per_switch
switch(config-applet)# event fcns entries max-per-switch 9000
switch(config-applet)# end
```

Related Commands

Command	Description
show event manager event-types	Displays information about EEM event triggers.
show event manager history events	Displays the history of EEM events.
show running-config eem	Displays all EEM applets.

event flogi

To trigger an Embedded Event Manager (EEM) policy when certain fabric login (FLOGI) thresholds are exceeded, use the **event flogi** command. To remove the FLOGI event detection from the EEM policy, use the **no** form of this command.

event flogi {**intf-max** |**module-max** |**switch-max**} *count*
no event flogi {**intf-max** |**module-max** |**switch-max**} *count*

Syntax Description

intf-max	Triggers an event when the number of successful and pending FLOGIs for any Fibre Channel interface exceeds the specified threshold.
module-max	Triggers an event when the number of successful and pending FLOGIs for any module exceeds the specified threshold.
switch-max	Triggers an event when the number of successful and pending FLOGIs for the switch exceeds the specified threshold.
count	Specifies the threshold value. The threshold value must be a positive integer. The FLOGI limit range per interface, module, and switch is platform specific. For more information on FLOGI limits for different platforms, see the Cisco MDS NX-OS Configuration Limits document.

Command Default

None.

Command Modes

EEM applet configuration (config-applet)

Command History

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

Usage Guidelines

To use these FLOGI event triggers you must override the corresponding default system policies with a new policy. The default system policies are:

event flogi	corresponding system policy
intf-max	**__flogi_fcid_max_per_intf**
module-max	**__flogi_fcid_max_per_module**
switch-max	**__flogi_fcid_max_per_switch**

Examples

This example shows an event trigger that occurs when the number of FLOGIs per interface exceeds the threshold value of 156:

```
switch# configure terminal
switch(config)# event manager applet flogiint override __flogi_fcids_max_per_intf
switch(config-applet)# event flogi intf-max 156
switch(config-applet)# end
```

This example shows an event trigger that occurs when the number of FLOGIs per module exceeds the threshold value of 1024:

```
switch# configure terminal
switch(config)# event manager applet flogimod override __flogi_fcids_max_per_module
switch(config-applet)# event flogi module-max 1024
switch(config-applet)# end
```

This example shows an event trigger that occurs when the number of FLOGIs per switch exceeds the threshold value of 2000:

```
switch# configure terminal
switch(config)# event manager applet flogiswitch override __flogi_fcids_max_per_switch
switch(config-applet)# event flogi switch-max 2000
switch(config-applet)# end
```

Related Commands

Command	Description
show event manager event-types	Displays information about EEM event triggers.
show event manager history events	Displays the history of EEM events.
show event manager system-policy	Displays default system policies.
show running-config eem	Displays all EEM applets.

event gold

To create an online diagnostic test failure related event, use the **event gold** command. To remove the online diagnostic test failure related event, use the **no** form of the command.

event gold module {*number* |**all**} **test** *name* [**severity** {**minor** |**moderate** |**major**}] **testing-type**{**scheduled | monitoring**} **consecutive-failure** *count*
no event gold module {*number* |**all**} **test** *name* [**severity** {**minor** |**moderate** |**major**}] **testing-type**{**scheduled | monitoring**} **consecutive-failure** *count*

Syntax Description

number	Specifies the module number.
all	Selects all the module IDs.
test *name*	Selects the diagnostic test. *name* specifies the test name.
severity	Specifies the severity of the failure. It has the following values: • **minor**—Minor failure • **moderate**—Moderate failure • **major**—Major failure
testing-type	Specifies the type of testing. It has the following values: • **scheduled**—(Deprecated) Scheduled test • **monitoring**—Monitoring test
consecutive-failure *count*	Specifies the consecutive number of times the failure has occurred. *count* specifies the failure count and the value is between 1 to 1000.

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

Release	Modification
NX-OS 6.2	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to configure an EEM event when the GOLD ASICRegisterCheck test fails on all modules 10 consecutive times.

```
switch# configure terminal
switch(config)# event manager applet gold
```

```
switch(config-applet)# event gold module all test ASICRegisterCheck testing-type monitoring
 consecutive-failure 10
```

This example shows how to configure an EEM event when the GOLD PwrMgmtBus test fails on module 5 only 20 consecutive times.

```
switch# configure terminal
switch(config)# event manager applet gold
switch(config-applet)# event gold module 5 test PwrMgmtBus testing-type monitoring
consecutive-failure 20
```

Related Commands

Command	Description
show event manager history events	Displays the history of EEM events.
show running-config eem	Displays all EEM applets.

event memory

To configure memory thresholds event specification, use the **event memory** command. To remove the memory threshold event, use the **no** form of the command.

event memory {**minor** |**severe** |**critical**}
no event memory {**minor** |**severe** |**critical**}

Syntax Description

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

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

Release	Modification
NX-OS 4.1(2)	This command was introduced.

Usage Guidelines

The event specification monitors the memory threshold specified in the applet and Embedded Event Manager takes an action based on the actions configured on the applet.

Examples

This example shows how to configure memory threshold event specification:

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

Related Commands

Command	Description
show event manager event-types	Displays information about EEM event triggers.
show event manager history events	Displays the history of EEM events.
show running-config eem	Displays all EEM applets.
show system internal memory-alerts-log	Displays the log of memory alerts.

event module

To configure the module event specification, use the **event module** command. To remove the module event specification, use the **no** form of the command.

event module [**tag** *tagname*] **status** {**online** |**offline** |**any**} **module** {**all** *slot*}
no event module [**tag** *tagname*] **status** {**online** |**offline** |**any**} **module** {**all** *slot*}

Syntax Description

tag *tagname*	(Optional) Configures an event tag identifier. *tagname* specifies a handle for combining multiple events and this handle can be any string value of 1 to 29 characters.
status	Configures the status condition.
online	Specifies module status changed to online.
offline	Specifies module status changed to offline.
any	Specifies module status changed to online or offline.
module	Configures which modules to monitor.
all	Specifies all modules.
slot	Specifies a module number. The range is platform specific.

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

Release	Modification
NX-OS 4.1(2)	This command was introduced.

Usage Guidelines

This event specification monitors the module status change. Embedded Event Manager takes an action based on the actions configured on the applet.

Examples

This example shows how to configure the module event specification in the device:

```
switch# configure terminal
switch(config)# event manager applet bad-applet
switch(config-applet)# event module status any module all
switch(config-applet)# action 1.0 syslog priority informational msg "module status changed"
switch(config-applet)# end
```

Related Commands

Command	Description
show event manager event-types	Displays information about EEM event triggers.

Command	Description
show event manager history events	Displays the history of EEM events.
show running-config eem	Displays all EEM applets.

event module-failure

To create a module failure event specification, use the **event module-failure** command. To remove the module failure event, use the **no** form of the command.

event module-failure [**tag** *tagname*] **type** *failure-type* **module** {**all** *slot*} **count** *count* [**time** *seconds*]
no event module-failure [**tag** *tagname*] **type** *failure-type* **module** {**all** *slot*} **count** *count* [**time** *seconds*]

Syntax Description

tag *tagname*	(Optional) Configures an event tag identifier. *tagname* specifies a handle for combining multiple events and this handle can be any string value of 1 to 29 characters.

type *failure-type*	Configures the failure type to monitor. *failure-type* specifies whether one or all modules must be monitored. *failure-type* specifies the type of failure conditions listed below: • addon-sequence-failure—Addon sequence failure • any • hitless-upgrade-diag-failure—Runtime diag failure after hitless upgrade • hitless-upgrade-failure—Hitless upgrade failure • hitless-upgrade-procmgr-notif—LC software failure after hitless upgrade • hitless-upgrade-reg-failure—Registration failure after hitless upgrade • hitless-upgrade-seq-timeout—Hitless upgrade sequence timeout • image-download-failed—Image download failure • image-upgrade-failed—Image upgrade failed • insertion-seq-failure—Insertion sequence failure • lc-failed—LC failed • lc-not-responding—LC not responding • lc-ready-timeout—LC ready timeout • lc-sw-failure—LC software failure • registration-failure—Registration failure • registration-timeout—Registration timeout • runtime-diag-failure—Runtime diag failure • runtime-diag-timeout—Runtime diag timeout • sequence-timeout—Sequence timeout • srg-info-resp-timeout—SRG info response timeout • unexpected-registration—Unexpected registration received • upgrade-srg-not-compatible—Upgrade SRG not compatible
module	Configures which modules to monitor.
all	Specifies all modules.
slot	Specifies a module number. The range is platform specific.
count *count*	Configures the number of matching occurrences before an Embedded Event Manager event is triggered. *count* specifies the number of repeated occurrences and this number must be an integer in the range 0 to 4294967295.

time *seconds*	(Optional) Configures a time period. *seconds* is the period of module in failure state in seconds and this number must be an integer in the range 0 to 10000000.

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

Release	Modification
NX-OS 4.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to configure a module failure event specification:

```
switch# configure terminal
switch(config)# event manager applet modfailed
switch(config-applet)# event module-failure type lc-failed module all count 1
switch(config-applet)# action 1.0 syslog priority critical msg module failure detected
switch(config-applet)# end
```

Related Commands

Command	Description
show event manager event-types	Displays information about EEM event triggers.
show event manager history events	Displays the history of EEM events.
show running-config eem	Displays all EEM applets.
tag	Correlate multiple events in an EEM applet. Correlate multiple events in an EEM applet.

event oir

To configure an Online Insertion Removal event specification, use the **event oir** command. To remove the Online Insertion Removal event, use the **no** form of the command.

event oir [**tag** *tagname*] {**fan** |**module** |**powersupply**} {**insert** |**remove** |**anyoir**} [*number*]
no event oir [**tag** *tagname*] {**fan** |**module** |**powersupply**} {**insert** |**remove** |**anyoir**} [*number*]

Syntax Description

tag *tagname*	(Optional) Configures an event tag identifier. *tagname* specifies a handle for combining multiple events and this handle can be any string value of 1 to 29 characters.
fan	Specifies the system fans. Optionally, specifies an individual fan.
module	Specifies the system modules. Optionally, specifies an individual module.
powersupply	Specifies the system power supplies. Optionally, specifies an individual power supply.
insert | **remove** | **anyoir**	Specify the OIR event that triggers the Embedded Event Manager applet. • **insert**—OIR insert • **remove**—OIR remove • **anyoir**—Either OIR insert or OIR remove
number	(Optional) If you select fan, enter a fan number to monitor for an OIR event. The range is platform specific. If you select module, enter a module number to monitor an OIR event. The range is platform specific. If you select power supply, enter a power supply number to monitor an OIR event. The range is platform specific.

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

Release	Modification
NX-OS 4.1(2)	This command was introduced.

Usage Guidelines

This event specification monitors whenever there is insertion or removal of the following components: fan, module, and power supply. Embedded Event Manager takes an action based on the actions configured on the applet.

Examples

This example shows how to configure the Online Insertion Removal event specification:

```
switch# configure terminal
switch(config)# event manager applet moduleOir
switch(config-applet)# event oir module anyoir
```

```
switch(config-applet)# action 1.0 syslog priority informational msg a module was oir-ed
switch(config-applet)# end
```

Related Commands

Command	Description
show event manager event-types	Displays information about EEM event triggers.
show event manager history events	Displays the history of EEM events.
show running-config eem	Displays all EEM applets.
tag	Correlate multiple events in an EEM applet. Correlate multiple events in an EEM applet.

event policy-default

To configure the event specification when the system policy is overridden, use the **event policy-default** command. To remove the configuration, use the **no** form of the command.

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

Syntax Description

count *count*	Configures the number of matching occurrences before an event is triggered. *count* specifies the number of repeated occurrences and this number must be an integer in the range 0 to 65000.
time *seconds*	(Optional) Configures the time interval during which one or more occurrences must take place. When this option is not specified no time limit is applied. *seconds* specifies the number of seconds and this number must be an integer in the range 0 to 4294967295.

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

Release	Modification
NX-OS 4.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to configure an event configuration when the system policy is overridden:

```
switch# configure terminal
switch(config)# event manager applet applet1
switch(config-applet)# event policy-default count 1
switch(config-applet)# end
```

Related Commands

Command	Description
show event manager history events	Displays the history of EEM events.
show running-config eem	Displays all EEM applets.

event poweroverbudget

The power over-budget policy gets triggered when the available power capacity drops below zero and the device is no longer able to keep the previously powered-up modules in the powered-up state. The default action is to print a syslog to notify the user of the occurrence of power over budget. To change the power over budget behavior, use the **event poweroverbudget** command. You must override the default system policy **__pfm_power_over_budget** with a new policy to do this. To remove the power over-budget event specification, use the **no** form of the command.

event poweroverbudget
no event poweroverbudget

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

Release	Modification
NX-OS 4.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to shut down modules starting from module 1 when the available power drops below zero:

```
switch# configure terminal
switch(config)# event manager applet pobOverride override __pfm_power_over_budget
switch(config-applet)# event poweroverbudget
switch(config-applet)# event 4 overbudgetshut
switch(config-applet)# end
```

Related Commands

Command	Description
show event manager event-types	Displays information about EEM event triggers.
show event manager history events	Displays the history of EEM events.
show running-config eem	Displays all EEM applets.

event snmp

To configure an SNMP event, use the **event snmp** command. To remove the SNMP event, use the **no** form of the command.

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

Syntax Description

tag *tagname*	(Optional) Configures an event tag identifier. *tagname* specifies a handle for combining multiple events and this handle can be any string value of 1 to 29 characters.
oid *oid*	Configures the OID to monitor. *oid* in dot notation.
get-type	Retrieve the OID exactly as specified.
exact	Retrieves the object ID specified by the OID value argument.
next	Retrieve the OID that is the alphanumeric successor to the named OID.
entry-op	Configures how to compare the value of the current OID with the specified value.
Operator	A logical operator with the following meanings: • **eq**—Equal to • **ge**—Greater than or equal to • **gt**—Greater than • **le**—Less than or equal to • **lt**—Less than • **ne**—Not equal to
entry-val *value*	Configures a value to compare against the current OID. *value* specifies a value and this number is an integer in the range from 0 to 2147483647.
exit-comb	(Optional) Configures a combination of exit conditions that must be met before event monitor is re-enabled.
and	(Optional) Specifies that an exit OID value and an exit time value must be reached.
or	(Optional) Specifies that an exit OID value or an exit time value must be reached.
exit-op	Configures how to compare the value of the current OID with the exit value. If there is a match an event is triggered and event monitoring is reenabled.

exit-val *value*	Configures the value with which the contents of the current OID are compared to decide whether the exit criteria are met. *value* specifies a value and this number is an integer in the range from 0 to 2147483647.
exit-time *time*	(Optional) Configures the time period after which the event monitoring is reenabled. The timing starts after the event is triggered. *time* is an integer in the range from 1 to 2147483647.
poll-interval	Configures the time interval between consecutive polls.

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

Release	Modification
NX-OS 4.1(2)	This command was introduced.

Usage Guidelines

An Embedded Event Manager event is triggered when one of the fields specified by an SNMP object ID crosses a defined threshold. If multiple conditions exist, the SNMP event is triggered when all the conditions are met.

Exit criteria are optional. If exit criteria are not specified, event monitoring will be re-enabled immediately. If exit criteria are specified on the basis of values or time periods, the event monitoring is not re-enabled until the criteria are met.

When the **entry-op** keyword is used and there is a match, an event is triggered and event monitoring is disabled until the exit criteria are met.

When the **exit-op** keyword is used and there is a match, an event is triggered and event monitoring is re-enabled.

The **entry-type** keyword triggers one of the following actions:

- If the **value** keyword is specified, the entry-value is an actual value and an SNMP event is raised whenever the absolute value occurs.
- If the **increment** keyword is specified, the entry-value is an increment and an SNMP event is raised whenever the incremental value is reached.
- If the **rate** keyword is specified, the entry-value is a rate of change and an SNMP event is raised whenever the rate of change value is reached.

When the optional **exit-type** keyword is used, the following conditions occur:

- If the **value** keyword is specified, the exit value is an actual value and the event monitoring is re-enabled whenever the absolute value occurs. This is the default.
- If the **increment** keyword is specified, the exit value is an increment and the event monitoring is re-enabled whenever the incremental value is reached.
- If the **rate** keyword is specified, the exit value is a rate of change and the event monitoring is re-enabled whenever the rate of change value is reached.

Examples

The following example shows how to monitor the CPU free memory OID and log a corresponding syslog:

```
switch# configure terminal
switch(config)# event manager applet snmp-applet
switch(config-applet)# event snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.13.1 get-type exact
entry-op lt entry-val 100000 poll-interval 60
switch(config-applet)# action 1.0 syslog priority warnings msg free memory fell below 100
Mb
switch(config-applet)# end
```

Related Commands

Command	Description
show event manager event-types	Displays information about EEM event triggers.
show event manager history events	Displays the history of EEM events.
show running-config eem	Displays all EEM applets.
tag	Correlate multiple events in an EEM applet. Correlate multiple events in an EEM applet.

event storm-control

By default, the packet storm feature takes limited action. The packet storm feature can be augmented with further actions, such as disabling the affected interface or sending SNMP traps, by using an EEM applet. To configure a packet storm event as an EEM applet trigger, use the **event storm-control** command. To delete the applet trigger, use the **no** form of the command.

event storm-control
no event storm-control

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

Release	Modification
NX-OS 4.1(2)	This command was introduced.

Usage Guidelines

This command is only available on platforms that support the packet storm feature.

Examples

The following example show how to shutdown an interface that exceeds the packet storm feature thresholds:

```
switch# configure terminal
switch(config)# event manager applet stormControlOverride
switch(config-applet)# event storm-control
switch(config-applet)# action 10 cli command "configure terminal"
switch(config-applet)# action 20 cli command "interface $interface"
switch(config-applet)# action 30 cli command "shutdown"
switch(config-applet)# action 40 cli command "end"
switch(config-applet)# action 50 syslog priority notifications msg Storm control: $interface
 shutdown due to $cause
switch(config-applet)# end
```

Related Commands

Command	Description
show event manager event-types	Displays information about EEM event triggers.
show event manager history events	Displays the history of EEM events.
show running-config eem	Displays all EEM applets.
storm-control	Configure packet storm thresholds on an interface.

event syslog

To specify event criteria for an Embeded Event Manager applet that is run by matching syslog messages, use the **event syslog** command in the applet configuration mode. To remove the syslog message event criteria, use the **no** form of the command.

event syslog [**tag** *tagname*] [{**occurs** *count* |**period** *interval* |**priority** {**0-7** |**alerts** |**critical** |**debugging** |**emergencies** |**errors** |**informational** |**notifications** |**warnings**}}] **pattern** *expression*
no event syslog [**tag** *tagname*] [{**occurs** *count* |**period** *interval* |**priority** {**0-7** |**alerts** |**critical** |**debugging** |**emergencies** |**errors** |**informational** |**notifications** |**warnings**}}] **pattern** *expression*

Syntax Description

tag *tagname*	(Optional) Configures an event tag identifier. *tagname* specifies a handle for combining multiple events and this handle can be any string value of 1 to 29 characters.
occurs *count*	(Optional) Specifies the number of occurrences of the matched syslog messages to count before triggering the policy event. *count* range is platform specific.
period *interval*	(Optional) Specifies the maximum time within which the timestamps of the triggering messages must fall. *interval* range is platform specific.
priority	(Optional) Specifies the number or name of the desired priority level at which syslog messages are matched. Messages at or numerically lower than the specified level are matched. The parameter for priority must be one of the following: • **0** | **emergencies**— Specifies syslog messages of emergency level (the system is unusable). • **1** | **alerts**— Specifies syslog messages of alert level (immediate action is needed). • **2** | **critical**— Specifies syslog messages of critical level (critical conditions). • **3** | **errors**— Specifies syslog messages of error level (error conditions). • **4** | **warnings**— Specifies syslog messages of warning level (warning conditions). • **5** | **notifications**— Specifies syslog messages of notification level (normal but significant conditions). • **6** | **informational**— Specifies syslog messages of informational level (informational messages). • **7** | **debugging**— Specifies syslog messages of debugging level (debugging messages).
pattern *expression*	Specifies a regular expression to match against syslog messages. The pattern must be quoted with " " quotes. *expression* maximum size is 256 characters.

Command Default

If the **occurs** parameter is not specified, the default value of 1 is used.

If the **period** parameter is not specified, the default value of 0 is used.

If the **priority** parameter is not specified, the default value of informational is used.

Command Modes

EEM applet configuration (config-applet).

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

The syslog and Embedded Event Manager client processes run on each supervisor module in a system. Therefore, in dual supervisor systems, an **event syslog** command will be matched on both the active and standby supervisors. Both Embedded Event Manager clients will notify the Embedded Event Manager master process on the active supervisor causing the applet to be triggered twice. Be sure to take this potential double triggering in to account in the applet.

This command does not require a license.

Examples

This example shows how to configure an applet to trigger after 10 "authentication failed" syslog events:

```
switch# configure terminal
switch(config)# event manager applet auth-fails-applet
switch(config-applet)# event syslog occurs 10 pattern "authentication failed"
Configuration accepted successfully
```

This example shows how to configure an applet to tag module power up and standby online syslog events:

```
switch# configure terminal
switch(config)# event manager applet mod-event-applet
switch(config-applet)# event syslog tag moduleEvent pattern "(powered up|is standby)"
Configuration accepted successfully
```

Related Commands

Command	Description
action syslog	Configures a syslog message to generate when an EEM applet is triggered.
show event manager history events	Displays the history of EEM events.
tag	Correlate multiple events in an EEM applet. Correlate multiple events in an EEM applet.

event sysmgr

To override default system EEM policies, use the **event sysmgr** command. To remove the system manager-related event specification, use the **no** form of the command.

event sysmgr {**memory** [**module** *mod-number*] **major** *value* **minor** *value* **clear** *value* |**switchover count** *count* **time** *seconds*}
no event sysmgr {**memory** [**module** *mod-number*] **major** *value* **minor** *value* **clear** *value* |**switchover count** *count* **time** *seconds*}

Syntax Description

memory	Configures memory alert thresholds.
module *mod-number*	(Optional) Configures for a module. Default is all modules. *mod-number* specifies a module number and the range is platform specific.
major *value*	Configures the major memory alert threshold. *value* specifies the amount of used memory as a percentage.
minor *value*	Configures the minor memory alert threshold. *value* specifies the amount of used memory as a percentage.
clear *value*	Configures the threshold memory usage must fall below to exit memory alert condition. *value* specifies the amount of used memory as a percentage.
switchover count *count*	Configures switchover rate alert threshold. Configures the number of switchovers. *count* range is from 1 to 65000.
time *seconds*	Configures the time interval during which the switchovers must take place to trigger the event. *seconds* specifies the time period and the range is from 1 to 4294967295 seconds.

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

Release	Modification
NX-OS 4.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following examples show the default system switchover EEM policy and override the default triggering values with user defined values. The default action is retained.

```
switch# show event manager system-policy __sysmgr_swover_count_alert
```

```
 Name : __sysmgr_swover_count_alert
 Description : Switchover count exceeded event. Default value: 20 switchovers within
 1200 seconds. Default action: All linecards will be powered down.
 Overridable : Yes
```

```
switch# configure terminal
switch(config)# event manager applet sup-so-override override __sysmgr_swover_count_alert
switch(config-applet)# event sysmgr switchover count 3 time 300
switch(config-applet)# action 1.0 policy-default
```

```
switch# show event manager system-policy __sysmgr_policy_mem_alert
 Name : __sysmgr_policy_mem_alert
 Description : service memory usage event
 Overridable : Yes
```

```
switch# configure terminal
switch(config)# event manager applet sup-mem-override override __sysmgr_policy_mem_alert
switch(config-applet)# event sysmgr memory major 90 minor 80 clear 70
switch(config-applet)# action 1.0 policy-default
```

Related Commands

Command	Description
show event manager event-types	Displays information about EEM event triggers.
show event manager system-policy	Displays the default system EEM policies.
show event manager history events	Displays the history of EEM events.
show running-config eem	Displays all EEM applets.

event temperature

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

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

Syntax Description

module *slot*	(Optional) Configures for particular modules. *slot* specifies a '-' and ',' delimited range of modules. The values are platform specific.
sensor *number*	(Optional) Configures for particular sensors. *number* specifies a '-' and ',' delimited range of sensors and the values are module specific.
threshold	Specifies the threshold event that triggers the Embedded Event Manager applet.
major	Specifies a major event.
minor	Specifies a minor event.
any	Specifies any event.

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

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

Usage Guidelines

None.

Examples

This example shows the default system major temperature EEM policy and only performs the default action for a major temperature alert for sensor #8 only.

```
switch# show event manager system __pfm_tempev_major
 Name : __pfm_tempev_major
 Description : TempSensor Major Threshold. Action: Shutdown
 Overridable : Yes


switch# configure terminal
switch(config)# event manager applet majortemp_override override __pfm_tempev_major
switch(config-applet)# event temperature module 1-3 sensor 8 threshold major
switch(config-applet)# action 1.0 policy-default
switch(config-applet)# end
```

Related Commands

Command	Description
show event manager event-types	Displays information about EEM event triggers.
show event manager history events	Displays the history of EEM events.
show event manager policy	Displays the register EEM applets.
show event manager system-policy	Displays the default system EEM applets.

event zone

To change the maximum number of zone elements allowed on a switch, use the **event zone** command. You must override the relevant default system policy with a new policy to do this. To remove the zone event criteria, use the **no** form of the command.

event zone {**zones max-per-switch** |**zonesets max-per-switch** |**zonemembers max-per-switch** |**dbsize max-per-vsan**} *count*
no event zone {**zones max-per-switch** |**zonesets max-per-switch** |**zonemembers max-per-switch** |**dbsize max-per-vsan**} *count*

Syntax Description

zones	Specifies Zone count at which Embedded Event Manager event to be triggered.
zonesets	Specifies the zoneset count at which Embedded Event Manager event to be triggered.
zonemembers	Specifies the zone member count at which Embedded Event Manager event to be triggered.
max-per-switch	Configures the maximum value for the switch.
max-per-vsan	Configures the maximum database limit size for the VSAN.
count	Specifies the maximum limit.

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

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

Usage Guidelines

By default, the threshold controlled by the 'zone' events are set by the following system policies:

- __zone_dbsize_max_per_vsan
- __zone_members_max_per_sw
- __zone_zones_max_per_sw
- __zone_zonesets_max_per_sw

These policies log syslog messages when preconfigured thresholds are reached to alert the user of high resource usage by the zone service. The thresholds and actions may be over ridden by the user or the actions augmented by further actions (such as sending an SNMP trap).

Examples

This example shows the default system per VSAN maximum zone database size EEM policy and overrides the database size. The default action is retained.

```
switch(config)# show event manager system-policy __zone_dbsize_max_per_vsan
```

```
Name : __zone_dbsize_max_per_vsan
Description : Syslog warning when Zone database size exceeds the max limit of
4000000 bytes for a vsan.
Overridable : Yes
```

```
switch# configure terminal
switch(config)# event manager applet newzonedb override __zone_dbsize_max_per_vsan
switch(config-applet)# event zone dbsize max-per-vsan 1000000
switch(config-applet)# action 1.0 policy-default
switch(config-applet)# end
```

This example shows how to configure an EEM applet to override the maximum zone count on a system:

```
switch# configure terminal
switch(config)# event manager applet zonemaxsw override __zone_zones_max_per_sw
switch(config-applet)# action 1.0 syslog priority informational msg "zone zonemaxswitch
override"
switch(config-applet)# end
```

This example shows how to configure an EEM applet to override the maximum zoneset count on a system:

```
switch# configure terminal
switch(config)# event manager applet zonesetmaxsw override __zone_zonesets_max_per_sw
switch(config-applet)# action 1.0 syslog priority informational msg "zone zonesetmaxswitch
 override"
switch(config-applet)# end
```

Related Commands

Command	Description
show event manager event-types	Displays information about EEM event triggers.
show event manager history events	Displays the history of EEM events.
show event manager policy internal	Displays the register EEM applets.
show event manager system-policy	Displays the default system EEM applets.

event manager applet

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

event manager applet *applet-name* [**override** *system-policy*]
no event manager applet *applet-name*

Syntax Description

applet-name	The applet name can be any case-sensitive alphanumeric string up to 29 characters.
override *system-policy*	(Optional) Configures the applet to override an existing system policy. *system-policy* specifies the name of the system policy to override.

Command Default

None.

Command Modes

Global configuration.

Command History

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

Usage Guidelines

None.

Examples

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

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

Related Commands

Command	Description
show event manager history events	Displays the history of EEM events.

event manager environment

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

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

Syntax Description

environment-name	Specifies the name of the EEM environment variable. The variable name can be any case-sensitive alphanumeric string up to 29 characters.
environment-value	Specifies the value of the EEM environment. The variable name can be any case-sensitive alphanumeric string up to 39 characters.

Command Default

None.

Command Modes

Global configuration.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to set an EEM environment variable:

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

Related Commands

Command	Description
show event manager environment	Displays the name and value of the EEM.
show event manager history events	Displays the history of EEM events.
show event manager policy	Displays the register EEM applets.

event manager policy

To register and activate an Embedded Event Manager (EEM) script policy, use the **event manager policy** command in the global configuration mode. To deactivate the script policy, use the **no** form of the command.

event manager policy *policy-script*
no event manager policy *policy-script*

Syntax Description

policy-script	Specifies the Embedded Event Manager policy script. This name becomes the name of the Embedded Event Manager policy. The maximum size of the name is 29 characters.

Command Default

None.

Command Modes

Global Configuration.

Command History

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

Usage Guidelines

User policy scripts must be installed in the bootflash://eem/user_script_policies directory before they can be used. If this directory does not exist, create this directory before the first use of this command and install the policy scripts in it.

The Embedded Event Manager schedules and runs policies on the basis of an event specification that is contained within the policy itself. When the **event manager policy** command is invoked, the Embedded Event Manager examines the policy and registers it to be run when the specified event occurs.

Examples

The following example shows how to register a policy:

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

Related Commands

Command	Description
show event manager history events	Displays the history of EEM events.
event manager applet	Displays an applet with the EEM.

event zone

To change the maximum number of zone elements allowed on a switch, use the **event zone** command. You must override the relevant default system policy with a new policy to do this. To remove the zone event criteria, use the **no** form of the command.

event zone {**zones max-per-switch** |**zonesets max-per-switch** |**zonemembers max-per-switch** |**dbsize max-per-vsan**} *count*
no event zone {**zones max-per-switch** |**zonesets max-per-switch** |**zonemembers max-per-switch** |**dbsize max-per-vsan**} *count*

Syntax Description

zones	Specifies Zone count at which Embedded Event Manager event to be triggered.
zonesets	Specifies the zoneset count at which Embedded Event Manager event to be triggered.
zonemembers	Specifies the zone member count at which Embedded Event Manager event to be triggered.
max-per-switch	Configures the maximum value for the switch.
max-per-vsan	Configures the maximum database limit size for the VSAN.
count	Specifies the maximum limit.

Command Default

None.

Command Modes

EEM applet configuration (config-applet).

Command History

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

Usage Guidelines

By default, the threshold controlled by the 'zone' events are set by the following system policies:

- __zone_dbsize_max_per_vsan
- __zone_members_max_per_sw
- __zone_zones_max_per_sw
- __zone_zonesets_max_per_sw

These policies log syslog messages when preconfigured thresholds are reached to alert the user of high resource usage by the zone service. The thresholds and actions may be over ridden by the user or the actions augmented by further actions (such as sending an SNMP trap).

Examples

This example shows the default system per VSAN maximum zone database size EEM policy and overrides the database size. The default action is retained.

```
switch(config)# show event manager system-policy __zone_dbsize_max_per_vsan
```

```
Name : __zone_dbsize_max_per_vsan
Description : Syslog warning when Zone database size exceeds the max limit of
4000000 bytes for a vsan.
Overridable : Yes
```

```
switch# configure terminal
switch(config)# event manager applet newzonedb override __zone_dbsize_max_per_vsan
switch(config-applet)# event zone dbsize max-per-vsan 1000000
switch(config-applet)# action 1.0 policy-default
switch(config-applet)# end
```

This example shows how to configure an EEM applet to override the maximum zone count on a system:

```
switch# configure terminal
switch(config)# event manager applet zonemaxsw override __zone_zones_max_per_sw
switch(config-applet)# action 1.0 syslog priority informational msg "zone zonemaxswitch
override"
switch(config-applet)# end
```

This example shows how to configure an EEM applet to override the maximum zoneset count on a system:

```
switch# configure terminal
switch(config)# event manager applet zonesetmaxsw override __zone_zonesets_max_per_sw
switch(config-applet)# action 1.0 syslog priority informational msg "zone zonesetmaxswitch
 override"
switch(config-applet)# end
```

Related Commands

Command	Description
show event manager event-types	Displays information about EEM event triggers.
show event manager history events	Displays the history of EEM events.
show event manager policy internal	Displays the register EEM applets.
show event manager system-policy	Displays the default system EEM applets.

exit

To exit any configuration mode or close an active terminal session and terminate the EXEC, use the **exit** command at the system prompt.

exit

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC and configuration modes.

Command History

Release	Modification
4.1(1b)	Modified the command output.
1.0(2)	This command was introduced.

Usage Guidelines

Use the **exit** command at the EXEC levels to exit the EXEC mode. Use the **exit** command at the configuration level to return to privileged EXEC mode. Use the **exit** command in interface configuration mode to return to configuration mode. You also can press **Ctrl-Z**, or use the **end** command, from any configuration mode to return to EXEC mode.

Note The **exit** command is associated with privilege level 0. If you configure AAA authorization for a privilege level greater than 0, this command will not be included in the command set for that privilege level.

Examples

The following example displays an exit from the submode:

```
switch(config-port-monitor)# exit
switch(config)#
```

The following example displays an exit from the interface configuration mode for VRRP to return to the interface configuration mode:

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

The following example displays an exit from the interface configuration mode to return to the configuration mode:

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

The following example shows how to exit an active session (log-out):

```
switch# exit
```

Related Commands

Command	Description
end	Returns you to EXEC mode.

F Commands

fabric

To add a fabric to the cluster, use the fabric command in the Cisco SME cluster configuration submode.

fabric *fabric name*

Syntax Description

fabric name	Specifies the fabric name. The maximum length is 32 characters.

Command Default

None.

Command Modes

Cisco SME cluster configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example adds a fabric named sw-xyz to a cluster:

```
switch# config terminal
switch(config)# sme cluster c1
switch(config-sme-cl)# fabric sw-xyz
```

Related Commands

Command	Description
show sme cluster	Displays information about Cisco SME cluster.

fabric-binding activate

To activate fabric binding in a VSAN, use the **fabric-binding activate** command in configuration mode. To disable this feature, use the **no** form of the command.

fabric-binding activate vsan *vsan-id* **[force]**
no fabric-binding activate vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN. The ID of the VSAN is from 1 to 4093.
force	(Optional) Forces fabric binding activation.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Extended support for fabric binding to Fibre Channel VSANs.

Usage Guidelines

Fabric binding is configured on a per-VSAN basis and can be implemented in both FICON VSANs and Fibre Channel VSANs.

Examples

The following example activates the fabric binding database for the specified VSAN:

```
switch# config terminal
switch(config)# fabric-binding activate vsan 1
```

The following example deactivates the fabric binding database for the specified VSAN:

```
switch(config)# no fabric-binding activate vsan 10
```

The following example activates the fabric binding database for the specified VSAN forcefully, even if the configuration is not acceptable:

```
switch(config)# fabric-binding activate vsan 3 force
```

The following example reverts to the previously, configured state or to the factory default (if no state is configured):

```
switch(config)# no fabric-binding activate vsan 1 force
```

Related Commands

Command	Description
fabric-binding database	Configures a fabric binding database.
fabric-binding enable	Enables fabric binding.

fabric-binding database copy

To copy from the active fabric binding database to the configuration fabric binding database, use the **fabric-binding database copy** command in EXEC mode.

fabric-binding database copy vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN. The ID of the VSAN is from 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Extended support for fabric binding to Fibre Channel VSANs.

Usage Guidelines

Fabric binding is configured on a per-VSAN basis and can be implemented in both FICON VSANs and Fibre Channel VSANs.

If the configured database is empty, this command is not accepted.

Examples

The following example copies from the active database to the configuration database in VSAN 1:

```
switch# fabric-binding database copy vsan 1
```

Related Commands

Command	Description
fabric-binding diff	Provides the differences between the fabric binding databases.

fabric-binding database diff

To view the differences between the active database and the configuration database in a VSAN, use the **fabric-binding database diff** command in EXEC mode.

fabric-binding database diff {**active**|**config**} **vsan** *vsan-id*

Syntax Description

active	Provides information on the differences in the active database with respect to the configuration database.
config	Provides information on the differences in the configuration database with respect to the active database.
vsan *vsan-id*	Specifies the VSAN. The ID of the VSAN is from 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Extended support of fabric binding to Fibre Channel VSANs.

Usage Guidelines

Fabric binding is configured on a per-VSAN basis and can be implemented in both FICON VSANs and Fibre Channel VSANs.

Examples

The following example displays the differences between the active database and the configuration database in VSAN 1:

```
switch# fabric-binding database diff active vsan 1
```

The following example displays information on the differences between the configuration database and the active database:

```
switch# fabric-binding database diff config vsan 1
```

Related Commands

Command	Description
fabric-binding copy	Copies from the active to the configuration fabric binding database.

fabric-binding database vsan

To configure a user-specified fabric binding list in a VSAN, use the **fabric-binding database vsan** command in configuration mode. To disable an FC alias, use the **no** form of the command.

fabric-binding database vsan *vsan-id* **swwn** *switch-wwn* **domain** *domain-id*
no fabric-binding database vsan *vsan-id* **swwn** *switch-wwn* **domain** *domain-id*

Syntax Description

vsan-id	Specifies the VSAN. The ID of the VSAN is from 1 to 4093.
swwn *switch-wwn*	Configures the switch WWN in dotted hex format.
domain *domain-id*	Specifies the specified domain ID. The domain ID is a number from 1 to 239.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Extended support of fabric binding to Fibre Channel VSANs.

Usage Guidelines

Fabric binding is configured on a per-VSAN basis and can be implemented in both FICON VSANs and Fibre Channel VSANs.

In a FICON VSAN, the fabric binding feature requires all sWWNs connected to a switch and their persistent domain IDs to be part of the fabric binding active database. In a Fibre Channel VSAN, only the sWWN is required; the domain ID is optional.

A user-specified fabric binding list contains a list of switch WWNs (sWWNs) within a fabric. If an sWWN attempts to join the fabric, and that sWWN is not on the list or the sWWN is using a domain ID that differs from the one specified in the allowed list, the ISL between the switch and the fabric is automatically isolated in that VSAN and the switch is denied entry into the fabric.

The persistent domain ID must be specified along with the sWWN. Domain ID authorization is required in FICON VSANs where the domains are statically configured and the end devices reject a domain ID change in all switches in the fabric.

Note All switches in a non-FICON VSAN must be running Cisco MDS SAN-OS Release 3.x or later.

Examples

The following example enters the fabric binding database submode and adds the sWWN and domain ID of a switch to the configured database list:

```
switch# config terminal
```

```
switch(config)# fabric-binding database vsan 5
switch(config-fabric-binding)# swwn 21:00:05:30:23:11:11:11 domain 102
```

The following example deletes a fabric binding database for the specified VSAN:

```
switch# config terminal
switch(config)# no fabric-binding database vsan 10
```

The following example deletes the sWWN and domain ID of a switch from the configured database list:

```
switch# config terminal
switch(config)# fabric-binding database vsan 5
switch(config-fabric-binding)# no swwn 21:00:15:30:23:1a:11:03 domain 101
```

Related Commands

Command	Description
fabric-binding activate	Activates fabric binding.
fabric-binding enable	Enables fabric binding.

fabric-binding enable

To enable fabric binding in a VSAN, use the **fabric-binding enable** command. To disable fabric binding, use the **no** form of the command.

fabric-binding enable
no fabric-binding enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Extended support of fabric binding to Fibre Channel VSANs.
NX-OS 4.1(1b)	This command was deprecated.

Usage Guidelines

Fabric binding is configured on a per-VSAN basis and can be implemented in both FICON VSANs and Fibre Channel VSANs.

The fabric binding feature must be enabled in each switch in the fabric that participates in the fabric binding.

Examples

The following example enables fabric binding on that switch:

```
switch# config t
switch(config)# fabric-binding enable
```

The following example disables fabric binding on that switch:

```
switch# config t
switch(config)# no fabric-binding enable
```

Related Commands

Command	Description
fabric-binding activate	Activates fabric binding.
fabric-binding database	Configures a fabric binding database.

fabric-membership

To configure a node to a fabric, use the **fabric-membership** command. To remove the node from the fabric, use the **no** form of the command,

fabric-membership *fabric name*
no fabric-membership *fabric name*

Syntax Description

fabric name	Specifies the fabric name. The maximum length is 32 characters.

Command Default

None.

Command Modes

Cisco SME cluster node configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

Use the **fabric-membership** command to put a node in a fabric. This command has to be configured before the interface sme slot/port [force] can be accepted. It also cannot be removed if the **interface sme** *slot/port* **[force]** command is enabled.

Examples

The following example specifies a fabric to which the node belongs:

```
switch# config t
switch(config)# sme cluster clustername1
switch(config-sme-cl)# node local
switch(config-sme-cl-node)# fabric-membership f1
```

Related Commands

Command	Description
interface sme	Configures the Cisco SME interface to a cluster.
shutdown	Enables or disables an interface.
show interface sme	Displays interface information.

fcalias clone

To clone a Fibre Channel alias, use the **fcalias clone** command.

fcalias clone *origFcalias-Name cloneFcalias-Name* **vsan** *vsan-id*

Syntax Description

origFcalias-Name *cloneFcalias-Name*	Clones a Fibre Channel alias from the current name to a new name. Maximum length of names is 64 characters.
vsan	Specifies the clone Fibre Channel alias is for a VSAN.
vsan-id	The ID of the VSAN is from 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

To disable an FC alias, use the **no** form of the **fcalias name** command.

Examples

The following examples show how to clone a fcalias named origAlias to cloneAlias on VSAN 45:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# fcalias clone origAlias cloneAlias vsan 45
```

Related Commands

Command	Description
show fcalias	Displays the member name information in a Fibre Channel alias (fcalias).

fcalias name

To configure an FC alias, use the **fcalias name** command. To disable an FC alias, use the **no** form of the command.

fcalias name *alias name* **vsan** *vsan-id*
no fcalias name *alias name* **vsan** *vsan-id*

Syntax Description

alias-name	The name of the fcalias. Maximum length is 64 characters.
vsan	The fcalias is for a VSAN.
vsan-id	The ID of the VSAN is from 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

To include multiple members in any alias, use the FCID, fWWN, or pWWN values.

Examples

The following examples show how to configure an fcalias called AliasSample on VSAN 3:

```
switch# config terminal
switch(config)# fcalias name AliasSample
vsan 3
switch(config-fcalias)#
```

Related Commands

Command	Description
member (fcalias configuration mode)	Configures alias member for a specified zone.

fcalias rename

To rename a Fibre Channel alias (fcalias), use the **fcalias rename** command.

fcalias rename *current-name* *new-name* **vsan** *vsan-id*

Syntax Description

current-name	Specifies the current fcalias name. The maximum length is 64.
new-name	Specifies the new fcalias name. The maximum length is 64.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to rename an fcalias:

```
switch# config terminal
switch(config)# fcalias rename oldalias newalias vsan 10
```

Related Commands

Command	Description
fcalias name	Configures fcalias names.
show fcalias	Displays fcalias information.

fcanalyzer local

To configure local Cisco Fabric Analyzer, use the **fcanalyzer local** command in EXEC mode.

fcanalyzer|**ethanalyzer local** [{**interface** {**inband**|**mgmt**} [**capture-filter** *expression*] **[brief]** [[**display-filter** *expression*] [[**limit-captured-frames** *number*] [[**limit-frame-size** *bytes*] [**write** *uri2*]]]]|[**interface** {**inband**|**mgmt**} **[dump-pkt]**]}]

Syntax Description

interface	(Optional) Begins live capture on following interface.
inband	(Optional) Specifies an inband interface (default interface to capture on).
mgmt	(Optional) Specifies an management interface.
capture-filter	(Optional) Filters frames using a capture filter expression.
expression	Specifies capture filter expression.
brief	(Optional) Displays the protocol summary in a brief.
display-filter	(Optional) Filters frames using display filter expression.
expression	Specifies display filter expression.
limit-captured-frames *number*	(Optional) Limits the number of frames captured to 10. The range is 0 to 2147483647 frames. Use 0 if you do not want to limit the captured frames.
limit-frame-size *bytes*	(Optional) Limits the size of the frame captures. The range is 64 to 65536 bytes.
write	(Optional) Saves the captured frames to a specified file.
uri2	The filename to be written in (bootflash: or volatile:).
dump-pkt	Specifies Hex (ASCII) dumps packet, troubleshoot packet analyzer.

Command Default

Number of packets captured by default is changed from 100 to 10.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(1a)	Changed the display-filter syntax description.
NX-OS 4.2(2)	Moved local capture to EXEC mode, added support for capturing on mgmt interface along with inband (fc-interface). Also addded capture-filter support and support for hex dump of packets.
1.0(2)	This command was introduced.

Usage Guidelines

You can capture Fibre Channel control traffic from a switch and decode it without disrupting connectivity and without having to be local to the point of analysis.

Note When you capture on inband interface packets from the supervisor to the line card module are captured and vice versa.

Note Multiword capture and display filter expressions need to be either single-quoted or double-quoted depending on what the expression itself contains.

Note To stop capture at any time press Ctrl+C.

Examples

The following example shows how to display only protocol summary on VSAN1:

```
switch# fcanalyzer local interface inband brief

Capturing on inband interface
  0.000000     ff.fa.01 -> ff.fa.01     FC OHMS(Cisco MDS)
  0.001033     ff.fa.04 -> ff.fa.04     FC OHMS(Cisco MDS)
  4.996424     ff.fa.01 -> ff.fa.01     FC OHMS(Cisco MDS)
  4.997452     ff.fa.04 -> ff.fa.04     FC OHMS(Cisco MDS)
  9.996536     ff.fa.01 -> ff.fa.01     FC OHMS(Cisco MDS)
  9.997470     ff.fa.04 -> ff.fa.04     FC OHMS(Cisco MDS)
 14.996572     ff.fa.01 -> ff.fa.01     FC OHMS(Cisco MDS)
 14.997590     ff.fa.04 -> ff.fa.04     FC OHMS(Cisco MDS)
 19.996463     ff.fa.01 -> ff.fa.01     FC OHMS(Cisco MDS)
 19.997415     ff.fa.04 -> ff.fa.04     FC OHMS(Cisco MDS)
switch#
```

The following example shows how to display capture on inband interface:

```
switch# fcanalyzer local interface inband
Capturing on inband interface
Frame 1 (148 bytes on wire, 148 bytes captured)
    Arrival Time: Apr 15, 2010 11:20:47.577355000
    Time delta from previous packet: 0.000000000 seconds
    Time since reference or first frame: 0.000000000 seconds
    Frame Number: 1
    Packet Length: 148 bytes
    Capture Length: 148 bytes
Ethernet II, Src: 00:00:00:00:00:0a, Dst: 00:00:00:00:ee:00
    Destination: 00:00:00:00:ee:00 (00:00:00:00:ee:00)
    Source: 00:00:00:00:00:0a (00:00:00:00:00:0a)
    Type: Unknown (0xfcfc)
MDS Header(Unknown(0)/Unknown(0))
    MDS Header
        ...0 0000 0111 0110 = Packet Len: 118
        .... 0000 0000 00.. = Dst Index: 0x0000
        .... ..01 0010 0000 = Src Index: 0x0120
        .... 0000 0000 0001 = VSAN: 1
```

```
    MDS Trailer
        EOF: Unknown (0)
        CRC: 0xdeadbeef
Fibre Channel
    R_CTL: 0x20(Extended Link Services/0x0)
switch#
```

The following example shows how to display a hex dump of packets:

```
switch# fcanalyzer local interface inband dump-pkt
Warning:  Couldn't obtain netmask info (eth2: no IPv4 address assigned).
Capturing on eth2
  0.000000     ff.fa.01 -> ff.fa.01     FC OHMS(Cisco MDS)

0000  00 00 00 00 ee 00 00 00 00 00 00 0a fc fc 81 00   ................
0010  00 72 ff 00 01 20 00 01 00 00 00 10 01 00 20 ff   .r... ........ .
0020  fa 01 00 ff fa 01 01 00 00 03 00 00 00 00 ff ff   ................
0030  ff ff 00 00 00 00 00 00 00 00 00 00 03 49 00 00   .............I..
0040  00 29 f6 1f 73 d9 00 00 00 00 00 00 00 00 00 00   .)..s...........
0050  00 00 00 00 00 00 00 ff fa 01 00 ff fa 01 00 00   ................
0060  09 96 00 00 00 00 00 00 00 04 00 00 00 02 00 00   ................
0070  00 00 01 00 00 00 ff ff ff ff 00 09 f5 00 2b 99   ..............+.
0080  86 d2 8b df 4e 02 0b aa aa aa 00 00 de ad be ef   ....N...........

  0.001112 80:57:00:00:cb:07 -> 81:00:00:72:e7:00 LLC I P, N(R) = 127, N(S) = 16
; DSAP NULL LSAP Group, SSAP 68 Command

0000  81 00 00 72 e7 00 80 57 00 00 cb 07 00 10 01 68   ...r...W.......h
0010  20 ff fa 01 00 ff fa 01 01 00 00 03 00 00 00 00    ................
0020  ff ff ff ff 00 00 00 00 00 00 00 00 00 00 03 49   ...............I
0030  00 00 00 29 f6 1f 73 d9 00 00 00 29 f6 1f d4 00   ...)..s....)....
0040  00 00 00 00 00 00 00 00 00 00 ff fa 01 00 ff fa 01   ................
0050  00 00 09 96 00 00 00 00 00 00 00 04 00 00 00 02   ................
0060  00 00 00 00 01 00 00 00 ff ff ff ff 00 09 f5 00   ................
0070  2b 99 86 d2 8b df 4e 02 0b aa aa aa 00 00 de ad   +.....N.........
0080  4d 94                                             M.

  0.001763     ff.fa.04 -> ff.fa.04     FC OHMS(Cisco MDS)

0000  00 00 00 00 ee 00 00 00 00 00 00 0a fc fc 81 00   ................
0010  00 96 ff 80 81 20 00 01 00 00 00 10 01 00 20 ff   ..... ........ .
0020  fa 04 00 ff fa 04 01 00 00 00 00 00 00 00 ff ff   ................
0030  ff ff 00 00 00 00 00 00 00 00 00 00 03 49 00 00   .............I..
0040  00 29 f6 1f fc e2 00 00 00 00 00 00 00 00 00 00   .)..............
0050  00 00 00 00 00 00 00 ff fa 04 00 ff fa 04 00 00   ................
0060  09 96 00 00 00 00 00 00 00 00 00 00 00 01 00 00   ................
0070  00 00 06 08 20 00 06 08 20 00 00 30 d1 00 f6 cc   .... ... ..0....
0080  99 87 01 c8 72 e1 ad c5 a0 dd 09 c3 d6 2d 56 8b   ....r........-V.
0090  18 96 0a 43 2f 90 15 bb 70 63 bd 7b e1 b3 47 7a   ...C/...pc.{..Gz
00a0  3a 49 42 ac 2a ef 71 ca cd 7a 8e a3 a7 e4 00 00   :IB.*.q..z......
00b0  de ad be ef                                       ....

  0.002248 81:20:00:01:cb:07 -> 81:00:00:96:ff:80 LLC I P, N(R) = 127, N(S) = 16
; DSAP NULL LSAP Group, SSAP NetWare Command
```

The following example shows how to use a display filter on inband interface and display its summary:

```
switch# fcanalyzer local interface inband brief display-filter 'mdshdr.vsan==0x1 && (fc.d_id
 == "ff.fa.01") || (fc.s_id == "ff.fa.04")'
Capturing on inband interface
  0.000000     ff.fa.01 -> ff.fa.01     FC OHMS(Cisco MDS)
  0.001782     ff.fa.04 -> ff.fa.04     FC OHMS(Cisco MDS)
```

```
  4.996741     ff.fa.01 -> ff.fa.01     FC OHMS(Cisco MDS)
  4.997725     ff.fa.04 -> ff.fa.04     FC OHMS(Cisco MDS)
  9.996670     ff.fa.01 -> ff.fa.01     FC OHMS(Cisco MDS)
  9.997483     ff.fa.04 -> ff.fa.04     FC OHMS(Cisco MDS)
 14.996623     ff.fa.01 -> ff.fa.01     FC OHMS(Cisco MDS)
 14.997642     ff.fa.04 -> ff.fa.04     FC OHMS(Cisco MDS)
 19.996739     ff.fa.01 -> ff.fa.01     FC OHMS(Cisco MDS)
 19.997554     ff.fa.04 -> ff.fa.04     FC OHMS(Cisco MDS)
switch#
```

The following example shows how to write captured packets in PCAP format and display captures on the screen:

```
switch# fcanalyzer local interface inband display-filter 'mdshdr.vsan==0x1 && (fc.d_id ==
"ff.fa.01") || (fc.s_id == "ff.fa.04")' limit-captured-frames 2 write bootflash:fc_cap
Frame 2 (160 bytes on wire, 160 bytes captured)
    Arrival Time: May  6, 2010 09:53:38.020767000
    Time delta from previous packet: 0.000000000 seconds
    Time since reference or first frame: 0.000000000 seconds
    Frame Number: 2
    Packet Length: 160 bytes
    Capture Length: 160 bytes
Ethernet II, Src: 00:00:00:00:00:0a, Dst: 00:00:00:00:ee:00
    Destination: 00:00:00:00:ee:00 (00:00:00:00:ee:00)
    Source: 00:00:00:00:00:0a (00:00:00:00:00:0a)
    Type: Unknown (0xfcfc)
MDS Header(Unknown(0)/Unknown(0))
    MDS Header
        ...0 0000 1000 0010 = Packet Len: 130
        .... 0000 0000 00.. = Dst Index: 0x0000
        .... ..01 0010 0000 = Src Index: 0x0120
        .... 0000 0000 0001 = VSAN: 1
    MDS Trailer
        EOF: Unknown (0)
        CRC: 0xdeadbeef
Fibre Channel
    R_CTL: 0x20(Extended Link Services/0x0)
    Dest Addr: ff.fa.01
    CS_CTL: 0x00
    Src Addr: ff.fa.01
    Type: Ext Link Svc (0x01)
    F_CTL: 0x000000  Exchange Originator, Seq Initiator, CS_CTL, Last Data Frame
 - No Info, ABTS - Abort/MS,
        0... .... .... .... .... .... = ExgRpd: Exchange Originator
        .0.. .... .... .... .... .... = SeqRec: Seq Initiator
        ..0. .... .... .... .... .... = ExgFst: NOT exchg first
        ...0 .... .... .... .... .... = ExgLst: NOT exchg last
        .... 0... .... .... .... .... = SeqLst: NOT seq last
        .... ..0. .... .... .... .... = Pri: CS_CTL
        .... ...0 .... .... .... .... = TSI: NOT transfer seq initiative
        .... .... 00.. .... .... .... = LDF: Last Data Frame - No Info (0x000000
)
        .... .... ..00 .... .... .... = A01: no ack required (0x000000)
        .... .... .... ..0. .... .... = RetSeq: NOT retransmitted sequence
        .... .... .... .... ..00 .... = AA: ABTS - Cont (0x000000)
        .... .... .... .... .... 0... = RelOff: rel offset NOT set
    SEQ_ID: 0x00
    DF_CTL: 0x00
    SEQ_CNT: 0
    OX_ID: 0xffff
    RX_ID: 0xffff
    Parameter: 0x00000000
Data (106 bytes)
```

```
0000  01 00 00 00 00 00 04 1a 00 00 00 34 19 a0 be 60   ...........4...`
0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0020  00 ff fa 01 00 ff fa 01 00 00 09 96 00 00 00 00   ................
0030  00 00 00 04 00 00 00 02 00 00 00 00 01 00 00 00   ................
0040  ff ff ff ff 00 1c c0 00 c1 24 50 6e 4d aa 55 a6   .........$PnM.U.
0050  19 81 9c d3 6d b2 58 34 8a 30 6a e6 d6 cf 31 ff   ....m.X4.0j...1.
0060  ca cd 83 0e 00 00 de ad be ef                     ..........
switch#
```

The following example shows how to use capture filter on the mgmt interface and redirect the console output to a file:

```
switch# fcanalyzer local interface mgmt capture-filter "arp" > mgmt_capture.txt
Capturing on mgmt interface
switch#
```

Related Commands

Command	Description
show fcanalyzer	Displays the list of hosts configured for a remote capture.

fcanalyzer remote

To configure remote Cisco Fabric Analyzer, use the **fcanalyzer remote** command in configuration mode. To disable this command, use the **no** form of the command.

no fcanalyzer remote *ip address* [**active** *[port-number]*]

Syntax Description

ip-address	Maximum length is 1024 characters.
active	(Optional) Enables active mode (passive is the default) with the remote host.
port-number	(Optional) Specifies the port number.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can capture Fibre Channel control traffic from a switch and decode it without having to disrupt connectivity and without having to be local to the point of analysis.

Examples

The following example shows how to configure remote Cisco Fabric analyzer:

```
switch(config)# fcanalyzer remote 1.1.1.1
switch(config)#
```

Related Commands

Command	Description
clear fcanalyzer	Clears the entire list of configured hosts.
show fcanalyzer	Displays the list of hosts configured for a remote capture.

filter

To specify the fields of the certificate map, use the **filter** command in configuration mode. The CA certificate or certificate chain is assumed to already be available in Privacy Enhanced Mail (PEM) (base-64) encoded format.

filter {**altname-email** *email-id*|**altname-upn** *username*|**subject-name** *subject-name*}

Syntax Description

altname-email *email-id*	Specifies an Email ID as an alternate name. The maximum size is 64 characters.
altname-upn *username*	Specifies user principal name as an alternate name. The maximum size is 64 characters.
subject-name *subject-name*	Specifies subject name of the certificate. The maximum size is 64 characters

Command Default

None.

Command Modes

Configuration submode.

Command History

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

Usage Guidelines

%username% substitutes the user's login name.

%hostname% substitute the peer hostname.

Note Two maps currently can be configured for a given issuer name. The certificate will be filtered based on these two configured maps. If a default configuration is provided then the certificates are filtered against the default map in case if there is no map for that particular issuer name.

Examples

The following example shows how to configure an Email ID as an alternate name:

```
switch(config)# crypto certificatemap mapname map1
switch(config-certmap-filter)# filter subject-name cn=%username%,ou=PKI,o=Cisco Systems,c=US

switch(config-certmap-filter)#
```

The following example shows how to configure the user principal as an alternate name:

```
switch(config-certmap-filter)# filter altname-email %username%@cisco.com
switch(config-certmap-filter)#
```

The following example shows how to configure the subject name as an certificate:

```
switch(config-certmap-filter)# filter altname-upn%username%@%hostname%
switch(config-certmap-filter)#
```

Related Commands

Command	Description
show crypto ssh-auth-map	Displays mapping filters applied for SSH authentication.

fcc enable

To enable Fibre Channel Congestion Control (FCC), use the **fcc enable** command in configuration mode. To disable this feature, use the **no** form of the command.

fcc enable
no fcc enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was deprecated.
1.0(2)	This command was introduced.

Usage Guidelines

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 FCC:

```
switch# config terminal
switch(config)# fcc enable
```

The following example shows how to disable FCC:

```
switch# config terminal
switch(config)#  no fcc enable
```

Related Commands

Command	Description
show fcc	Displays FCC settings.

fc-management database

To configure the Fibre Channel Common Transport (FC-CT) Management Security database, use the **fc-management database** command.

fc-management database vsan *vsan-id*

Syntax Description

vsan	Specifies the VSAN.
vsan-id	Specifies the VSAN ID. The range is from 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 6.2(9)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the management security database:

```
switch(config)# fc-management database vsan 1
switch(config-fc-mgmt)#
```

Related Commands

Command	Description
fc-management enable	Enables the FC-CT Management Security.

fc-management enable

To enable the Fibre Channel Common Transport (FC-CT) Management Security, use the **fc-management enable** command. To disable this feature command, use the **no** form of the command.

fc-management enable
no fc-management enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 6.2(9)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable the FC-CT management security:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# fc-management enable
switch(config)#
```

Related Commands

Command	Description
show fc-management	Displays the FC-CT management security information.

fcc priority

To assign the FCC priority to the entire switch, use the **fcc priority** command in configuration mode. To revert to the default, use the **no** form of the command.

fcc priority *number*
no fcc priority *number*

Syntax Description

number	The FCC priority threshold. The range is 0 to 7, where 0 is the lowest priority and 7 the highest priority.

Command Default

The default priority is 4.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
5.0(1a)	This command was deprecated.

Usage Guidelines

FCC reduces the congestion in the traffic without interfering with the standard Fibre Channel protocol.

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 configure the FCC priority threshold as 2:

```
switch# config terminal
switch(config)# fcc priority 2
```

Related Commands

Command	Description
show fcc	Displays FCC settings.

fcdomain

To configure the Fibre Channel domain feature, use the **fcdomain** command. To disable the FC domain, use the **no** form of the command.

fcdomain {**allowed** *domain* **vsan** *vsan-id*|**auto-reconfigure vsan** *vsan-id*|**contiguous-allocation vsan** *vsan-id*|**domain** *id* {**preferred**|**static**} **vsan** *vsan-id*|**fabric-name name vsan** *vsan-id*|**fcid** {**database**|**persistent vsan** *vsan-id*}|**optimize all vsan** *vsan-id*|**optimize fast-restart vsan** *vsan-id*|**optimize scale-restart vsan** *vsan-id*|**optimize selective-restart vsan** *vsan-id*|**priority value vsan** *vsan-id*|**restart [disruptive] vsan** *vsan-id*|**vsan** *vsan-id*}
no fcdomain {**allowed** *domain* **vsan** *vsan-id*|**auto-reconfigure vsan** *vsan-id*|**contiguous-allocation vsan** *vsan-id*|**domain id** {**preferred**|**static**} **vsan** *vsan-id*|**fabric-name name vsan** *vsan-id*|**fcid persistent vsan** *vsan-id*|**optimize all vsan** *vsan-id*|**optimize fast-restart vsan** *vsan-id*|**optimize scale-restart vsan** *vsan-id*|**optimize selective-restart vsan** *vsan-id*|**priority value vsan** *vsan-id*|**vsan** *vsan-id*}

Syntax Description

allowed domain	Configures the allowed domain ID list ranging from 1 to 239.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
auto-reconfigure	Configures auto-reconfigure.
contiguous-allocation	Configures contiguous allocation.
domain *id*	Configures the domain ID and its type. The range is 0 to 239.
preferred	Configures the domain ID as preferred. By default, the local switch accepts the domain ID assigned by the principal switch and the assigned domain ID becomes the runtime domain ID.
static	Configures the domain ID as static. The assigned domain ID is discarded, all local interfaces are isolated, and the local switch assigns itself the configured domain ID, which becomes the runtime domain ID.
fabric-name *name*	Specifies the fabric name. The name format is *hh:hh:hh:hh:hh:hh:hh:hh*.
fcid	Configures FC domain persistent FC IDs.
database	Enters persistent FC IDs submode.
persistent	Enables or disables FC domain persistent FC IDs.
optimize all	Enables a domain manager all optimization on a specified VSAN.
optimize fast-restart	Enables a domain manager fast restart on a specified VSAN.
optimize scale-restart	Enables a domain manager scale restart on a specified VSAN.
optimize selective restart	Enables a domain manager selective restart on a specified VSAN.
priority *value*	Specifies the FC domain priority. The range is 1 to 254.

restart	Starts a disruptive or nondisruptive reconfiguration.
disruptive	Forces the disruptive fabric reconfiguration.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(9)	Added the **optimize all** and **scale-restart** keywords to the syntax description.
5.x	**disruptive** keyword is hidden from **fcdomain restart** command.
1.1(1)	This command was introduced.
2.0(1)	The **global-enable** keyword was deprecated.
3.0(2)	Added the **optimize fast-restart** option.

Usage Guidelines

You can use this command to select the principal switch, configure domain ID distribution, reconfigure the fabric, and allocate FC IDs.

We recommend using the **optimize fast-restart** option on most fabrics, especially those with a large number of logical ports (3200 or more), where a logical port is an instance of a physical port in a VSAN.

Examples

The following examples show how to configure the Fibre Channel domain feature:

```
switch# config terminal
switch(config)# fcdomain domain 3 preferred vsan 87
switch(config)# no fcdomain domain 3 preferred vsan 87
switch(config)# fcdomain domain 2 static vsan 237
switch(config)#  no fcdomain domain 2 static vsan 237
switch(config)# fcdomain restart vsan 1
switch(config)# fcdomain restart disruptive vsan 1
switch(config)# fcdomain optimize all vsan 3
switch(config)# fcdomain optimize all vsan 7 - 10
switch(config)# fcdomain optimize fast-restart vsan 3
switch(config)# fcdomain optimize fast-restart vsan 7 - 10
switch(config)# fcdomain optimize scale-restart vsan 3
switch(config)# fcdomain optimize scale-restart vsan 7 - 10
switch(config)# fcdomain optimize selective-restart vsan 3
switch(config)# fcdomain optimize selective-restart vsan 7 - 10
switch(config)# fcdomain priority 25 VSAN 99
switch(config)# no fcdomain priority 25 VSAN 99
switch(config)# fcdomain auto-reconfigure vsan 10
switch(config)# fcdomain contiguous-allocation vsan 81-83
switch(config)# no fcdomain contiguous-allocation vsan 1030
switch(config)# fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan 3
switch(config)# no fcdomain fabric-name 20:1:ac:16:5e:0:21:01 vsan 3010
switch(config)# fcdomain allowed 50-110 vsan 4
switch(config)# no fcdomain allowed 50-110 vsan 5
```

Related Commands

Command	Description
show fcdomain	Displays global information about the FC domain configurations.

fcdomain abort vsan

To flush cached data without committing and to release the lock, use the **fcdomain abort vsan**

fcdomain abort vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to commit cached data:

```
switch# config terminal
switch(config)# fcdomain abort vsan 10
```

Related Commands

Command	Description
fcdomain	Configures Fibre Channel domain features.
fcdomain commit vsan	Commits cached data and releases the lock.
show fcdomain	Displays global information about the FC domain configurations.

fcdomain commit vsan

To commit cached data and release the lock, use the **fcdomain commit vsan** command.

fcdomain commit vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Note After the FC domain commit is completed the running configuration has been modified on all switches participating in the FCd omain distribution. You can then use the copy running-config startup-config fabric command to save the running configuration to the startup configuration on all the switches in the fabric.

Examples

The following example shows how to commit cached data:

```
switch# config terminal
switch(config)# fcdomain commit vsan 10
```

Related Commands

Command	Description
fcdomain	Configures Fibre Channel domain features.
fcdomain abort vsan	Flushes cached data without committing and releases the lock.
show fcdomain	Displays global information about the FC domain configurations.

fcdomain distribute

To enable fabric distribution using Cisco Fabric Services (CFS), use the **fcdomain distribute** command. To disable fabric distribution using CFS, us the **no** form of the command.

fcdomain distribute
no fcdomain distribute

Syntax Description

This command has no arguments or keywords

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example enables fabric distribution using CFS:

```
switch# config terminal
switch(config)# fcdomain distribute
```

The following example disables fabric distribution using CFS:

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

Related Commands

Command	Description
fcdomain	Configures Fibre Channel domain features.
show fcdomain	Displays global information about the FC domain configurations.

fcdomain rcf-reject

To enable the RCF reject flag for a Fibre Channel or FCIP interface, use the **fcdomain** option. To disable this feature, use the **no** form of the command.

fcdomain rcf-reject vsan *number*
no fcdomain rcf-reject vsan *number*

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

Enabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1a)	This command was introduced.

Usage Guidelines

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

Use this option to configure the RCF reject option for the selected Fibre Channel or FCIP interface.

Examples

The following example shows how to configure the FCIP RCF reject fcdomain feature:

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# fcdomain rcf-reject vsan 1
```

Related Commands

Command	Description
show fcdomain	Displays global information about the FC domain configurations.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

fcdroplatency

To configure the network and switch FC drop latency time, use the **fcdroplatency** command in configuration mode. To disable the FC latency time, use the **no** form of the command.

fcdroplatency {**network** *milliseconds* [**vsan** *vsan-id*]|**switch** *milliseconds*}
no fcdroplatency {**network** *milliseconds* [**vsan** *vsan-id*]|**switch** *milliseconds*}

Syntax Description

network *milliseconds*	Specifies network latency. The range is 500 to 60000.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
switch *milliseconds*	Specifies switch latency. The range is 0 to 60000 milliseconds.

Command Default

2000 millisecond network latency.

500 millisecond switch latency.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
8.2(1)	The **switch** keyword was deprecated.

Usage Guidelines

None.

Examples

The following example shows how to configure the network latency to 5000 milliseconds:

```
switch# config terminal
switch(config)#
switch(config)# fcdroplatency network 5000
switch(config)#
```

The following example shows how to revert to the default network latency:

```
switch(config)# no fcdroplatency network 5000
switch(config)#
```

The following example shows how to configure the switch latency to 4000 milliseconds:

```
switch(config)# fcdroplatency switch 4000
switch(config)#
```

The following example shows how to revert to the default switch latency:

```
switch(config)# no fcdroplatency switch 4000
switch(config)#
```

Related Commands

Command	Description
show fcdroplatency	Displays the configured FC drop latency parameters.

fcflow stats

To configure FC flow statistics, use the **fcflow stats** command in configuration mode. To disable the counter, use the **no** form of the command.

fcflow stats {**aggregated module** *module-number* **index** *flow-number* **vsan** *vsan-id*|**module** *module-number* **index** *flow-number flow-numberdestination-fcid source-fcid netmask* **vsan** *vsan-id*} **no fcflow stats** {**aggregated module** *module-number* **index** *flow-number*|**module module-number index** *flow-number*}

Syntax Description

aggregated	Configures aggregated FC flow statistics.
module *module-number*	Configures FC flow statistics on a module.
index *flow-number*	Specifies a flow index. The range is 1 to 2147483647.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
destination-fcid	The destination FCID in hexadecimal format.
source-fcid	The source FCID in hexadecimal format.
netmask	The mask for the source and destination FCID (restricted to 6 hexadecimal characters ranging from 0xff0000 to 0xffffff).

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If you enable flow counters, you can enable a maximum of I K entries for aggregate flow and flow statistics. Be sure to assign an unused flow index to a module for each new flow. Flow indexes can be repeated across modules. The number space for flow index is shared between the aggregate flow statistics and the flow statistics.

Examples

The following example shows how to configure aggregated fcflow statistics for module 1:

```
switch-config# fcflow stats aggregated module 1
switch-config#
```

The following example enables the aggregated flow counter.

```
switch(config)# fcflow stats aggregated module 1 index 1005 vsan 1
```

The following example disables the aggregated flow counter.

```
switch(config)# no fcflow stats aggregated module 1 index 1005
```

The following example enables the flow counter for module 1:

```
switch(config)# fcflow stats module 1 index 1 0x145601 0x5601 0xffffff vsan 1
```

The following example disables the flow counter for module 1.

```
switch(config)# no fcflow stats module 2 index 1001
```

Related Commands

Command	Description
show fcflow stats	Displays the configured FC drop latency parameters.

fcid-allocation

Use the **fcid-allocation** command to manually add a FCID to the default area company ID list. Use the **no** form of the command to remove a FCID from the default area company ID list.

fcid-allocation area company-id *company-id*
no fcid-allocation area company-id *company-id*

Syntax Description

area	Modifies the auto area list of company IDs.
company-id *company-id*	Configures the company IDs.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0	This command was introduced.

Usage Guidelines

Fibre Channel standards require a unique FCID to be allocated to an N port attached to a Fx port in any switch. To conserve the number of FCIDs used, Cisco MDS 9000 Family switches use a special allocation scheme.

Some HBAs do not discover targets that have FCIDs with the same domain and area. Prior to Cisco MDS SAN-OS Release 2.0, the Cisco MDS SAN-OS software maintained a list of tested company ID (also know as Organizational Unit Identifier, or OUI) which do not exhibit this behavior. These Host Bus Adapters (HBAs) were allocated with single FCIDs, and for others a full area was allocated.

The FCID allocation scheme available in Release 1.3 and earlier, allocates a full area to these HBAs. This allocation isolates them to that area and are listed with their pWWN during a fabric login. The allocated FCIDs are cached persistently and are still available in Cisco MDS SAN-OS Release 2.0 (see the "FCID Allocation for HBAs" section on page 38-22).

As of Cisco MDS SAN-OS Release 2.0, to allow further scalability for switches with numerous ports, the Cisco MDS SAN-OS software is maintaining a list of HBAs exhibiting this behavior. Each HBA is identified by its company ID used in the pWWN during a fabric log in. A full area is allocated to the N ports with company IDs that are listed and for the others a single FCID is allocated. Irrespective of the kind (whole area or single) of FCID allocated, the FCID entries remain persistent.

Examples

The following example adds a new company ID to the default area company ID list:

```
switch# config terminal
switch(config)# fcid-allocation area company-id 0x003223
```

Related Commands

Command	Description
show fcid-allocation	Displays the configured company IDs.

fcid-last-byte

Use the **fcid-last-byte** command to allocate the last byte FCID for the fabric address. To disable the configuration or to revert to factory defaults, use the **no** form of the command.

fcid-last-byte *last-byte-id*
no fcid-last-byte *last-byte-id*

Syntax Description

last-byte-fcid	Specifies the last-byte FCID range from 0 to 250.

Command Default

None.

Command Modes

FICON configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	This command was deprecated.

Usage Guidelines

This is an optional configuration. If you are not sure of the EBCDIC format to be used, we recommend retaining the **us-canada** (default) option.

Examples

The following example assigns the last byte FCID for the fabric address:

```
switch# config terminal
switch(config)# ficon vsan 2
switch(config-ficon)# fcid-last-byte 12
```

The following example removes the configured last byte FCID for the fabric address and reverts to the default:

```
switch# config terminal
switch(config)# ficon vsan 2
switch(config-ficon)# no fcid-last-byte 3
```

Related Commands

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

fcinterop fcid-allocation

To allocate FCIDs on the switch, use the **fcinterop fcid-allocation** command in configuration mode. To disable FCIDs on the switch, use the **no** form of the command.

fcinterop fcid-allocation {**auto**|**flat**|**none**}
no fcinterop fcid-allocation {**auto**|**flat**|**none**}

Syntax Description

auto	Assigns single FCID to compatible HBAs.
flat	Assigns single FCID.
none	Assigns FCID range.

Command Default

The default is **fcinterop fcid-allocation auto.**

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command defines how the switch assigns FCIDs.

Examples

The following example shows how to allocate FCIDs on the switch:

```
switch# config terminal
switch(config)# fcinterop fcid-allocation none
switch(config)# fcinterop fcid-allocation flat
switch(config)# fcinterop fcid-allocation auto
```

Related Commands

Command	Description
show flogi database	Displays the fabric login (FLOGI) table.

fcinterop loop-monitor

To monitor removal of discs from a loop port, use the **fcinterop loop-monitor** command in configuration mode. To disable loop monitoring, use the **no** form of the command.

fcinterop loop-monitor
no fcinterop loop-monitor

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command detects devices that are removed from a looped port:

Examples

The following example shows how to enable monitoring of NL ports in a loop:

```
switch# config terminal
switch(config)# fcinterop loop-monitor
```

The following example shows how to disable monitoring of NL ports in a loop:

```
switch# config terminal
switch(config)# no fcinterop loop-monitor
```

Related Commands

Command	Description
show flogi database	Verifies if a storage device is displayed in the Fabric login (FLOGI) table.

fcip-enhanced

To enable write acceleration support on port channels of FCIP interfaces on a Cisco MDS 9250i switch, use the **fcip-enhanced** command. To remove write acceleration support on port channels of FCIP interfaces on a Cisco MDS 9250i switch, use the **no** form of this command.

fcip-enhanced
no fcip-enhanced

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
7.3(1)DY(1)	This command was introduced.

Usage Guidelines

- This command can be issued only on Cisco MDS 9250i Switches running on Cisco MDS NX-OS Release 7.3(1)DY(1) or later.
- This command can be issued only for port channels on FCIP interfaces.
- This command should be issued only between a Cisco MDS 9250i Switch and a Cisco MDS 24/10 port SAN Extension Module (on Cisco MDS 9700 Directors).
- The port channel mode must be set to **active** on both peers before issuing this command.
- This command must be issued before a member is added to a port channel. If an interface is already added as a member, remove the interface before issuing the command.

Example

The following example shows how to enable write acceleration support on port channels of FCIP interfaces on a Cisco MDS 9250i switch:

```
switch# configure terminal
switch(config)# interface port-channel 1
switch(config-if)# channel mode active
switch(config-if)# fcip-enhanced
FCIP enhanced will be enabled. Please ensure the peer link is connected to m97xx
switch(config-if)# end
```

Related Commands

Command	Description
interface port-channel *number*	Configures the specified port channel using the default **on** mode.
show port-channel database	Displays the port channel configured in the default **on** mode and **active** mode.

fcip enable

To enable the FCIP feature in any switch in the Cisco MDS 9000 Family, use the **fcip enable** command.

fcip enable
no fcip enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
NX-OS 4.1(1b)	This command was deprecated.

Usage Guidelines

The configuration and verification commands for the iSCSI feature are only available when FCIP is enabled on a switch. When you disable this feature, all related configurations are automatically discarded.

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 command enables the FCIP feature:

```
switch(config)# fcip enable
```

The following command disables the FCIP feature (default):

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

Related Commands

Command	Description
show fcip	Displays FCIP information.

fcip profile

To create and configure an FCIP profile, use the **fcip profile** command. To remove an FCIP profile, use the **no** form of the command.

fcip profile *profile-id*
no fcip profile *profile-id*

Syntax Description

profile-id	Specifies a ID range from 1 to 255.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

When you perform this command, the CLI enters FCIP profile configuration mode.

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 configure an FCIP profile:

```
switch## config terminal
switch(config)# fcip profile 5
switch(config-profile)#
```

Related Commands

Command	Description
interface fcip interface_number use-profile profile-id	Configures the interface using an existing profile ID from 1 to 255.
show fcip profile	Displays information about the FCIP profile.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

fcns bulk-notify

To enable transmission of multiple name server entry change notifications in one Messaging and Transaction Services (MTS) payload, use the **fcns bulk-notify** command. To disable bulk notify, use the **no** form of this command.

fcns bulk-notify
no fcns bulk-notify

Syntax Description

This command has no keywords or arguments.

Command Default

Bulk notification from the name server is disabled by default. For 6.2(9) and later releases, bulk notification from the name server is enabled by default.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(7)	This command was introduced.
6.2(9)	This command was deprecated.

Usage Guidelines

Enabling the **fcns bulk-notify** command would improve the performance of the components like Zone, IVR, QOS, IPS.

Note Run the **show fcns internal info global** command to determine if the bulk notification is enabled.

Examples

The following example shows how to enable transmission of multiple name server entry change notifications in one MTS payload:

```
switch# config terminal
switch(config)# fcns bulk-notify
switch(config)#
```

Related Commands

Command	Description
show fcns internal info global	Displays the FCNS global configuration.

fcns no-bulk-notify

To disable transmission of multiple name server entry change notifications in one MTS payload, use the **fcns no-bulk-notify** command. To re-enable bulk notification once it is disabled, use the **no** form of this command.

fcns no-bulk-notify
no fcns no-bulk-notify

Syntax Description

This command has no keywords or arguments.

Command Default

Bulk notification from the name server is disabled by default. For 6.2(9) and later releases, bulk notification from the name server is enabled by default.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(9)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to disable transmission of multiple name server entry change notifications in one MTS payload:

```
switch# config terminal
switch(config)# fcns no-bulk-notify
switch(config)#
```

The following example shows how to re-enable bulk notification once it has been disabled:

```
switch# config terminal
switch(config)# no fcns no-bulk-notify
switch(config)#
```

Related Commands

Command	Description
fcns bulk-notify	Available until Release 6.2(7) only. Enables transmission of multiple name server entry change notifications in one MTS payload.

fcns proxy-port

To register a name server proxy, use the **fcns proxy-port** command in configuration mode.

fcns proxy-port *wwn-id* **vsan** *vsan-id*
no fcns proxy-port *wwn-id* **vsan** *vsan-id*

Syntax Description

wwn-id	Specifies the port WWN, with the format hh:hh:hh:hh:hh:hh:hh:hh.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

One name server can be configured to proxy another name server and name server information can be displayed using the CLI. The name server can be viewed using the CLI or Cisco Fabric Manager.

All name server registration requests come from the same port whose parameter is registered or changed. If it does not, then the request is rejected.

Examples

The following example shows configuring a proxy port for VSAN 2:

```
switch# config terminal
switch(config)# fcns proxy-port 21:00:00:e0:8b:00:26:d vsan 2
```

Related Commands

Command	Description
show fcns	Displays the name server database and statistical information for a specified VSAN or for all VSANs.

fcns reject-duplicate-pwwn vsan

To reject the same pwwn from logging in the different switch, use the **fcns reject-duplicate-pwwn vsan** command in configuration mode.

fcns reject-duplicate-pwwn vsan *vsan-id*
no fcns reject-duplicate-pwwn vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example rejects duplicate FCNS pWWNs for VSAN 2:

```
switch# configure terminal
switch(config)# fcns reject-duplicate-pwwn vsan 2
```

Related Commands

Command	Description
show fcns	Displays the name server database and statistical information for a specified VSAN or for all VSANs.

fcping

To ping an N port with a specified FCID, use the **fcping fcid** command in EXEC mode.

fcping {**device-alias** *aliasname*|**fcid** {*fc-portdomain-controller-id*}|**pwwn** *pwwn-id*} **vsan** *vsan-id* [**count** *number* [**timeout** *value* [**usr-priority** *priority*]]]

Syntax Description

device-alias *aliasname*	Specifies the device alias name. Maximum length is 64 characters.
fcid	The FCID of the destination N port.
fc-port	The port FCID with the format 0xhhhhhh.
domain-controller-id	Verifies connection to the destination switch.
pwwn *pwwn-id*	Specifies the port WWN of the destination N port, with the format hh:hh:hh:hh:hh:hh:hh:hh.
vsan *vsan-id*	Specifies the VSAN ID of the destination N port. The range is 1 to 4093.
count *number*	(Optional) Specifies the number of frames to send. A value of 0 sends forever. The range is 0 to 2147483647.
timeout *value*	(Optional) Specifies the timeout value in seconds. The range is 1 to 10.
usr-priority *priority*	(Optional) Specifies the priority the frame receives in the switch fabric. The range is 0 to 1.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
1.2(1)	Allowed the domain controller ID as an FCID.
2.0(x)	Added the **device-alias** *aliasname* option.

Usage Guidelines

To obtain the domain controller address, concatenate the domain ID with **FFFC**. For example, if the domain ID is **0xda**(218), the concatenated ID is **0xfffcda**.

Examples

The following example shows a fcping operation for the specified pWWN or the FCID of the destination. By default, five frames are sent.

```
switch# fcping fcid 0xd70000 vsan 1
28 bytes from  0xd70000  time = 730 usec
28 bytes from  0xd70000  time = 165 usec
```

```
28 bytes from  0xd70000  time = 262 usec
28 bytes from  0xd70000  time = 219 usec
28 bytes from  0xd70000  time = 228 usec
5 frames sent, 5 frames received, 0 timeouts
Round-trip min/avg/max = 165/270/730 usec
```

The following example shows the setting of the number of frames to be sent using the count option. The range is from 0 through 2147483647. A value of 0 will ping forever.

```
switch# fcping fcid 0xd70000 vsan 1 count 10
28 bytes from  0xd70000  time = 730 usec
28 bytes from  0xd70000  time = 165 usec
28 bytes from  0xd70000  time = 262 usec
28 bytes from  0xd70000  time = 219 usec
28 bytes from  0xd70000  time = 228 usec
28 bytes from  0xd70000  time = 230 usec
28 bytes from  0xd70000  time = 230 usec
28 bytes from  0xd70000  time = 225 usec
28 bytes from  0xd70000  time = 229 usec
28 bytes from  0xd70000  time = 183 usec
10 frames sent, 10 frames received, 0 timeouts
Round-trip min/avg/max = 165/270/730 usec
```

The following example shows the setting of the timeout value. The default period to wait is 5 seconds. The range is from 1 through 10 seconds.

```
switch# fcping fcid 0xd500b4 vsan 1 timeout 10
28 bytes from  0xd500b4  time = 1345 usec
28 bytes from  0xd500b4  time = 417 usec
28 bytes from  0xd500b4  time = 340 usec
28 bytes from  0xd500b4  time = 451 usec
28 bytes from  0xd500b4  time = 356 usec
5 frames sent, 5 frames received, 0 timeouts
Round-trip min/avg/max = 340/581/1345 usec
```

This command shows the No response from the N port message even when the N port or NL port is active. This is due to resource exhaustion at the N port or NL port. Retry the command a few seconds later.

```
switch# fcping fcid 0x010203 vsan 1
No response from the N port.
switch# fcping pwwn 21:00:00:20:37:6f:db:dd vsan 1
28 bytes from 21:00:00:20:37:6f:db:dd time = 1454 usec
28 bytes from 21:00:00:20:37:6f:db:dd time = 471 usec
28 bytes from 21:00:00:20:37:6f:db:dd time = 372 usec
28 bytes from 21:00:00:20:37:6f:db:dd time = 364 usec
28 bytes from 21:00:00:20:37:6f:db:dd time = 1261 usec
5 frames sent, 5 frames received, 0 timeouts
Round-trip min/avg/max = 364/784/1454 usec
```

The following example displays fcping operation for the device alias of the specified destination:

```
switch# fcping device-alias x vsan 1
28 bytes from 21:01:00:e0:8b:2e:80:93 time = 358 usec
28 bytes from 21:01:00:e0:8b:2e:80:93 time = 226 usec
28 bytes from 21:01:00:e0:8b:2e:80:93 time = 372 usec
```

fc-redirect version2 enable

To enable FC redirect version2 mode, use the **fc-redirect version2 enable** command in configuration mode. To disable this feature, use the **no** form of the command.

fc-redirect version2 enable
no fc-redirect version2 enable

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

AAM mode can be enabled in version1 mode also.

Examples

The following example shows how to enable FC redirect version2 mode:

```
switch# config terminal
switch(config)# fc-redirect version2 enable

Please make sure to read and understand the following implications
before proceeding further:

   1) This is a Fabric wide configuration. All the switches in the
      fabric will be configured in Version2 mode.Any new switches
      added to the fabric will automatically be configured in version2
      mode.

   2) SanOS 3.2.x switches CANNOT be added to the Fabric after Version2
      mode is enabled. If any 3.2.x switch is added when Version2 mode
      is enabled, all further FC-Redirect Configuration changes will Fail
      across the fabric. This could lead to traffic disruption for
      applications like SME.

   3) If enabled, Version2 mode CANNOT be disabled till all FC-Redirect
      configurations are deleted. FC-Redirect configurations can be
      deleted ONLY after all the relevant application configurations
      are deleted. Please use the command 'show fc-redirect configs'
      to see the list of applications that created FC-Redirect
      configurations.

   4) 'write erase' will NOT disable this command. After 'write erase'
      on ANY switch in the fabric, the user needs to do:
               'clear fc-redirect decommission-switch'
      on that that switch. Without that, if the user moves the switch
      to a different fabric it will try to convert all the switches
      in the fabric to Version2 mode automatically. This might lead
      to Error conditions and hence Traffic disruption.
```

```
Do you want to continue? (Yes/No) [No]
isola-77(config)#
```

The following example shows how to disable FC redirect version2 mode:

```
switch# config terminal
switch(config)# no fc-redirect version2 enable
WARNING: This command will disable Version2 mode throughout the fabric.
         This is NOT a recommended step.
Do you want to continue? (Yes/No) [No]
switch(config)#
```

Related Commands

Command	Description
show fc-redirect-active configs	Displays all active configurations on a switch.

fc-redirect ivr-support enable

To enable FC redirect IVR support, use the **fc-redirect ivr-support enable** command in configuration mode. To disable this feature, use the **no** form of the command.

fc-redirect ivr-support enable
no fc-redirect ivr-support enable

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to enable FC redirect IVR support:

```
switch# config terminal
switch(config)# fc-redirect ivr-support enable
switch(config)#
```

The following example shows how to disable FC redirect IVR support:

```
switch# config terminal
switch(config)# no fc-redirect ivr-support enable
switch(config)#
```

Related Commands

Command	Description
show fc-redirect-active configs	Displays all active configurations on a switch.

fcroute

To configure Fibre Channel routes and to activate policy routing, use the **fcroute** command. To remove a configuration or revert to factory defaults, use the **no** form of the command.

fcroute {*fcid network-mask* **interface** {**fc** *slot/port*|**port-channel** *port*} **domain** *domain-id* {**metric** *number*|**remote**|**vsan** *vsan-id*}|*policy fcroute-map* **vsan** *vsan-id* [*route-map-identifier*]}
no fcroute {*fcid network-mask* **interface** {**fc** *slot/port*|**port-channel** *port*} **domain** *domain-id* {**metric** *number*|**remote**|**vsan** *vsan-id*}|*policy fcroute-map* **vsan** *vsan-id* [*route-map-identifier*]}

Syntax Description

fcid	Specifies the FC ID. The format is **0x***hhhhhh*.
network-mask	Specifies the network mask of the FC ID. The format is **0x***0* to **0x***ffffff*.
interface	Specifies an interface.
fc *slot*/*port*	Specifies a Fibre Channel interface.
port-channel *port*	Specifies a PortChannel interface.
domain *domain-id*	Specifies the route for the domain of the next hop switch. The range is 1 to 239.
metric *number*	Specifies the cost of the route. The range is 1 to 65535. Default cost is 10.
remote	Configures the static route for a destination switch remotely connected.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
policy fcroute-map	Activates policy routing.
route-map-identifier	(Optional) Specifies the route map identifier. The range is 1 to 65535.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(9)	This command was deprecated.
1.0(2)	This command was introduced.
3.0(3)	Added the **policy** option.

Usage Guidelines

Use this command to assign forwarding information to the switch and to activate a preferred path route map.

Examples

The following example specifies the Fibre Channel interface and the route for the domain of the next hop switch for VSAN 2:

```
switch# config terminal
switch(config)# fcroute 0x111211 interface fc1/1 domain 3 vsan 2
```

The following example removes this configuration:

```
switch(config)# no fcroute 0x111211 interface fc1/1 domain 3 vsan 2
```

The following example specifies the PortChannel interface and the route for the domain of the next hop switch for VSAN 4:

```
switch# config terminal
switch(config)# fcroute 0x111211 interface port-channel 1 domain 3 vsan 4
```

The following example removes this configuration:

```
switch(config)# no fcroute 0x111211 interface port-channel 1 domain 3 vsan 4
```

The following example specifies the Fibre Channel interface, the route for the domain of the next hop switch, and the cost of the route for VSAN 1:

```
switch# config terminal
switch(config)# fcroute 0x031211 interface fc1/1 domain 3 metric 1 vsan 1
```

The following example removes this configuration:

```
switch(config)# no fcroute 0x031211 interface fc1/1 domain 3 metric 1 vsan 1
```

The following example specifies the Fibre Channel interface, the route for the domain of the next hop switch, the cost of the route, and configures the static route for a destination switch remotely connected for VSAN 3:

```
switch# config terminal
switch(config)# fcroute 0x111112 interface fc1/1 domain 3 metric 3 remote vsan 3
```

The following example removes this configuration:

```
switch(config)# no fcroute 0x111112 interface fc1/1 domain 3 metric 3 remote vsan 3
```

Related Commands

Command	Description
fcroute-map	Specifies a preferred path Fibre Channel route map.
fcroute policy fcroute-map	Activates the preferred path Fibre Channel route map.
show fcroute	Displays Fibre Channel routes.
show fcroute-map	Displays the preferred path route map configuration and status.

fcroute-map vsan

To configure a preferred path Fibre Channel route map, use the **fcroute-map vsan** command. To remove a configuration, use the **no** form of the command.

fcroute-map vsan *vsan-id route-map-identifier*
no fcroute-map vsan *vsan-id route-map-identifier*

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
route-map-identifier	Specifies the route map identifier. The range is 1 to 65535.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(3)	This command was introduced.

Usage Guidelines

As of Cisco MDS SAN-OS Release 3.0(3) and later, you can use preferred path routes for Fibre Channel to route traffic over selected paths that are not necessarily the shortest path as chosen by routing protocols such as FSPF. This kind of control allows you to choose paths based on characteristics such as frames received on a selected interface or frames with a selected source FC ID. This ensures path separation between a host and a target.

Examples

The following example specifies a Fibre Channel route map and places you in the Fibre Channel route map configuration submode.

```
switch# config terminal
switch(config)# fcroute-map vsan 2 12
switch(config-fcroute-map)#
```

The following example removes the Fibre Channel route map.

```
switch(config)# no fcroute-map vsan 2 12
```

Related Commands

Command	Description
fcroute	Specifies Fibre Channel routes and activates policy routing.
show fcroute-map	Displays the preferred path route map configuration and status.
match (fcroute-map configuration submode)	Specifies the source and destination FC ID match criteria.

Command	Description
set (fcroute-map configuration submode)	Specifies the interface, the preference level for this interface, and the IVR next hop VSAN ID for this interface.

fcrxbbcredit extended enable

To enable Fibre Channel extended buffer-to-buffer credits (BB_credits), use the **fcrxbbcredit extended enable** command **in configuration mode.** To disable the feature, use the **no** form of the command.

fcrxbbcredit extended enable
no fcrxbbcredit extended enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

Use the **fcrxbbcredit extended enable** command to enable the **switchport fcrxbbcredit extended** command.

The **fcrxbbcredit extended enable** command is not supported on the following switches:

- Cisco MDS 9124 Multilayer Fabric Switch
- Cisco Fabric Switch for HP c-Class BladeSystem
- Cisco Fabric Switch for IBM BladeCenter
- Cisco MDS 9134 Multilayer Fabric Switch
- Cisco MDS 9148 Multilayer Fabric Switch
- Cisco MDS 9148S 16G Multilayer Fabric Switch
- Cisco MDS 9250i Multiservice Fabric Switch

The following example shows how to enable Fibre Channel extended BB_credits:

```
switch# config terminal
switch(config)# fcrxbbcredit extended enable
```

The following example shows how to disable Fibre Channel extended BB_credits:

```
switch# config terminal
switch(config)# no fcrxbbcredit extended enable
```

Related Commands

Command	Description
show interface	Displays interface information and status.
switchport fcrxbbcredit extended	Configures Fibre Channel extended BB_credits on an interface.

fcs plat-check-global vsan

To enable FCS platform and node name checking fabric-wide, use the **fcs plat-check-global vsan** command in configuration mode. To disable this feature, use the **no** form of the command.

fcs plat-check-global vsan *vsan-id*
no fcs plat-check-global vsan *vsan-id*

Syntax Description

vsan-id	Specifies the VSAN ID for platform checking, which is from 1 to 4096.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

```
switch# config terminal
switch(config)# fcs plat-check-global vsan 2
```

Related Commands

Command	Description
show fcs	Displays fabric configuration server information.

fcs register

To register FCS attributes, use the **fcs register** command in configuration mode. To disable this feature, use the **no** form of the command.

fcs register platform name *name* **vsan** *vsan-id*
no fcs register platform name *name* **vsan** *vsan-id*

Syntax Description

platform name *name*	Specifies the name of the platform to register. Maximum size is 255 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4096.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to register FCS attributes:

```
switch# config terminal
switch(config)# fcs register
switch(config-fcs-register)# platform Platform1 vsan 10
```

Related Commands

Command	Description
show fcs	Displays fabric configuration server information.

fcs virtual-device-add

To include a virtual device in a query about zone information from an FCS, use the **fcs virtual-device-add** command in configuration mode. To remove a virtual device, use the **no** form of the command.

fcs virtual-device-add [**vsan-ranges** *vsan-ids*]
no fcs virtual-device-add [**vsan-ranges** *vsan-ids*]

Syntax Description

vsan-ranges *vsan-ids*	(Optional) Specifies one or multiple ranges of VSANs. The range is 1 to 4093.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.1(2)	This command was introduced.

Usage Guidelines

VSAN ranges are entered as *vsan-ids*-*vsan-ids*. When you specify more than one range, separate each range with a comma. If no range is specified, the command applies to all VSANs.

Examples

The following example shows how to add to one range of VSANs:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# fcs virtual-device-add vsan-ranges 2-4
```

The following example shows how to add to more than one range of VSANs:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# fcs virtual-device-add vsan-ranges 2-4,5-8
```

Related Commands

Command	Description
show fcs	Displays fabric configuration server information.

fcsp

To configure a Fibre Channel Security Protocol (FC-SP) authentication mode for a specific interface in an FC-SP-enabled switch, use the **fcsp** command. To disable an FC-SP on the interface, use the **no** form of the command.

fcsp {**auto-active**|**auto-passive**|**esp manual**|**off**|**on**} [*timeout-period*]
no fcsp {**auto-active**|**auto-passive**|**esp manual**|**off**|**on**} [*timeout-period*]

Syntax Description

auto-active	Configures the auto-active mode to authenticate the specified interface.
auto-passive	Configures the auto-passive mode to authenticate the specified interface.
esp	Configures the Encapsulating Security Payroll for an interface.
manual	Configures the Encapsulating Security Payroll in manual mode.
on	Configures the auto-active mode to authenticate the specified interface.
off	Configures the auto-active mode to authenticate the specified interface.
timeout-period	(Optional) Specifies the timeout period to reauthenticate the interface. The time ranges from 0 (the default where no authentication is performed) to 100,000 minutes.

Command Default

Auto-passive.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(1)	Fibre Channel Security Protocol (FC-SP) is currently not supported on MDS 9710, but targeted for a future release.
NX-OS 4.2(1)	Added esp keyword for the syntax description.
1.3(1)	This command was introduced.

Usage Guidelines

To use this command, FC-SP must be enabled using the **feature fcsp** command.

Examples

The following example shows how to configure the ESP in manual mode:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface fc 2/1 - 3
switch(config-if)# fcsp esp manual
switch(config-if-esp)#
```

The following example turns on the authentication mode for ports 1 to 3 in Fibre Channel interface 2:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface fc 2/1 - 3
switch(config-if)# fcsp on
switch(config-if)#
```

The following example reverts to the factory default of auto-passive for these Fibre Channel interfaces:

```
switch(config-if)# no fcsp
```

The following example changes these Fibre Channel interfaces to initiate FC-SP authentication, but does not permit reauthentication:

```
switch(config-if)# fcsp auto-active 0
```

The following example changes these Fibre Channel interfaces to initiate FC-SP authentication and permits reauthentication within two hours (120 minutes) of the initial authentication attempt:

```
switch(config-if)# fcsp auto-active 120
```

Related Commands

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

fcsp dhchap devicename

Asymmetric DHCHAP secrets may be used on FC-SP links. To populate the FC-SP DHCHAP secret database on the local switch with the secrets used by remote switches use the **fcsp dhchap devicename** command. To remove these entries use the **no** form of the command.

fcsp dhchap devicename *remote-switch-wwn* **password** [{**0**|**7**}] *remote-secret*
no fcsp dhchap devicename *remote-switch-wwn* **password** [{**0**|**7**}] *remote-secret*

Syntax Description

remote-switch-wwn	Switch World Wide Name (WWN) of the remote device. The WWN format is *hh:hh:hh:hh:hh:hh:hh:hh*.
password	Configures the DHCHAP secret for the remote device.
0	(Optional) Specifies that the secret is in cleartext.
7	(Optional) Specifies that the secret is in encrypted text. This is the default value.
remote-secret	DHCHAP secret. Maximum of 64 alphanumeric characters.

Command Default

The default entry format for the secret is encrypted.

Command Modes

Global configuration (config)

Command History

Release	Modification
1.3 (1)	This command was introduced.

Usage Guidelines

The **fcsp dhchap devicename** command is available only when the FC-SP feature is enabled.

Example

The following example shows how to configure an encrypted secret of a remote switch:

```
switch(config)# fcsp dhchap devicename 00:11:22:33:44:aa:bb:cc password mypassword
```

The following example shows how to remove the remote switch secret of the previous example from the local switch DHCHAP secret database:

```
switch(config)# no fcsp dhchap devicename 00:11:22:33:44:aa:bb:cc password mypassword
```

The following example shows an asymmetric secret configuration for a link between the local switch and a remote switch with switch WWN of *01:01:01:01:01:01:01:01*. The secret on the local switch is 'local_secret' and the remote switch has a secret of 'far_secret'. The configuration is for the local switch and the secrets:

```
switch(config)# fcsp dhchap password 0 local_secret 01:01:01:01:01:01:01:01
switch(config)# fcsp dhchap devicename 01:01:01:01:01:01:01:01 password 0 far_secret
```

Related Commands

Command	Description
fcsp enable	Enables FC-SP.
fcsp dhchap dhgroup	Configure FC-SP group priority list.
fcsp dhchap hash	Configure FC-SP hash priority list.
fcsp dhchap password	Configure FC-SP link secrets.
show fcsp	Displays configured FC-SP information.

fcsp dhchap dhgroup

To change the FC-SP DHCHAP group priority list, use the **fcsp dhchap dhgroup** command in global configuration mode. To revert to the default group priority list, use the **no** form of this command. .

fcsp dhchap dhgroup *group-id* [*group-id* [*group-id* [*group-id* [*group-id*]]]]
no fcsp dhchap dhgroup *group-id* [*group-id* [*group-id* [*group-id* [*group-id*]]]]

Syntax Description

group-id	**0**|**1**|**2**|**3**|**4** Specifies an FC-SP DHCHAP group priority list entry.

Command Default

The default DH group priority list, from highest to lowest is **0 4 1 2 3**.

Command Modes

Global configuration (config)

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The **fcsp dhchap dhgroup** command is available only when the FC-SP feature is enabled.

There must be at least one member in the DH group priority list. Each group may only be specified once.

If you change the default FC-SP DH group priority list, ensure that you change it globally for all the switches in the fabric.

The following table maps the Cisco Group Number with the corresponding RFC Group Number and Modular Exponentiation (MODP) Group:

Table 1: Cisco Group Number with Corresponding RFC Group Number and MODP Group

Cisco Group Number	RFC Group Number	MODP Group
0	null	null DH algorithm
1	2	1024
2	—	1280
3	5	1536
4	14	2048

Example

The following example shows how to configure the used DH group list to only groups 2, 3, and 4, in the same order of priority:

```
switch(config)# fcsp dhchap dhgroup 2 3 4
```

The following example shows how to revert a previously configured DH group priority list of the 'null' group only back to the default priority list:

```
switch(config)# no fcsp dhchap dhgroup 0
```

Related Commands

Command	Description
fcsp enable	Enables FC-SP.
fcsp dhchap devicename	Configure FC-SP asymmetric secrets.
fcsp dhchap hash	Configure FC-SP hash priority list.
fcsp dhchap password	Configure FC-SP link secrets.
show fcsp	Displays configured FC-SP information.

fcsp dhchap hash

To configure the hash algorithm priority list for FC-SP DHCHAP authentication use the **fcsp dhchap hash** command. To return to the default hash algorithm priority list use the **no** form of the command.

fcsp dhchap hash {**md5 [sha1]** | **sha1 [md5]**}
no fcsp dhchap hash {**md5 [sha1]** | **sha1 [md5]**}

Syntax Description

md5	(Optional) Specifies the MD5 hash algorithm.
sha1	(Optional) Specifies the SHA-1 hash algorithm.

Command Default

The default FC-SP DHCHAP hash algorithm priority list has the following order:

- MD5
- SHA-1

Command Modes

Global configuration (config)

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The **fcsp dhchap hash** command is available only when the FC-SP feature is enabled.

If you change the default hash algorithm list order, then change it in all switches in the fabric.

Warning If FC-SP DHCHAP authentication via AAA is enabled, the MD5 hash algorithm must be set if the AAA authentication uses RADIUS or TACACS+. This is because RADIUS and TACACS+ applications do not support other hash algorithms.

Example

The following example shows how to configure the DHCHAP authentication hash priority list to be SHA-1 followed by MD5:

```
switch(config)# fcsp dhchap hash sha1 md5
```

The following example shows how to configure the use of the SHA-1 hash algorithm only:

```
switch(config)# fcsp dhchap hash sha1
```

The following example shows how to revert the previous example to the default priority list:

```
switch(config)# no fcsp dhchap hash sha1
```

Related Commands

Command	Description
fcsp enable	Enables FC-SP.
fcsp dhchap devicename	Configure FC-SP asymmetric secrets.
fcsp dhchap dhgroup	Configure FC-SP group priority list.
fcsp dhchap password	Configure FC-SP link secrets.
show fcsp	Displays configured FC-SP information.

fcsp dhchap password

To configure the FC-SP DHCHAP secret database used for FC-SP peer switch link authentication via DHCHAP use the **fcsp dhchap password** command. To remove secrets from the FC-SP DHCHAP database use the **no** form of the command.

fcsp dhchap password [{**0** |**7**}] *secret* [*remote-switch-wwn*]
no fcsp dhchap password [{**0** |**7**}] *secret* [*remote-switch-wwn*]

Syntax Description

secret	DHCHAP secret. Maximum of 64 alphanumeric characters.
remote-switch-wwn	(Optional) Switch World Wide Name of the remote switch to use this secret with. The WWN format is *hh:hh:hh:hh:hh:hh:hh:hh*.

Command Default

The default entry format for the secret is encrypted.

Command Modes

Global configuration (config)

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The **fcsp dhchap password** command is available only when the FC-SP feature is enabled.

Be sure to configure an FC-SP DHCHAP database on each switch in the fabric when this facility is being used.

To configure a fabric-wide global FC-SP DHCHAP secret use the command without any switch WWN specifier. There can be only a single global FC-SP DHCHAP secret in a fabric. Additionally, switch specific secrets may be configured. To configure these specify the switch WWN.

Example

The following example show how to configure the global FC-SP DHCHAP secret in cleartext:

```
switch(config)# fcsp dhchap password 0 mypassword
```

The following example show how to configure a secret to be used with the specified peer switch in cleartext:

```
switch(config)# fcsp dhchap password 0 mypassword 30:11:bb:cc:dd:33:11:22
```

The following example show how to remove a secret to be used with the specified peer switch by entering the secret in cleartext, even though the configuration is stored in the configuration in encrypted form:

```
switch(config)# no fcsp dhchap password 0 mypassword 30:11:bb:cc:dd:33:11:22
```

The following example shows how to configure symmetric secrets on a link between switch1 with sWWN of *01:01:01:01:01:01:01:01* and switch2 with sWWN of *02:02:02:02:02:02:02:02*. The FC-SP DHCHAP secret is in cleartext format:

```
switch1(config)# fcsp dhchap password 0 very_secret 02:02:02:02:02:02:02:02
switch2(config)# fcsp dhchap password 0 very_secret 01:01:01:01:01:01:01:01
```

Related Commands

Command	Description
fcsp enable	Enables FC-SP.
fcsp dhchap devicename	Configure asymmetric secrets.
fcsp dhchap dhgroup	Configure FC-SP group priority list.
fcsp dhchap hash	Configure FC-SP hash priority list.
show fcsp	Displays configured FC-SP information.

fcsp enable

To enable the Fibre Channel Security Protocol (FC-SP) in a switch, use the **fcsp enable** command in configuration mode. Additional FC-SP commands are available when the FC-SP feature is enabled. To disable FC-SP, use the **no** form of the command.

fcsp enable
no fcsp enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
NX-OS 4.1(1b)	This command was deprecated.

Usage Guidelines

None.

Examples

The following example enables FC-SP:

```
switch# config terminal
switch(config)# fcsp enable
switch(config)#
```

Related Commands

Command	Description
show fcsp	Displays configured FC-SP information.

fcsp esp sa

To configure the parameters for the Security Association (SA), use the **fcsp esp sa** command. To delete the SA between the switches, use the **no** form of the command.

fcsp esp sa *spi-number*
no fcsp esp sa *spi-number*

Syntax Description

spi-number	Configures the Security Protocol Interface (SPI) of the Security Association. The range is from 256 to 4294967295.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.2(1)	The spi-number range has been reduced from 256 4294967295 to 256 65536.
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the command for ESP:

```
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)#
```

Related Commands

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

fcsp timeout

To configure the timeout value for FC-SP message, use the **fcsp timeout** command in configuration mode. Use the **no** form of the command to revert to factory defaults.

fcsp timeout *timeout-period*
no fcsp timeout *timeout-period*

Syntax Description

timeout-period	Specifies the timeout period. The time ranges from 20 to 100 seconds. The default is 30 seconds.

Command Default

30 seconds.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

You can only see the **fcsp timeout** command if you enter the **fcsp enable** command.

Examples

The following example configures the FCSP timeout value:

```
switch# config terminal
switch(config)# fcsp enable
switch(config)# fcsp timeout 60
```

Related Commands

Command	Description
fcsp enable	Enables FC-SP.
show fcsp	Displays configured FC-SP information.

fctimer

To change the default Fibre Channel timers, use the **fctimer** command in configuration mode. To revert to the default values, use the **no** form of the command.

fctimer {**d_s_tov** *milliseconds* [**vsan** *vsan-id*]|**e_d_tov** *milliseconds* [**vsan** *vsan-id*]|**r_a_tov** *milliseconds* [**vsan** *vsan-id*]}
no fctimer {**d_s_tov** *milliseconds* [**vsan** *vsan-id*]|**e_d_tov** *milliseconds* [**vsan** *vsan-id*]|**r_a_tov** *milliseconds* [**vsan** *vsan-id*]}

Syntax Description

d_s_tov *milliseconds*	Specifies the distributed services time out value. The range is 5000 to 10,000 milliseconds, with a default of 5000.
vsan *vsan-id*	(Optional) Specifies the VSAN ID. The range is 1 to 4096.
e_d_tov *milliseconds*	Specifies the error detect time out value. The range is 1000 to 4,000 milliseconds, with a default of 2000.
r_a_tov *milliseconds*	Specifies the resolution allocation time out value. The range is 5000 to 10,000 milliseconds, with a default of 10,000.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The Cisco MDS 9000, Brocade, and McData FC Error Detect (ED_TOV) and Resource Allocation (RA_TOV) timers default to the same values. They can be changed if needed. In accordance with the FC-SW2 standard, these values must be the same on each switch within the fabric.

Use the **vsan** option to configure different TOV values for VSANs with special types of links such as FC or IP tunnels.

Examples

The following example shows how to change the default Fibre Channel timers:

```
switch# config terminal
switch(config)# fctimer e_d_tov 3000
switch(config)# fctimer r_a_tov 7000
```

Related Commands

Command	Description
show fctimer	Displays the configured Fibre Channel timer values.

fctimer abort

To discard a Fibre Channel timer (fctimer) Cisco Fabric Services (CFS) distribution session in progress, use the **fctimer abort** command in configuration mode.

fctimer abort

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to discard a CFS distribution session in progress:

```
switch# config terminal
switch(config)# fctimer abort
```

Related Commands

Command	Description
fctimer distribute	Enables CFS distribution for fctimer.
show fctimer	Displays fctimer information.

fctimer commit

To apply the pending configuration pertaining to the Fibre Channel timer (fctimer) Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **fctimer commit** command in configuration mode.

fctimer commit

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Note After the FC timer commit is completed the running configuration has been modified on all switches participating in fctimer distribution. You can then use the copy running-config startup-config fabric command to save the running configuration to the startup configuration on all the switches in the fabric.

Examples

The following example shows how to commit changes to the active Fibre Channel timer configuration:

```
switch# config terminal
switch(config)# fctimer commit
```

Related Commands

Command	Description
fctimer distribute	Enables CFS distribution for fctimer.
show fctimer	Displays fctimer information.

fctimer distribute

To enable Cisco Fabric Services (CFS) distribution for Fibre Channel timer (fctimer), use the **fctimer distribute** command. To disable this feature, use the **no** form of the command.

fctimer distribute
no fctimer distribute

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to change the default Fibre Channel timers:

```
switch# config terminal
switch(config)# fctimer distribute
```

Related Commands

Command	Description
fctimer commit	Commits the Fibre Channel timer configuration changes to the active configuration.
show fctimer	Displays fctimer information.

fctrace

To trace the route to an N port, use the **fctrace** command in EXEC mode.

fctrace {**device-alias** *aliasname*|**fcid** *fcid* **vsan** *vsan-id* [**timeout** *value*]|**pwwn** *pwwn-id* [**timeout** *seconds*]}

Syntax Description

device-alias *aliasname*	Specifies the device alias name. Maximum length is 64 characters.
fcid *fcid*	The FCID of the destination N port, with the format **0x**hhhhhh
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
timeout *value*	(Optional) Configures the timeout value. The range is 1 to 10.
pwwn *pwwn-id*	The PWWN of the destination N port, with the format hh**:**hh**:**hh**:**hh**:**hh**:**hh**:**hh**:**hh.

Command Default

By default, the period to wait before timing out is 5 seconds.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0(x)	Added the **device-alias** *aliasname* option.

Usage Guidelines

None.

Examples

The following example traces a route to the specified fcid in VSAN 1:

```
switch# fctrace fcid 0x660000 vsan 1
Route present for :  0x660000
20:00:00:05:30:00:5f:1e(0xfffc65)
Latency: 0 msec
20:00:00:05:30:00:61:5e(0xfffc66)
Latency: 0 msec
20:00:00:05:30:00:61:5e(0xfffc66)
```

The following example traces a route to the specified device alias in VSAN 1:

```
switch# fctrace device-alias x vsan 1
Route present for : 21:01:00:e0:8b:2e:80:93
20:00:00:05:30:00:4a:e2(0xfffc67)
```

fc-tunnel

To terminate a Fibre Channel tunnel in a destination switch, use the **fc-tunnel** command. To remove a configuration or revert it to factory defaults, use the no form of the command.

fc-tunnel {**enable**|**explicit-path** *name* [**next-address** *ip-address* {**loose**|**strict**}]|**tunnel-id-map** *tunnel-id* **interface fc** *slot-number*}
no fc-tunnel {**enable**|**explicit-path** *name*|**tunnel-id-map** *tunnel-id*}

Syntax Description

enable	Enables the FC tunnel feature.
explicit-path *name*	Specifies an explicit path. Maximum length is 16 characters.
next-address *ip-address*	(Optional) Specifies the IP address of the next hop switch.
loose	Specifies that a direct connection to the next hop is not required.
strict	Specifies that a direct connection to the next hop is required.
tunnel-id-map *tunnel-id*	Specifies FC tunnel ID to an outgoing interface. The range is 1 to 255.
interface fc *slot/port*	Configures the Fiber Channel interface in the destination switch.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(5)	All the fc-tunnel commands are not supported in Cisco MDS 9250i Multiservice Fabric Switch.
6.2(1)	Added the output for remote span configuration on local and remote switches.
1.2(1)	This command was introduced.

Usage Guidelines

All VSANs with RSPAN traffic must be enabled. If a VSAN containing RSPAN traffic is not enabled, it will be dropped.

The FC tunnel can only be configured in the same subnet as the VSAN interface.

The Fibre Channel tunnel feature must be enabled (the **interface fc-tunnel** command) on *each* switch in the end-to-end path of the Fibre Channel fabric in which RSPAN is to be implemented.

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 enables the FC tunnel feature:

```
switch# config terminal
switchS(config)# fc-tunnel enable
```

The following example displays remote SPAN configuration on a local switch:

```
switch(config)# fc-tunnel enable
switch(config)# interface vsan 1
switch(config)# ip address 10.10.10.66 255.255.254.0
switch(config)# no shut
switch(config)# interface fc-tunnel 102
switch(config)# source 10.10.10.66
switch(config)# destination 10.10.10.77
switch(config)# no shut
```

The following example displays remote SPAN Configuration on a remote switch:

```
switch(config)# fc-tunnel enable
switch(config)# interface  vsan 1
switch(config)# ip address 10.10.10.77 255.255.254.0
switch(config)# no shut
switch(config)# interface fc1/16
switch(config)# switchport mode sd
switch(config)# fc-tunnel tunnel-id-map 102 interface fc1/16
```

The following example places you at the explicit path prompt for the path named Path and specifies that the next hop VSAN interface IP addresses:

```
switch# config terminal
switchS(config)# fc-tunnel explicit-path Path1
switchS(config-explicit-path)# next-address 209.165.200.226
switchS(config-explicit-path)# next-address 209.165.200.227
switchS(config-explicit-path)# next-address 209.165.200.228
```

The following example places you at the explicit path prompt for the path named Path and configures a minimum cost path in which this IP address exists:

```
switchS(config)# fc-tunnel explicit-path Path3
switchS(config-explicit-path)# next-address 209.165.200.226 loose
```

The following example configures the FC tunnel (100) in the destination switch (switch D):

```
switchD(config)# fc-tunnel tunnel-id-map 100 interface fc2/1
```

The following example creates two explicit paths and configures the next hop addresses for each path in the source switch (switch S):

```
switchS# config t

switchS(config)# fc-tunnel explicit-path Path1
switchS(config-explicit-path)# next-address 209.165.200.226
switchS(config-explicit-path)# next-address 209.165.200.227
switchS(config-explicit-path)# next-address 209.165.200.228
switchS(config-explicit-path)# exit
switchS(config)# fc-tunnel explicit-path Path3
```

```
switchS(config-explicit-path)# next-address 209.165.200.226 loose
```

The following example references the configured path in the source switch (switch S):

```
switchS# config t

switchS(config)# interface fc-tunnel 100
 switchS(config)# explicit-path Path1
```

feature

To enable a feature or service on the switch, use the **feature** command. To disable a feature or service on the switch, use the **no** form of the command.

feature {**cimserver**|**cluster**|**crypto** {**ike**|**ipsec**} **dpvm**|**fport-channel-trunk**|**fabric-binding**|**fcip**|**fcrxbbcredit extended**
fcsp|**ficon**|**fport-channel-trunk**|**http-server**|**ioa**|**iscsi**|**ivr**|**npiv**|**npv**|**nxapi**|**port-security**|**privilege**|**port-track**|**san-ext-tuner**|**scheduler**|**sdv**|**sme**|**ssh**|**tacacs+**|**telnet**}
no feature {**cimserver**|**cluster**|**crypto** {**ike**|**ipsec**}
dpvm|**fport-channel-trunk**|**fabric-binding**|**fcip**|**fcrxbbcredit extended**
fcsp|**ficon**|**fport-channel-trunk**|**http-server**|**ioa**|**iscsi**|**ivr**|**npiv**|**npv**|**nxapi**|**port-security**|**privilege**|**port-track**|**san-ext-tuner**|**scheduler**|**sdv**|**sme**|**ssh**|**tacacs+**|**telnet**}

Syntax Description

cimserver	Enables or disables CIM server.
cluster	Enables or disables cluster.
crypto	Sets crypto settings.
ike	Enables or disables IKE.
ipsec	Enables or disables IPsec.
dpvm	Enables or disables the Dynamic Port VSAN Membership.
fport-channel-trunk	Enables or disables the F port channel trunking feature.
fabric-binding	Enables or disables fabric binding.
fcip	Enables or disables FCIP.
fcrxbbcredit	Enables or disables the extended rx b2b credit configuration.
extended	Sets extended settings.
fcsp	Enables or disables FCSP.
ficon	Enables or disables the FICON.
http-server	Enables or disables the HTTP server.
ioa	Enables or disables I/O Accelerator.
iscsi	Enables or disables ISCSI.
ivr	Enables or disables inter-VSAN routing.
npiv	Enables or disables the NX port ID virtualization.
npv	Enables or disables the Fibre Channel N port virtualizer.
nxapi	Enables or disables NX-API.
port-security	Enables or disables the port security.

privilege	Enables or disables Cisco IOS type privilege level support.
port-track	Enables or disables the port track feature.
san-ext-turner	Enables or disables the SAN Extension Turner Tool.
scheduler	Enables or disables scheduler.
sdv	Enables or disables the SAN Device Virtualization.
sme	Enables or disables the Storage Media Encryption.
ssh	Enables or disables SSH.
tacacs+	Enables or disables TACACS+.
telnet	Enables or disables Telnet.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	Added keyword privilege to the syntax description.
NX-OS 4.2(1)	Added keyword ioa to the syntax description.
NX-OS 4.1(3)	Added features fport-channel-trunk, npiv and npv to the syntax description.
NX-OS 4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable a feature on the switch :

```
switch(config)# feature privilege
switch(config)# feature fcip
switch(config)# feature cluster
switch(config)# feature ioa
switch(config)# feature fcsp
switch(config)# feature sdv
switch(config)# feature cimserver
switch(config)# feature scheduler
switch(config)# feature fport-channel-trunk
switch(config)# feature http-server
switch(config)# feature npv
switch(config)# feature npiv
```

Related Commands

Command	Description
show fcip	Displays FCIP information.

ficon enable

To enable the FICON feature on a switch, use the **ficon enable** command in configuration mode. To disable the feature or to revert to factory defaults, use the **no** form of the command.

ficon enable
no ficon enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.
NX-OS 4.1(1b)	This command was deprecated.

Usage Guidelines

The effects of enabling the FICON feature in a Cisco MDS switch are as follows:

- You cannot disable in-order delivery for the FICON-enabled VSAN.
- You cannot disable fabric binding or static domain ID configurations for the FICON-enabled VSAN.
- The load balancing scheme is changed to Source ID (SID)—Destination ID (DID). You cannot change it back to SID—DID—OXID.
- The IPL configuration file is automatically created.

When FICON is enabled on a VSAN, it is implicitly enabled everywhere. However, when FICON is disabled on a VSAN, it remains globally enabled. You must explicitly disable FICON to disable it throughout the fabric.

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 enables FICON on the switch:

```
switch(config)# ficon enable
```

The following example disables FICON on the switch:

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

Related Commands

Command	Description
show ficon	Displays configured FICON details.

ficon logical-port assign port-numbers

To reserve FICON port numbers for logical interfaces on the switch, use the **ficon logical-port assign port-numbers** command in configuration mode. To release the port numbers, use the **no** form of the command.

ficon logical-port assign port-numbers *[port-numbers]*
no ficon logical-port assign port-numbers *[port-numbers]*

Syntax Description

port-numbers	(Optional) Specifies the range of port numbers to assign. The range can be 0 through 153 or 0x0 through 0x99.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You must reserve port numbers for logical interfaces, such as FCIP and PortChannels, if you plan to use them.

You cannot change or release port numbers for interfaces that are active. You must disable the interfaces using the shutdown command.

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 reserves port numbers 230 through 249 for FCIP and PortChannel interfaces:

```
switch(config)# ficon logical-port assign port-numbers 230-249
```

The following example reserves port numbers 0xe6 through 0xf9 for FCIP and PortChannel interfaces:

```
switch(config#  ficon logical-port assign port-numbers 0xe6-0xf9
```

The following example releases the port numbers:

```
switch(config)# no ficon logical-port assign port-numbers 230-249
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.

ficon port default-state prohibit-all

To set the FICON port default state to prohibit all, use the **ficon port default-state prohibit-all** command in configuration mode. To disable the feature or to revert to factory defaults, use the **no** form of the command.

ficon port default-state prohibit-all
no ficon port default-state prohibit-all

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(2)	This command was introduced.

Usage Guidelines

You can change the default port prohibiting state to enabled in VSANs that you create and then selectively disable port prohibiting on implemented ports, if desired. Only the FICON configuration files created after you change the default have the new default setting.

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 enables port prohibiting as the default for all implemented interfaces on the switch:

```
switch(config)# ficon port default-state prohibit-all
```

The following example disables port prohibiting as the default for all implemented interfaces on the switch:

```
switch(config)# no port default-state prohibit-all
```

Related Commands

Command	Description
show ficon port default-state	Displays default FICON port prohibit state.

ficon slot assign port-numbers

To reserve FICON port numbers for a slot on the switch, use the **ficon slot assign port-numbers** command in configuration mode. To release the port numbers, use the **no** form of the command.

ficon slot *slot* **assign port-numbers** *[port-numbers]*
no ficon slot *slot* **assign port-numbers** *[port-numbers]*

Syntax Description

slot	Specifies the slot number, 1 through 6.
port-numbers	Specifies the range of port numbers to assign. The range can be 0 through 153, or 0x0 through 0x99. For 9513, the port numbers can be between 0 through 249, or 0x0 through 0xf9.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

A range of 255 port numbers are available for you to assign to all the ports on a switch. You can have more than 255 physical ports on a switch and the excess ports do not have ports numbers in the default numbering scheme. When you have more than 255 physical ports on your switch, you can assign unimplemented port numbers to the ports, or assign duplicate port numbers if they are not used in the same FICON VSAN. For example, you can configure port number 1 on interface fc1/1 in FICON VSAN 10 and fc10/1 in FICON VSAN 20.

FICON port numbers are not changed for ports that are active. You must first disable the interfaces using the shutdown command.

You can configure port numbers even when no module is installed in the slot, and before FICON is enabled on any VSAN.

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 reserves FICON port numbers 0 through 15 and 48 through 63 for up to 32 interfaces in slot 3:

```
swich# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ficon slot 3 assign port-numbers 0-15, 48-63
```

The following example reserves FICON port numbers 0 through 15 for the first 16 interfaces and 0 through 15 for the second 32 interfaces in slot 3:

```
switch(config)# ficon slot 3 assign port-numbers 0-15, 0-15
```

The following example changes the reserved FICON port numbers for up to 24 interfaces in slot 3:

```
switch(config)# ficon slot 3 assign port-numbers 0-15, 56-63
```

The following example releases the port numbers:

```
switch(config)# no ficon slot 3 assign port-numbers 0-15, 56-63
```

The following example shows the switch output when there are duplicate port numbers:

```
switch(config)
switch(config)# no ficon slot 1 assign port-numbers
switch(config)# ficon slot 1 assign port-numbers 0-14, 0
WARNING: fc1/16 and fc1/1 have duplicated port-number 0 in port VSAN 99
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.

ficon swap

To enable the FICON feature in a specified VSAN, use the **ficon swap** command in configuration mode.

ficon swap {**interface fc** *slot* **fc** *slot*|**portnumber** *port-number port-number*} [**after swap noshut**]

Syntax Description

interface	Configures the interfaces to be swapped.
fc	Specifies the Fibre Channel interface.
slot	Specifies the slot number, 1 through 6.
portnumber	Configures the FICON port number for this interface.
port-number	Specifies the port numbers that must be swapped
after swap noshut	(Optional) Initializes the port shut down after the ports are swapped.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Added the **interface** option.

Usage Guidelines

The **ficon swap portnumber** *old-port-number new port-number* command causes all configuration associated with *old-port-number* and *new port-number* to be swapped, including VSAN configurations. This command is only associated with the two ports in concerned. You must enter this VSAN-independent command from the EXEC mode.

If you specify the **ficon swap portnumber after swap noshut** command, the ports are automatically initialized.

The **ficon swap interface** *old-interface new-interface* command allows you to swap physical Fibre Channel ports, including port numbers, when there are duplicate port numbers on the switch.

If you specify the **ficon swap interface** *old-interface new-interface* **after swap noshut** command, the ports are automatically initialized.

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 swaps the contents of ports 3 with port 15, shuts them down, and automatically initializes both ports:

```
switch# ficon swap portnumber 3 15 after swap noshut
```

The following example swaps the contents of ports 3 with port 15 and shuts them down:

```
switch# ficon swap portnumber 3 15
```

The following example swaps port 1 with port 6:

```
switch# ficon swap interface fc1/1 fc1/6
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.

ficon-tape-read-accelerator

To enable FICON tape read acceleration for the FCIP interface, use the **ficon-tape-read-accelerator** command in interface configuration submode. To disable FICON tape read acceleration for the FCIP interface, use the **no** form of the command.

ficon-tape-read-accelerator
no ficon-tape-read-accelerator

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Interface configuration submode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to enable FICON tape read acceleration on the FCIP interface:

```
switch# config terminal
switch(config)# interface fcip 2
switch(config-if)# ficon-tape-read-accelerator
switch(config-if)#
```

The following example shows how to disable FICON tape read acceleration on the FCIP interface:

```
switch# config terminal
switch(config)# interface fcip 2
switch(config-if)#  no ficon-tape-read-accelerator
switch(config-if)#
```

Related Commands

Command	Description
show fcip	Displays FCIP profile information.

ficon-tape-accelerator vsan

To enable FICON tape acceleration for the FCIP interface, use the **ficon-tape-accelerator vsan** command in interface configuration submode. To disable FICON tape acceleration for the FCIP interface, use the **no** form of the command.

ficon-tape-accelerator vsan vsan-id
no ficon-tape-accelerator vsan vsan-id

Syntax Description

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

Command Default

Disabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Cisco MDS NX-OS software provides acceleration for FICON tape write operations over FCIP for the IBM VTS and tape libraries that support the 3490 command set. FICON tape read acceleration over FCIP is not supported.

FICON tape acceleration will not work if multiple inter-switch links (ISLs) are present in the VSAN.

FICON write acceleration and tape acceleration can be enabled at the same time on the FCIP interface.

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 enables FICON tape acceleration on the FCIP interface:

```
switch# config terminal
switch(config)# interface fcip 2
switch(config-if)# ficon-tape-accelerator vsan 100
This configuration change will disrupt all traffic on the FCIP interface in all
VSANs.  Do you wish to continue? [no] y
```

The following example disables FICON tape acceleration on the FCIP interface:

```
switch(config-if)# no ficon-tape-accelerator vsan 100
This configuration change will disrupt all traffic on the FCIP interface in all
VSANs.  Do you wish to continue? [no] y
```

Related Commands

Command	Description
show fcip	Displays FCIP profile information.
write-accelerator	Enables write acceleration and tape acceleration for the FCIP interface.

ficon vsan (EXEC mode)

To configure FICON related parameters in EXEC mode, use the **ficon vsan** command. To remove the configuration or revert to the default values, use the **no** form of the command.

ficon vsan *vsan-id*|**apply file** *file-name*|**copy file** *old-file-name new-file-name*|**offline**|**online**

vsan-id	The FICON configuration mode for the specified VSAN (from 1 to 4096).
apply file *file-name*	Specifies the existing FICON configuration file-name after switch initialization. Maximum length is 80 characters.
copy file	Copies of the specified FICON configuration file.
old-file-name	Specifies the old (existing) FICON configuration file name.
new-file-name	Specifies the new name for the copied file.
offline	Logs out all ports in the VSAN that needs to be suspended.
online	Removes the offline condition to allow ports to log on again.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

When an MDS switch is booting up with saved configuration, if FICON is enabled on a VSAN, the IPL configuration file is applied automatically by the NX-OS software after the switch initialization is completed.

Use the **ficon vsan** *vsan-id* **copy file** *exiting-file-name save-as-file-name* command to copy an existing FICON configuration file. You can see the list of existing configuration files by issuing the **show ficon vsan** *vsan-id* command.

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 applies the configuration from the saved files to the running configuration:

```
switch# ficon vsan 2 apply file SampleFile
```

The following example copies an existing FICON configuration file called IPL and renames it to IPL3.

```
switch# ficon vsan 20 copy file IPL IPL3
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.

ficon vsan (configuration mode)

To enable the FICON feature in a specified VSAN, use the **ficon vsan** command in configuration mode. To disable the feature or to revert to factory defaults, use the **no** form of the command.

ficon vsan *vsan-id*
no ficon vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Enters the FICON configuration mode for the specified VSAN (from 1 to 4096).

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

An IPL configuration file is automatically created:

Once you enable FICON, you cannot disable in-order delivery, fabric binding, or static domain ID configurations.

When you disable FICON, the FICON configuration file is also deleted.

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 enables FICON on VSAN 2:

```
switch(config)# ficon vsan 2
```

The following example disables FICON on VSAN 6:

```
switch(config)# no ficon vsan 6
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.

file

To access FICON configuration files in a specified VSAN, use the **file** command. To disable the feature or to revert to factory defaults, use the **no** form of the command.

file *file-name*
no file *file-name*

Syntax Description

file-name	The FICON configuration file in the specified VSAN

Command Default

None.

Command Modes

FICON configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The configuration file submode allows you to create and edit FICON configuration files. If a specified file does not exist, it is created. Up to 16 files can be saved. Each file name is restricted to 8 alphanumeric characters.

Examples

The following example accesses the FICON configuration file called IplFile1 for VSAN 2. If this file does not exist, it is created:

```
switch# config terminal
switch(config)# ficon vsan 2
switch(config-ficon)# file IplFile1
switch(config-ficon-file)#
```

The following example deletes a previously created FICON configuration file:

```
switch(config-ficon)# no file IplFileA
```

Related Commands

Command	Description
ficon vsan	Enables FICON for a VSAN.
show ficon	Displays configured FICON details.

find

To display a list of files on a file system, use the **find** command in EXEC mode.

find *filename*

Syntax Description

filename	Specifies a search string to match to the files in the default directory. Maximum length is 64 characters.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use the **find** (Flash file system) command to display more details about the files in a particular file system.

Examples

The following example is sample output of all files that begin with the letter *a*:

```
switch# find a
./accountingd
./acl
./ascii_cfg_server
./arping
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
dir	Displays all files in a given file system.

flex-attach virtual-pwwn

To map the real port WWN (pWWN) and a user-specific virtual pWWN, use the**flex-attach virtual-pwwn** command. To disable the mapping, use the **no** form of the command.

flex-attach virtual-pwwn *vpwwn* **pwwn** *pwwn*
no flex-attach virtual-pwwn *vpwwn* **pwwn** *pwwn*

Syntax Description

vpwwn	Specifies the virtual pWWN chosen by the user.
pwwn *pwwn*	Specifies the pWWN to be mapped to the user-specific virtual pWWN. **Note** pWWN must not be logged in.

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to map the real pWWN and a user-specific virtual pWWN on an interface:

```
switch# config
Enter configuration commands, one per line.  End with CNTL/Z.
switch# (config) flex-attach virtual-pwwn 20:04:00:a0:b8:16:92:18 pwwn 21:03:00:a0:b9:16:92:16
```

Related Commands

Command	Description
flex-attach virtual-pwwn auto	Enables the FlexAttach virtual pWWN on a specific interface.
flex-attach virtual-pwwn interface	Sets the user-specific FlexAttach virtual pWWN.

flex-attach virtual-pwwn auto

To enable the FlexAttach virtual port WWN (pWWN) on a specific interface, use the **flex-attach virtual-pwwn** auto command. To disable the virtual pWWN, use the **no** form of the command.

flex-attach virtual-pwwn auto [**interface auto** *interface-list*]
no flex-attach virtual-pwwn auto [**interface auto** *interface-list*]

Syntax Description

interface auto *interface-list*	Specifies the interface list on which FlexAttach virtual pWWN should be enabled. **Note** All interfaces in the interface-list value must be in the shut mode. If the interface-list value is not provided, then all ports must be in the shut mode.

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

The NPV switch assigns the virtual pWWNs to the interface on which FlexAttach is enabled.

Examples

The following example shows how to enable FlexAttach virtual pWWN on a interface:

```
switch# config
Enter configuration commands, one per line. End with CNTL/Z.
switch#(config)# flex-attach virtual-pwwn auto interface fc 1/1
```

Related Commands

Command	Description
flex-attach virtual-pwwn interface	Sets the user-specific FlexAttach virtual pWWN.

flex-attach virtual-pwwn interface

To set the user-specific FlexAttach virtual port WWN (pWWN) on an interface, use the **flex-attach virtual-pwwn interface** command. To disable the virtual pWWN, use the **no** form of the command.

flex-attach virtual-pwwn *vpwwn* **interface** *interface* [**vsan** *vsan*]
no flex-attach virtual-pwwn *vpwwn* **interface** *interface* [**vsan** *vsan*]

Syntax Description

vpwwn	Specifies the virtual pWWN chosen by the user.
interface	Specifies the interface on which the FlexAttach virtual port has to be enabled. **Note** The interface must be in the shut state.
vsan *vsan*	(Optional) Specifies the VSAN on which FlexAttach should be enabled.

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to set the user-specific virtual pWWN on an interface:

```
switch# config
Enter configuration commands, one per line.  End with CNTL/Z.
```

Related Commands

Command	Description
flex-attach virtual-pwwn auto	Enables the FlexAttach virtual pWWN on a specific interface.

flowgroup

To configure an IOA flow group, use the **flowgroup** command.

flowgroup *{name}*
no flowgroup *{name}*

Syntax Description

name	Specifies an IOA flow group name. The maximum size is 31 characters.

Command Default

None.

Command Modes

Configuration submode.

Command History

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

Usage Guidelines

None.

Examples

```
The following example shows how to configure the IOA flow group:
switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ioa cluster tape_vault
switch(config-ioa-cl)# flowgroup tsm
switch(config-ioa-cl)#
```

Related Commands

Command	Description
interface ioa	Configures the IOA interface.

format

To erase all the information on a module, use the **format** command in EXEC mode.

format {**bootflash:** | **logflash:** | **slot0:** | **usb1:** | **usb2:**}

Syntax Description

bootflash:	Specifies bootflash: memory.
logflash:	Specifies logflash: memory.
slot0:	Specifies the flash device in slot 0.
usb1:	Specifies the USB memory in host1.
usb2:	Specifies the USB memory in host 2.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.3(1a)	Added the USB1 and USB 2 parameters.

Usage Guidelines

The SAN-OS and NX-OS software supports Cisco-certified CompactFlash devices that are formatted using Cisco MDS 9000 switches. Using uncertified CompactFlash devices may result in unpredictable consequences; formatting CompactFlash devices using other platforms may result in errors.

Examples

The following example erases all information on the bootflash memory.

```
switch# format bootflash:
This command is going to erase the contents of your bootflash:.
Do you want to continue? (y/n)  [n]
```

The following example erases all information on the logflash memory.

```
switch# format logflash:
This command is going to erase the contents of your logflash:.
Do you want to continue? (y/n)  [n]
The following example erases all information on slot0.
switch# format
slot0:
This command is going to erase the contents of your slot0:
Do you want to continue? (y/n)  [n]
```

The following example erases all information on usb1:

```
switch# format
usb1:
This command is going to erase the contents of your usb1:.
Do you want to continue? (y/n)  [n]
```

The following example erases all information on usb2:.

```
switch# format
usb2:
This command is going to erase the contents of your usb2:.
Do you want to continue? (y/n)  [n]
```

fspf config vsan

To configure an FSPF feature for the entire VSAN, use the **fspf config vsan** command in configuration mode. To delete FSPF configuration for the entire VSAN, use the **no** form of the command.

fspfconfigvsan*vsan-id***min-ls-arrival***ls-arrival-time***min-ls-interval***ls-interval-time***region***region-id***spf**{**hold-time***spf-holdtime*|**static**}
nofspfconfigvsan*vsan-id***min-ls-arrivalmin-ls-intervalregionspf**{**hold-time**|**static**}

Syntax Description

vsan-*id*	Specifies a VSAN ID. The range is 1 to 4093.
min-ls-arrival *ls-arrival-time*	Specifies the minimum time before a new link state update for a domain will be accepted by switch. The parameter ls-arrival-time is an integer specifying time in milliseconds. The range is 0 to 65535.
min-ls-interval *ls-interval-time*	Specifies the minimum time before a new link state update for a domain will be generated by the switch. The parameter ls-interval-time is an integer specifying time in milliseconds. The range is 0 to 65535.
region *region-id*	Specifies the autonomous region to which the switch belongs. The backbone region has region-id=0. The parameter region-id is an unsigned integer value ranging from 0 to 255.
spf	Specifies parameters related to SPF route computation.
hold-time *spf-holdtime*	Specifies the time between two consecutive SPF computations. If the time is small then routing will react faster to changes but CPU usage will be more. The parameter spf-holdtime is an integer specifying time in milliseconds. The range is 0 to 65535.
static	Forces static SPF computation.

Command Default

In the FSPF configuration mode, the default is dynamic.

If configuring spf hold-time, the default value for FSPF is 0.

If configuring min-ls-arrival, the default value for FSPF is 1000 msecs.

If configuring min-ls-interval, the default value for FSPF is 5000 msecs.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command configures FSPF on VSANs globally.

For the commands entered in FSPF configuration mode, you do not have to specify the VSAN number every time. This prevents configuration errors that might result from specifying the wrong VSAN number for these commands.

Examples

The following example configures FSPF globally in VSAN 1, deletes the FSPF configured in VSAN 3, disables FSPF in VSAN 5, and enables FSPF in VSAN 7:

```
switch## config terminal
switch(config)##
switch(config)# fspf config vsan 1
switch-config-(fspf-config)# spf static
switch-config-(fspf-config)# exit
switch(config)#
switch(config)# no fspf config vsan 3
switch(config)#
```

Related Commands

Command	Description
fspf cost	Configures the cost for the selected interface in the specified VSAN (from the switch(config-if)# prompt).
fspf enable	Enables FSPF routing protocol in the specified VSAN (from the switch(config-if)# prompt).
fspf hello-interval	Specifies the hello message interval to verify the health of a link in the VSAN (from the switch(config-if)# prompt).
fspf passive	Disables the FSPF protocol for the specified interface in the specified VSAN (from the switch(config-if)# prompt).
fspf retrasmit	Specifies the retransmit time interval for unacknowledged link state updates in specified VSAN (from the switch(config-if)# prompt).
show fspf interface	Displays information for each selected interface.

fspf cost

To configure FSPF link cost for a Fibre Channel interface, use the **fspf cost** command. To revert to the default value, use the **no** form of the command.

fspfcost*link-cost***vsan***vsan-id*
nofspfcost*link-cost***vsan***vsan-id*

Syntax Description

link-cost	Enters FSPF link cost. The range is 1 to 30000.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

1000 for 1 Gbps

500 for 2 Gbps

250 for 4 Gbps

250 for 4 Gbps

125 for 8 Gbps

100 for 10 Gbps

62 for 16 Gbps

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.

FSPF tracks the state of links on all switches in the fabric, associates a cost with each link in its database, and then chooses the path with a minimal cost. The cost associated with an interface can be changed using the **fspf cost** command to implement the FSPF route selection.

Examples

The following example configures the FSPF link cost on an Fibre Channel interface:

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# fspf cost 5000 vsan 1
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

fspf dead-interval

To set the maximum interval for which a hello message must be received before the neighbor is considered lost, use the **fspf dead-interval** command. To revert to the default value, use the **no** form of the command.

fspfdead-interval*seconds***vsan***vsan-id*
nofspfdead-interval*seconds***vsan***vsan-id*

Syntax Description

seconds	Specifies the FSPF dead interval in seconds. The rage is 2 to 65535.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

80 seconds.

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.

Note This value must be the same in the ports at both ends of the ISL.

Caution An error is reported at the command prompt if the configured dead time interval is less than the hello time interval.

Examples

The following example configures the maximum interval of 400 seconds for a hello message before the neighbor is considered lost:

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# fspf dead-interval 4000 vsan 1
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

fspf enable vsan

To enable FSPF for a VSAN, use the **fspf enable** command in configuration mode. To disable FSPF routing protocols, use the **no** form of the command.

fspfenablevsan*vsan-id*
nofspfenablevsan*vsan-id*

Syntax Description

vsan-id	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command configures FSPF on VSANs globally.

Examples

The following example enables FSPF in VSAN 5 and disables FSPF in VSAN 7:

```
switch## config terminal
switch(config)# fspf enable vsan 5
switch(config)# no fspf enable vsan 7
```

Related Commands

Command	Description
fspf config vsan	Configures FSPF features for a VSAN.
show fspf interface	Displays information for each selected interface.

fspf hello-interval

To verify the health of the link, use the **fspf hello-interval** command. To revert to the default value, use the **no** form of the command.

fspfhello-interval*seconds***vsan***vsan-id*
nofspfhello-interval*seconds* **vsan***vsan-id*

Syntax Description

seconds	Specifies the FSPF hello-interval in seconds. The rage is 1 to 65534.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

20 seconds.

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.

This command configures FSPF for the specified FCIP interface.

Note This value must be the same in the ports at both ends of the ISL.

Examples

The following example configures a hello interval of 3 seconds on VSAN 1:

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# fspf hello-interval 3 vsan 1
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

fspf passive

To disable the FSPF protocol for selected interfaces, use the **fspf passive** command. To revert to the default state, use the **no** form of the command.

fspf passive vsan *vsan-id*
no fspf passive vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

FSPF is enabled.

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.

By default, FSPF is enabled on all E ports and TE ports. FSPF can be disabled by setting the interface as passive using the **fspf passive** command.

Note FSPF must be enabled on the ports at both ends of the ISL for the protocol to operate correctly.

Examples

The following example disables the FSPF protocol for the selected interface on VSAN 1:

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# fspf passive vsan 1
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

fspf retransmit-interval

To specify the time after which an unacknowledged link state update should be transmitted on the interface, use the **fspf retransmit-interval** command. To revert to the default value, use the **no** form of the command.

fspf retransmit-interval *seconds* **vsan** *vsan-id*
no spf retransmit-interval *seconds* **vsan** *vsan-id*

Syntax Description

seconds	Specifies FSPF retransmit interval in seconds. The range is 1 to 65535.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

5 seconds.

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.

Note This value must be the same in the ports at both ends of the ISL.

Examples

The following example specifies a retransmit interval of 6 seconds after which an unacknowledged link state update should be transmitted on the interface for VSAN 1:

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# fspf retransmit-interval 6 vsan 1
```

Related Commands

Command	Description
show fspf interface	Displays information for each selected interface.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

G Commands

group

To configure a Modular Exponentiation (MODP) Diffie-Hellman (DH) group for an IKE protocol policy, use the **group** command in IKE policy configuration submode. To revert to the default, use the **no** form of the command.

group {**1**|**2**|**5**}
no group

Syntax Description

1	Specifies 768-bit MODP DH group.
2	Specifies 1024-bit MODP DH group.
5	Specifies 1536-bit MODP DH group.

Command Default

1.

Command Modes

IKE policy configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Examples

The following example shows how to configure the DH group for the IKE protocol:

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# policy 1
switch(config-ike-ipsec-policy)# group 1
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
policy	Configures IKE policy parameters.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

gzip

To compress (zip) a specified file using LZ77 coding, use the **gzip** command in EXEC mode.

gzip {**bootflash:**|**slot0:**|**volatile:**} *filename*

Syntax Description

bootflash:	Source location for the file to be compressed and destination of the compressed file.
slot0:	Source location for the file to be compressed and destination of the compressed file.
volatile:	Source location for the file to be compressed and destination of the compressed file. This is the default directory.
filename	The name of the file to be compressed.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is useful in compressing large files. The output of the **show tech-support** command can directed to a file and compressed for further use. The **gzip** command replaces the source file with a compressed .gz file.

Examples

This example directs the output of the **show tech-support** command to a file (Samplefile) and then zips the file and displays the difference in the space used up in the volatile: directory:

```
switch# show tech-support > Samplefile
Building Configuration ...
switch# dir
    1525859     Jul 04 00:51:03 2003  Samplefile
Usage for volatile://
    1527808 bytes used
   19443712 bytes free
   20971520 bytes total
switch# gzip volatile:Samplefile
switch# dir
     266069     Jul 04 00:51:03 2003  Samplefile.gz
Usage for volatile://
     266240 bytes used
   20705280 bytes free
   20971520 bytes total
```

Related Commands

Command	Description
gunzip	Uncompresses LZ77 coded files.

gunzip

To uncompress (unzip) LZ77 coded files, use the **gunzip** command in EXEC mode.

gunzip {**bootflash:**|**slot0:**|**volatile:**} *filename*

Syntax Description

bootflash:	Specifies the source location for the compressed file and destination of the uncompressed file.
slot0:	Specifies the source location for the compressed file and destination of the uncompressed file.
volatile:	Specifies the source location for the compressed file and destination of the uncompressed file. This is the default directory.
filename	Specifies the name of the compressed file.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is useful in uncompressing large files. The **gunzip** command replaces the compressed.gz source file with an uncompressed file.

Examples

This example unzips a compressed file on volatile: directory and displays the space used:

```
switch# dir
     266069     Jul 04 00:51:03 2003  Samplefile.gz
Usage for volatile://
     266240 bytes used
   20705280 bytes free
   20971520 bytes total
switch# gunzip Samplefile
switch# dir
    1525859     Jul 04 00:51:03 2003 Samplefile
Usage for volatile://
    1527808 bytes used
   19443712 bytes free
   20971520 bytes total
```

Related Commands

Command	Description
gzip	Compresses a specified file using LZ77 coding.

H Commands

hardware ejector enable

To enable the hardware card ejector functionality when the ejector lever is unlocked, use the hardware ejector enable command.

hardware ejector enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Global configuration mode.

Command History

Release	Modification
6.2(3)	This command was introduced.

Usage Guidelines

This command does not require a license.

The purpose of the ejector release button on the supervisor or linecard is to unlock the ejector release lever. When enabled, this command causes the supervisor to power down when the ejector release button is pressed. In the case of a linecard, both ejector release buttons have to be pressed in order for the power down of the linecard to occur.

Examples

This example shows the configuration command to enable the hardware power down feature when the ejector release button(s) are pressed:

```
switch# config terminal
switch(config)# hardware ejector enable
```

This example shows the configuration command to disable the hardware power down feature when the ejector release button is pressed:

```
switch# config terminal
switch(config)# no hardware ejector enable
```

hardware fabric crc

To enable internal CRC detection and isolation functionality, use the **hardware fabric crc** command in configuration mode. To disable this functionality, use the no form of the command.

hardware fabric crc [**threshold** *threshold-count*]
no hardware fabric crc

Syntax Description

threshold-count	Specifies the threshold count, taken over a 24-hour period, consecutively. The range is 1 to 100.

Command Default

3.

Command Modes

Configuration mode.

Usage Guidelines

None.

Examples

The following example shows how to enable internal CRC detection and isolation:

```
switch# config terminal
switch(config)# hardware fabric crc [threshold  threshold-count ]
switch(config)#
```

The following example shows how to disable internal CRC detection and isolation:

```
switch# config terminal
switch(config)# no hardware fabric crc
switch(config)#
```

hash

To configure a hash algorithm for an IKE protocol policy, use the **hash** command in IKE policy configuration submode. To revert to the default, use the **no** form of the command.

hash {**md5**|**sha**}
no hash

Syntax Description

md5	Specifies the MD5[4] hash algorithm.
sha	Specifies the SHA[5].

[4] MD5 = Message-Digest
[5] SHA = Secure Hash Algorithm

Command Default

SHA.

Command Modes

IKE policy configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Examples

The following example shows how to configure the hash algorithm for the IKE protocol:

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# policy 1
switch(config-ike-ipsec-policy)# hash md5
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
policy	Configures IKE policy parameters.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

host

To configure the host PWWN for the flow, use the **host** command. To delete a flow from a given flowgroup, use the **no** form of the command.

host *pwwn* **target** *pwwn* **vsan** *vsan id* **[tape] [compression]**
no host *pwwn* **target** *pwwn* **vsan** *vsan id* **[tape] [compression]**

Syntax Description

pwwn	Specifies the host and target pwwn for the flow.
vsan	Specifies the VSAN where this flow is accelerated.
vsan id	Specifies the vsan ID where this flow is accelerated. The range is from 1 to 4093.
tape	Enables tape acceleration.
compression	Enables compression.

Command Default

None.

Command Modes

Configuration submode.

Command History

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

Usage Guidelines

None.

Examples

```
The following example shows how to add a flow from a given flowgroup:
switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ioa cluster tape_vault
switch(config-ioa-cl)# flowgroup tsm
switch(config-ioa-cl-flgrp)# host 10:0:0:0:0:0:0:1 target 11:0:0:0:0:0:0:1 vsan 100 tape
switch(config-ioa-cl-flgrp)# host 10:0:0:0:0:0:0:1 target 11:0:0:0:0:0:0:1 vsan 100
compression
switch(config-ioa-cl-flgrp)# host 10:0:0:0:0:0:0:2 target 11:0:0:0:0:0:0:2 vsan 100 tape
compression
sjc-sw2(config-ioa-cl-flgrp)# end
```

Related Commands

Command	Description
flowgroup	Configures IOA flowgroup.

host

Use the **host** command to configure the switch offline state, the mainframe access control parameters, and the mainframe time stamp parameters. To disable the configuration or to revert to factory defaults, use the **no** form of the command.

host {**control** [**switch offline**]|**port control**|**set-timestamp**}
no host {**control** [**switch offline**]|**port control**|**set-timestamp**}

Syntax Description

control	Allows the host control of FICON.
switch offline	(Optional) Allows the host to move the switch to an offline state and shut down the ports (default).
port control	Enables the host to configure FICON parameters.
set-timestamp	Allows the host to set the director clock.

Command Default

Host offline control enabled.

Command Modes

FICON configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

By default, the clock in each VSAN is the same as the switch hardware clock. Mainframe users are allowed to change the VSAN-clock.

Examples

The following example prohibits mainframe users from moving the switch to an offline state:

```
switch# config terminal
switch(config)# ficon vsan 2
switch(config-ficon)# no host control switch offline
```

The following example allows the host to move the switch to an offline state and shut down the ports:

```
switch(config-ficon)# host control switch offline
```

The following example prohibits mainframe users to configure FICON parameters in the Cisco MDS switch (default):

```
switch(config-ficon)# no host port control
```

The following example allows mainframe users to configure FICON parameters in the Cisco MDS switch:

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

The following example prohibits mainframe users from changing the VSAN-specific clock:

```
switch(config-ficon)# no host set-timestamp
```

The following example allows the host to set the clock on this switch (default):

```
switch(config-ficon)# host set-timestamp
```

Related Commands

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

hw-module logging onboard

To configure on-board failure logging (OBFL), use the **hw-module logging onboard** command. To disable this feature, use the **no** form of the command.

hw-module logging onboard [**module** *slot*] *[log-type]*
no hw-module logging onboard [**module** *slot*] *[log-type]*

Syntax Description

module *slot*	Configures OBFL for a specified module.
log-type	Specifies the type of events for on-board failure logging.
cpu-hog	Specifies CPU hog events.
environmental-history	Specifies environmental history events.
error-stats	Specifies error statistics events.
interrupt-stats	Specifies interrupt statistics events.
mem-leak	Specifies memory leak events.
miscellaneous-error	Specifies miscellaneous information events.
obfl-logs	Specifies boot uptime, device version, and OBFL history.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

OBFL data uses the module's persistent logging facility to store data in its CompactFlash memory. When OBFL is disabled, the persistent logging facility discards all entries sent to it for logging.

Examples

The following example configures on-board failure logging of memory leak events on module 2:

```
switch# config terminal
switch(config)# hw-module logging onboard module 2 mem-leak
```

Related Commands

Command	Description
clear logging onboard	Clears OBFL information.
show logging onboard	Displays OBFL information.

I Commands

identity

To configure the identity for the IKE protocol, use the **identity** command in IKE configuration submode. To delete the identity, use the **no** form of the command.

identity {**address**|**hostname**}
no identity {**address**|**hostname**}

Syntax Description

address	Sets the IKE identity to be the IPv4 address of the switch.
hostname	Sets the IKE identity to be the host name of the switch.

Command Default

None.

Command Modes

IKE configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Before configuring a certificate for the switch, configure the host name and domain name, and set the identity to be the host name. This allows the certificate to be used for authentication.

Note The host name is the fully qualified domain name (FQDN) of the switch. To use the switch FQDN for the IKE identity, you must first configure both the switch name and the domain name. The FQDN is required for using RSA signatures for authentication. By default address is identified.

Examples

The following example shows how to set the IKE identity to the IP address of the switch:

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# identity address
```

The following example shows how to delete the IKE identity:

```
switch(config-ike-ipsec)# no identity address
```

The following example shows how to set the IKE identity to the host name:

```
switch(config-ike-ipsec)# identity hostname
```

The following example shows how to delete the IKE identity:

```
switch(config-ike-ipsec)# no identity hostname
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

ingress-sa

To configure the Security Association (SA) to the ingress hardware, use the **ingress-sa** command. To delete the SA from the ingress hardware, use the **no** form of the command.

ingress-sa *spi-number*
no ingress-sa *spi-number*

Syntax Description

spi-number	The range is from 256 to 4294967295.

Command Default

None.

Command Modes

Configuration submode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure the SA to the ingress hardware:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface fc 2/1 - 3
switch(config-if)# fcsp esp manual
switch(config-if-esp)# ingress-sa 258
switch(config-if-esp)#
```

Related Commands

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

initiator

To configure the initiator version and address, use the **initiator** command IKE configuration submode. To revert to the default, use the **no** form of the command.

initiator version *version* **address** *ip-address*
no initiator version *version* **address** *ip-address*

Syntax Description

version	Specifies the protocol version number. The only valid value is 1.
address *ip-address*	Specifies the IP address for the IKE peer. The format is *A.B.C.D*.

Command Default

IKE version 2.

Command Modes

IKE configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Examples

The following example shows how initiator information for the IKE protocol:

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# initiator version 1 address 10.1.1.1
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

in-order-guarantee

To enable in-order delivery, use the **in-order-guarantee** command in configuration mode. To disable in-order delivery, use the **no** form of the command.

in-order-guarantee [**vsan** *vsan-id*]
no in-order-guarantee [**vsan** *vsan-id*]

Syntax Description

vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is 1 to 4093.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

In-order delivery of data frames guarantees frame delivery to a destination in the same order that they were sent by the originator.

Examples

The following example shows how to enable in-order delivery for the entire switch:

```
switch# config terminal
switch(config) # in-order-guarantee
```

The following example shows how to disable in-order delivery for the entire switch:

```
switch(config)# no in-order-guarantee
```

The following example shows how to enable in-order delivery for a specific VSAN:

```
switch(config)# in-order-guarantee vsan 3452
```

The following example shows how to disable in-order delivery for a specific VSAN:

```
switch(config)# no in-order-guarantee vsan 101
```

Related Commands

Command	Description
show in-order-guarantee	Displays the in-order-guarantee status.

install all

To upgrade all modules in any Cisco MDS 9000 family switch, use the **install all** command. This upgrade can happen nondisruptively or disruptively depending on the current configuration of your switch.

install all [{**asm-sfn** *file name* |**kickstart**|**ssi**|**system**} **URL**]

Syntax Description

asm-sfn *filename*	(Optional) Upgrades the ASM image.
kickstart	(Optional) Upgrades the kickstart image.
ssi	(Optional) Upgrades the SSI image.
system	(Optional) Upgrades the system image.
URL	(Optional) Specifies the location URL of the source file to be installed.

The following table lists the aliases for *URL*.

bootflash:	Source location for internal bootflash memory.
slot0:	Source location for the CompactFlash memory or PCMCIA card.
volatile:	Source location for the volatile file system.
tftp:	Source location for a Trivial File Transfer Protocol (TFTP) network server. The syntax for this URL is **tftp: [[//location] /directory] /filename.**
ftp:	Source location for a File Transfer Protocol (FTP) network server. The syntax for this URL is **ftp: [[//location] /directory] /filename.**
sftp:	Source location for a Secure Trivial File Transfer Protocol (SFTP) network server. The syntax for this URL is **sftp: [[//<username@>location] /directory] /filename.**
scp:	Source location for a Secure Copy Protocol (SCP) network server. The syntax for this URL is **scp: [[//location] /directory] /filename.**
image-filename	The name of the source image file.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(3)	This command was introduced.
1.2(2)	Added the **asm-sfn** keyword and made all keywords optional.
2.0(1b)	Added the **ssi** keyword.

Usage Guidelines

The **install all** command upgrades all modules in any Cisco MDS 9000 Family switch.

Tip During a software upgrade to Cisco MDS SAN-OS 3.1(3), all modules that are online are tested and the installation stops if any modules are running with a faulty CompactFlash. When this occurs, the switch can not be upgraded until the situation is corrected. A system message displays the module information and indicates that you must issue the **system health cf-crc-check module** CLI command to troubleshoot.

To copy a remote file, specify the entire remote path exactly as it is.

Caution If a switchover is required when you issue the **install all** command from a Telnet or SSH session, all open sessions are terminated. If no switchover is required, the session remains unaffected. The software issues a self-explanatory warning at this point and provides the option to continue or terminate the installation.

Examples

The following example displays the result of the **install all** command if the system and kickstart files are specified locally:

```
switch# install all sys bootflash:isan-1.3.1 kickstart bootflash:boot-1.3.1

Verifying image bootflash:/boot-1.3.1
[####################] 100% -- SUCCESS

Verifying image bootflash:/isan-1.3.1
[####################] 100% -- SUCCESS

Extracting "slc" version from image bootflash:/isan-1.3.1.
[####################] 100% -- SUCCESS

Extracting "ips" version from image bootflash:/isan-1.3.1.
[####################] 100% -- SUCCESS

Extracting "system" version from image bootflash:/isan-1.3.1.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image bootflash:/boot-1.3.1.
[####################] 100% -- SUCCESS

Extracting "loader" version from image bootflash:/boot-1.3.1.
[####################] 100% -- SUCCESS


Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes  non-disruptive       rolling
     2       yes      disruptive       rolling  Hitless upgrade is not supported
     3       yes      disruptive       rolling  Hitless upgrade is not supported
     4       yes  non-disruptive       rolling
     5       yes  non-disruptive         reset
     6       yes  non-disruptive         reset


Images will be upgraded according to following table:
Module       Image       Running-Version           New-Version  Upg-Required
------  ----------  --------------------  --------------------  ------------
     1         slc               1.3(2a)                1.3(1)           yes
```

```
      1       bios     v1.1.0(10/24/03)     v1.1.0(10/24/03)          no
      2        ips              1.3(2a)               1.3(1)         yes
      2       bios     v1.1.0(10/24/03)     v1.1.0(10/24/03)          no
      3        ips              1.3(2a)               1.3(1)         yes
      3       bios     v1.1.0(10/24/03)     v1.1.0(10/24/03)          no
      4        slc              1.3(2a)               1.3(1)         yes
      4       bios     v1.1.0(10/24/03)     v1.1.0(10/24/03)          no
      5     system              1.3(2a)               1.3(1)         yes
      5  kickstart              1.3(2a)               1.3(1)         yes
      5       bios     v1.1.0(10/24/03)     v1.1.0(10/24/03)          no
      5     loader               1.2(2)               1.2(2)          no
      6     system              1.3(2a)               1.3(1)         yes
      6  kickstart              1.3(2a)               1.3(1)         yes
      6       bios     v1.1.0(10/24/03)     v1.1.0(10/24/03)          no
      6     loader               1.2(2)               1.2(2)          no

Do you want to continue with the installation (y/n)?  [n] y

Install is in progress, please wait.

Syncing image bootflash:/boot-1.3.1 to standby.
[####################] 100% -- SUCCESS

Syncing image bootflash:/isan-1.3.1 to standby.
[####################] 100% -- SUCCESS

Jan 18 23:40:03 Hacienda %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from
Performing configuration copy.
[####################] 100% -- SUCCESS

Module 6: Waiting for module online.
|
Auto booting bootflash:/boot-1.3.1 bootflash:/isan-1.3.1...
Booting kickstart image: bootflash:/boot-1.3.1....
.....................................Image verification OK

Starting kernel...
INIT: version 2.78 booting
Checking all filesystems..r.r.. done.
Loading system software
Uncompressing system image: bootflash:/isan-1.3.1
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
INIT: Entering runlevel: 3
```

The following example displays the file output continuation of the **install all** command on the console of the standby supervisor module:

```
Hacienda(standby)#

Auto booting bootflash:/boot-1.3.1 bootflash:/isan-1.3.1...
Booting kickstart image: bootflash:/boot-1.3.1....
.....................................Image verification OK

Starting kernel...
INIT: version 2.78 booting
Checking all filesystems..r.r.. done.
Loading system software
Uncompressing system image: bootflash:/isan-1.3.1
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
INIT: Entering runlevel: 3
Continue on installation process, please wait.
The login will be disabled until the installation is completed.
```

```
Module 6: Waiting for module online.
Jan 18 23:43:02 Hacienda %PORT-5-IF_UP: Interface mgmt0 is up
Jan 18 23:43:19 Hacienda %LICMGR-3-LOG_LIC_NO_LIC: No license(s) present for feature
FM_SERVER_PKG. Application(s) shutdown in 53 days.
Jan 18 23:43:19 Hacienda %LICMGR-3-LOG_LIC_NO_LIC: No license(s) present for feature
ENTERPRISE_PKG. Application(s) shutdown in 50 days.
Jan 18 23:43:19 Hacienda %LICMGR-3-LOG_LIC_NO_LIC: No license(s) present for feature
SAN_EXTN_OVER_IP. Application(s) shutdown in 50 days.
Jan 18 23:43:19 Hacienda %LICMGR-3-LOG_LICAPP_NO_LIC: Application port-security running
without ENTERPRISE_PKG license, shutdown in 50 days
Jan 18 23:43:19 Hacienda %LICMGR-4-LOG_LICAPP_EXPIRY_WARNING: Application Roles evaluation
 license ENTERPRISE_PKG expiry in 50 days
Jan 18 23:44:54 Hacienda %BOOTVAR-5-NEIGHBOR_UPDATE_AUTOCOPY: auto-copy supported by neighbor,
 starting...

Module 1: Non-disruptive upgrading.
[#                   ]   0%Jan 18 23:44:56 Hacienda %MODULE-5-STANDBY_SUP_OK: Supervisor 5
 is standby
Jan 18 23:44:55 Hacienda %IMAGE_DNLD-SLOT1-2-IMG_DNLD_STARTED:  Module image download
process. Please wait until completion...
Jan 18 23:45:12 Hacienda %IMAGE_DNLD-SLOT1-2-IMG_DNLD_COMPLETE:  Module image download
process. Download successful.
Jan 18 23:45:48 Hacienda %MODULE-5-MOD_OK: Module 1 is online
[####################] 100% -- SUCCESS

Module 4: Non-disruptive upgrading.
[#                   ]   0%Jan 18 23:46:12 Hacienda %IMAGE_DNLD-SLOT4-2-IMG_DNLD_STARTED:
 Module image download process. Please wait until completion...
Jan 18 23:46:26 Hacienda %IMAGE_DNLD-SLOT4-2-IMG_DNLD_COMPLETE:  Module image download
process. Download successful.
Jan 18 23:47:02 Hacienda %MODULE-5-MOD_OK: Module 4 is online
[####################] 100% -- SUCCESS

Module 2: Disruptive upgrading.
...
-- SUCCESS

Module 3: Disruptive upgrading.
...
 -- SUCCESS

Install has been successful.

MDS Switch
Hacienda login:
```

The following example displays the result of the **install all** command if the system and kickstart files are specified remotely:

```
switch# install all system
scp://user@171.69.16.26/tftpboot/HKrel/qa/vegas/final/m9500-sf1ek9-mz.1.3.2a.bin kickstart
 scp://user@171.69.16.26/tftpboot/HKrel/qa/vegas/final/m9500-sf1ek9-kickstart-mz.1.3.2a.bin
For scp://user@171.69.16.26, please enter password:
For scp://user@171.69.16.26, please enter password:

Copying image from
scp://user@171.69.16.26/tftpboot/HKrel/qa/vegas/final/m9500-sf1ek9-kickstart-mz.1.3.2a.bin
 to bootflash:///m9500-sf1ek9-kickstart-mz.1.3.2a.bin.
[####################] 100% -- SUCCESS

Copying image from
scp://user@171.69.16.26/tftpboot/HKrel/qa/vegas/final/m9500-sf1ek9-mz.1.3.2a.bin to
```

```
bootflash:///m9500-sf1ek9-mz.1.3.2a.bin.
[####################] 100% -- SUCCESS

Verifying image bootflash:///m9500-sf1ek9-kickstart-mz.1.3.2a.bin
[####################] 100% -- SUCCESS

Verifying image bootflash:///m9500-sf1ek9-mz.1.3.2a.bin
[####################] 100% -- SUCCESS

Extracting "slc" version from image bootflash:///m9500-sf1ek9-mz.1.3.2a.bin.
[####################] 100% -- SUCCESS

Extracting "ips" version from image bootflash:///m9500-sf1ek9-mz.1.3.2a.bin.
[####################] 100% -- SUCCESS

Extracting "system" version from image bootflash:///m9500-sf1ek9-mz.1.3.2a.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image bootflash:///m9500-sf1ek9-kickstart-mz.1.3.2a.bin.
[####################] 100% -- SUCCESS

Extracting "loader" version from image bootflash:///m9500-sf1ek9-kickstart-mz.1.3.2a.bin.
[####################] 100% -- SUCCESS

Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes  non-disruptive       rolling
     2       yes      disruptive       rolling  Hitless upgrade is not supported
     3       yes  non-disruptive       rolling
     4       yes  non-disruptive       rolling
     5       yes  non-disruptive         reset
     6       yes  non-disruptive         reset
     7       yes  non-disruptive       rolling
     8       yes  non-disruptive       rolling
     9       yes      disruptive       rolling  Hitless upgrade is not supported

Images will be upgraded according to following table:
Module       Image       Running-Version           New-Version  Upg-Required
------  ----------  --------------------  --------------------  ------------
     1        slc                1.3(1)                1.3(2a)           yes
     1       bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no
     2        ips                1.3(1)                1.3(2a)           yes
     2       bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no
     3        slc                1.3(1)                1.3(2a)           yes
     3       bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no
     4        slc                1.3(1)                1.3(2a)           yes
     4       bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no
     5     system                1.3(1)                1.3(2a)           yes
     5   kickstart               1.3(1)                1.3(2a)           yes
     5       bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no
     5     loader                1.2(2)                 1.2(2)           no
     6     system                1.3(1)                1.3(2a)           yes
     6   kickstart               1.3(1)                1.3(2a)           yes
     6       bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no
     6     loader                1.2(2)                 1.2(2)           no
     7        slc                1.3(1)                1.3(2a)           yes
     7       bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no
     8        slc                1.3(1)                1.3(2a)           yes
     8       bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no
     9        ips                1.3(1)                1.3(2a)           yes
     9       bios      v1.1.0(10/24/03)      v1.0.8(08/07/03)            no
Do you want to continue with the installation (y/n)?  [n]
```

Command	Description
install module bios	Upgrades the supervisor or switching module BIOS.
install module loader	Upgrades the bootloader on the active or standby supervisor or modules.
show version	Displays software image version information.

install clock-module

To upgrade the EPLD images of the clock module on a Cisco MDS 9513 Switch Director, use the **install clock-module** command.

install clock-module [**epld** {**bootflash:**|**slot0:**|**volatile:**}]

Syntax Description

epld	(Optional) Installs the clock module EPLD from the EPLD image.
bootflash:	(Optional) Specifies the local URI containing EPLD image.
slot0:	(Optional) Specifies the local URI containing EPLD image.
volatile:	(Optional) Specifies the local URI containing EPLD image.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Use this command on the active supervisor to install the standby clock module EPLD from the specified EPLD image. After upgrading the clock module, power cycle the entire chassis for the change to take effect. It is not sufficient to reboot the chassis; you must turn the power off and on.

Note This command is supported only on the Cisco MDS 9513 Multilayer Switch Director.

Examples

The following example upgrades the EPLD images for the clock module:

```
switch# install clock-module epld bootflash:m9000-epld-3.0.0.278.img
Len 3031343, CS 0x58, string MDS series EPLD image, built on Fri Nov 11 01:11:09 2005
EPLD Curr Ver New Ver
------------------------------------------------------
Clock Controller 0x03 0x04
There are some newer versions of EPLDs in the image!
Do you want to continue (y/n) ? y
Proceeding to program Clock Module B.
Do you want to switchover Clock Modules after programming Clock Module B.
System Will Reset! y/n) ?n

|


Clock Module B EPLD upgrade is successful.
```

Related Commands

Command	Description
show version clock-module epld	Displays the current EPLD versions on the clock module.

install license

To program the supervisor or switching module BIOS, use the **install license** command.

install license [{**bootflash:**|**slot0:**|**volatile:**}] *file-name*

Syntax Description

bootflash:	(Optional) Specifies the source location for the license file.
slot0:	(Optional) Specifies the source location for the license file.
volatile:	(Optional) Specifies the source location for the license file.
file-name	Specifies the name of the license file.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

If a target filename is provided after the source URL, the license file is installed with that name. Otherwise, the filename in the source URL is used. This command also verifies the license file before installing it.

Examples

The following example installs a file named license-file which resides in the bootflash: directory:

```
switch# install license bootflash:license-file
```

Related Commands

Command	Description
show license	Displays license information.

install module bios

To program the supervisor or switching module BIOS, use the **install module bios** command.

install module *module-number* **bios** {**system** [{**bootflash:**|**slot0:**|**volatile:** *system-image*}]}

Syntax Description

module-number	Specifies the module number from slot 1 to 9 in a Cisco MDS 9500 Series switch. Specifies the module number from slot 1 to 2 in a Cisco MDS 9200 Series switch.
system	(Optional) Specifies the system image to use (optional). If system is not specified, the current running image is used.
bootflash:	(Optional) Specifies the source location for internal bootflash memory
slot0:	(Optional) Specifies the source location for the CompactFlash memory or PCMCIA card.
volatile:	(Optional) Specifies the source location for the volatile file system.
system-image	(Optional) Specifies the name of the system or kickstart image.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(3)	This command was introduced.

Usage Guidelines

If the BIOS is upgraded, you need to reboot to make the new BIOS effective. You can schedule the reboot at a convenient time so traffic will not be impacted.

The console baud rate automatically reverts to the default rate (9600) after any BIOS upgrade.

The URL is always the system image URL in the supervisor module, and points to the bootflash: or slot0: directories.

Examples

The following example shows how to perform a nondisruptive upgrade for the system:

```
switch# install module 1 bios
Started bios programming .... please wait
###
BIOS upgrade succeeded for module 1
```

In this example, the switching module in slot 1 was updated.

install module epld

To upgrade the electrically programmable logical devices (EPLDs) module, use the **install module epld** command. This command is only for supervisor modules, not switching modules.

install module *module-number* **epld** [{**bootflash:**|**ftp:**|**scp:**|**sftp:**|**tftp:**|**volatile:**}]

Syntax Description

module-number	Enters the number for the standby supervisor modules or any other line card.
bootflash:	(Optional) Specifies the source location for internal bootflash memory.
ftp	(Optional) Specifies the local/remote URI containing EPLD image.
scp	(Optional) Specifies the local/remote URI containing EPLD image.
sftp	(Optional) Specifies the local/remote URI containing EPLD image.
tftp	(Optional) Specifies the local/remote URI containing EPLD image.
volatile:	(Optional) Specifies the source location for the volatile file system.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

Issue this command from the active supervisor module to update any other module.

If you forcefully upgrade a module that is not online, all EPLDs are forcefully upgraded. If the module is not present in the switch, an error is returned. If the module is present, the command process continues.

Do not insert or extract any modules while an EPLD upgrade or downgrade is in progress.

Examples

The following example upgrades the EPLDs for the module in slot 2:

```
switch# install module 2 epld scp://user@10.6.16.22/users/dino/epld.img

The authenticity of host '10.6.16.22' can't be established.
RSA1 key fingerprint is 55:2e:1f:0b:18:76:24:02:c2:3b:62:dc:9b:6b:7f:b7.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.6.16.22' (RSA1) to the list of known hosts.
user@10.6.16.22's password:
epld.img             100% |****************************|  1269 KB    00:00
Module Number                                       2
EPLD                              Curr Ver     New Ver
-----------------------------------------------------
Power Manager                        0x06
XBUS IO                              0x07        0x08
```

```
UD chip Fix                          0x05
Sahara                               0x05        0x05

Module 2 will be powered down now!!
Do you want to continue (y/n) ? y
\ <-----------------------------------------------------------progress twirl
Module 2 EPLD upgrade is successful
```

The following example forcefully upgrades the EPLDs for the module in slot 2:

```
switch# install module 2 epld scp://user@10.6.16.22/epld-img-file-path

Module 2 is not online, Do you want to continue (y/n) ? y
cchetty@171.69.16.22's password:
epld.img             100% |****************************|  1269 KB    00:00
\ <-----------------------------------------------------------progress twirl
Module 2 EPLD upgrade is successful
```

Related Commands

Command	Description
show version epld	Displays the available EPLD versions.
show version module*number* **epld**	Displays the current EPLD versions.

install module loader

To upgrade the bootloader on either the active or standby supervisor module, use the **install module loader** command. This command is only for supervisor modules, not switching modules.

install module *module-number* **loader kickstart** [{**bootflash:**|**slot0:**|**volatile:***kickstart-image*}]

Syntax Description

module-number	Enters the module number for the active or standby supervisor modules (only slot 5 or 6).
kickstart	Specifies the kickstart image to use.
bootflash:	(Optional) Specifies the source location for internal bootflash memory
slot0:	(Optional) Specifies the source location for the CompactFlash memory or PCMCIA card.
volatile:	(Optional) Specifies the source location for the volatile file system.
kickstart-image	Specifies the name of the kickstart image.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(3)	This command was introduced.

Usage Guidelines

Before issuing the **install module loader** command, be sure to read the release notes to verify compatibility issues between the boot loader and the kickstart or system images.

If you install a loader version that is the same as the currently installed version, the loader will not be upgraded. When both the current version and the installed version are the same, use the **init system** command to force a loader upgrade.

Examples

The following example shows how to perform a non disruptive upgrade for the system:

```
switch# install module 6 loader bootflash:kickstart_image
```

Related Commands

Command	Description
show version	Verifies the output before and after the upgrade.

install ssi

To perform a nondisruptive upgrade of the SSI image on an SSM, use the **install ssi** command.

install ssi {**bootflash:**|**slot0:**|**modflash:**} *file-name* **module** *slot*

Syntax Description

bootflash:	Specifies the source location for the SSI boot image file.
slot0:	Specifies the source location for the SSI boot image file.
modflash:	Specifies the source location for the SSI boot image file.
file-name	Specifies the SSI boot image filename.
module *slot*	Specifies the module slot number.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
5.0(x)	This command has been deprecated (install ssi command is not supported for gen 2 card.
2.1(2)	This command was introduced.

Usage Guidelines

You can use the **install ssi** command to upgrade or downgrade the SSI boot image if the SSM is only configured for Fibre Channel switching. If your SSM is configured for VSFN or Intelligent Storage Services, you must use the **boot** command to reconfigure the SSI boot variable and reload the module.

The **install ssi** command implicitly sets the SSI boot variable.

Note The SSM must be running EPLD version 2.1(2) to use the **install ssi** command. You must install the SSM on a Cisco MDS 9500 Series switch to update the EPLD.

Note The **install ssi** command does not support files located on the SSM modflash.

Examples

The following example installs the SSI boot image on the module in slot 2:

```
switch# install ssi bootflash:lm9000-ek9-ssi-mz.2.1.2.bin module 2
```

Related Commands

Command	Description
boot	Configures the boot variables.
show boot	Displays the current contents of boot variables.
show module	Verifies the status of a module.

interface

To configure an interface on the Cisco MDS 9000 Family of switches, use the **interface** command in configuration mode.

interface {**cpp** {*module-numberprocessor-numbervsan-id*}|**ethernet** {*slot number*\ *port-number*}|**ethernet-port-channel** *ethernet-port-channel-number*|**fc** {*slot number*|**port number**|**fc-tunnel** *tunnel-id*}|**mgmt**|**port-channel** *port-channel-number*|**vfc** *vfc-id*|**vfc port-channel** *vfc port-channel-id*|**vsan** *vsan-id*}
nointerface {**cpp** {*module-numberprocessor-numbervsan-id*}|**ethernet** {*slot number*\ *port-number*}|**ethernet-port-channel** *ethernet-port-channel-number*|**fc** {*slot number*|**port number**|**fc-tunnel** *tunnel-id*}|**mgmt**|**port-channel** *port-channel-number*|**vfc** *vfc-id*|**vfc port-channel** *vfc port-channel-id*|**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:

Syntax Description

cpp	Configures a Control Plane Process (CPP) interface.
module-number	Specifies the module number. The range is 1 to 10.
processor-number	Specfies the processor number. The range is from 1 to 1.
vsan-id	Specifies the VSAN ID. The range is from 1 to 4093.
ethernet	Specfies the Ethernet IEEE 802.3z.
slot number / *port number*	Specifies the Ethernet slot number and port number. Slot range is from 1 to 253 and port number range is from 1 to 128.
ethernet-port-channel	Ethernet Port Channel interface. The range is from 513 to 4096.
ethernet-port-channel-number	Specifies the Port Channel number. The range is from 513 to 4096.
fc	(Optional) Configures a Fiber Channel interface on an MDS 9000 Family switch (see the **interface fc** command).
slot number / *port number*	Specifies the slot number. The range is from 1 to 10. Specifies the FC slot number and port number. Slot range is from 1 to 10 and port number range is from 1 to 48.
fc-tunnel	Configures a Fiber Channel link interface (see the **interface fc-tunnel** command).
tunnel-id	Specifies the tunnel ID. The range is from 1 to 255.
mgmt	Configures a management interface (see the **interface mgmt** command).

port-channel	Configures a Port Channel interface (see the **interface port-channel** command).
port-channel-number	Specifies the Port Channel number. The range is from 1 to 256.
vfc	Specifies the Virtual FC interface.
vfc-id	Specifies the virtual interface ID or slot. The range is from 1 to 8192.
vfc-port-channel	Specifies the virtual FC port-channel interface
vfc-port-channel-id	Specifies the virtual interface ID. The range is from 513 to 4096.
vsan	Specifies the IPFC VSAN interface.
vsan-id	Specfies the VSAN ID. The range is from 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(2)	This command was introduced.

Usage Guidelines

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

interface fc1/1 - 5 , fc2/5 - 7

The spaces are required before and after the dash (-) and before and after the comma (,).

Note For Cisco MDS 9500, 9700 and 9250i Series Switches support ethernet , vfc, vfc-port-channel and ethernet-port-channel commands.

Examples

The following example selects the mgmt 0 interface and enters interface configuration submode:

```
switch# config terminal
switch(config)# interface mgmt 0
```

Related Commands

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

interface fc

To configure a Fibre Channel interface on the Cisco MDS 9000 Family of switches, use the **interface fc** command in EXEC mode. To revert to defaults, use the **no** form of the command.

interface fc *slot/port* **channel-group** {*group-id* **[force]|auto**} **fcdomain rcf-reject vsan** *vsan-id*
fcsp
| fspf {**cost** *link-cost* **vsan** *vsan-id*|**ficon portnumber** *portnumber* |**dead-interval** *seconds* **vsan** *vsan-id*|**hello-interval** *seconds* **vsan** *vsan-id*|**passive vsan** *vsan-id*|**retransmit-interval** *seconds* **vsan** *vsan-id*}
nointerface fc *slot/port* **channel-group** {*group-id* **[force]|auto**} **fcdomain rcf-reject vsan** *vsan-id*
no fspf {**cost** *link-cost* **vsan** *vsan-id*|**ficon portnumber** *portnumber* |**dead-interval** *seconds* **vsan** *vsan-id*|**hello-interval** *seconds* **vsan** *vsan-id*|**passive vsan** *vsan-id*|**retransmit-interval** *seconds* **vsan** *vsan-id*}

Syntax Description

slot/*port*	Specifies a slot number and port number.
channel-group	Add to or remove chaneel group from a Port Channel.
group-id	Specifies a Port Channel group number from 1 to 128.
force	(Optional) Forcefully adds a port.
auto	Enables autocreation of Port Channels.
fcdomain	Enters the interface submode.
rcf-reject	Configures the rcf-reject flag.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
fcsp	Configures the FCSP for an interface.
fspf	Configures FSPF parameters.
cost *link-cost*	Configures FSPF link cost. The range is 1 to 30000.
ficon	Configures FICON parameters.
portnumber *portnumber*	Configures the FICON port number for this interface.
dead-interval *seconds*	Configures FSPF dead interval in seconds. The range is 2 to 65535.
hello-interval *seconds*	Configures FSPF hello-interval. The range is 1 to 65535.
passive	Enables or disables FSPF on the interface.
retransmit-interval *seconds*	Configures FSPF retransmit interface in seconds. The range is 1 to 65535.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 4.2(1)	Added fcsp keyword for the syntax description.
1.0(2)	This command was introduced.
2.0(x)	Added the **auto** option to the **channel-group** keyword.

Usage Guidelines

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

interface*space***fc1/1***space*-*space***5***space*,*space***fc2/5***space*-*space***7**

Use the **no shutdown** command to enable the interface.

The **channel-group auto** command enables autocreation of Port Channels. If autocreation of Port Channels is enabled for an interface, you must first disable this configuration before downgrading to earlier software versions or before configuring the interface in a manually configured channel group.

Examples

The following example configures ports 1 to 4 in Fibre Channel interface 9:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# int fc9/1 - 4
```

The following example enables the Fibre Channel interface:

```
switch# config terminal
switch(config)# interface fc1/1
switch(config-if)# no shutdown
```

The following example assigns the FICON port number to the selected Fibre Channel interface:

```
switch# config terminal
switch(config)# interface fc1/1
switch(config-if)# ficon portnumber 15
```

Related Commands

Command	Description
show interface	Displays an interface configuration for a specified interface.
shutdown	Disables and enables an interface.

interface fcip

To configure a Fibre Channel over IP Protocol (FCIP) interface, use the **interface fcip** command. To disable a FCIP interface, use the **no** form of the command.

interface fcip *interface_number* **bport bport-keepalives channel-group** *number* **[force] fcdomain rcf-reject vsan** *vsan-id* **ficon portnumber** *portnumber*| **fspf** {**cost** *link-cost*|**dead-interval** *seconds*|**hello-interval** *seconds*|**passive**|**retransmit-interval** *seconds*} **vsan** *vsan-id* **passive-mode peer-info ipaddr** *ip-address* [**port** *number*] **qos control** *control-value* **data** *data-value* **special-frame peer-wwn** *pwwn-id* **tcp-connections** *number* **time-stamp** [**acceptable-diff** *number*] **use-profile** *profile-id*
no interface fcip *interface_number* **bport bport-keepalives channel-group** *number* **[force] fcdomain rcf-reject vsan** *vsan-id* **ficon portnumber** *portnumber* **fspf** {**cost** *link-cost*|**dead-interval** *seconds*|**hello-interval** *seconds*|**passive**|**retransmit-interval** *seconds*} **vsan** *vsan-id* **qos** *control-value* **data** *data-value* **passive-mode peer-info ipaddr** *ip-address* [**port** *number*] **special-frame peer-wwn** *pwwn-id* **tcp-connections** *number* **time-stamp** [**acceptable-diff** *number*] **use-profile** *profile-id*

Syntax Description

interface-number	Configures the specified interface from 1 to 255.
bport	Sets the B port mode.
bport-keepalives	Sets the B port keepalive responses.
channel-group *number*	Specifies a PortChannel number from 1 to 128.
force	(Optional) Forcefully adds a port.
fcdomain	Enters the fcdomain mode for this FCIP interface
rcf-reject	Configures the rcf-reject flag.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
ficon	Configures FICON parameters.
portnumber *portnumber*	Configures the FICON port number for this interface.
fspf	Configures FSPF parameters.
cost *link-cost*	Enters FSPF link cost. The range is 1 to 30000.
dead-interval *seconds*	Specifies the dead interval in seconds. The range is 1 to 65535.
hello-interval *seconds*	Specifies FSPF hello-interval in seconds. The range is 1 to 65535.
passive	Enables or disables FSPF on the interface.
retransmit-interval	Specifies FSPF retransmit interface in seconds. The range is 1 to 65535.
passive-mode	Configures a passive connection.
peer-info	Configures the peer information.

ipaddr *ip-address*	Specifies the peer IP address.
port *number*	(Optional) Specifies the peer port number. The range is 1 to 65535.
qos	Configures the differentiated services code point (DSCP) value to mark all IP packets.
control *control-value*	Specifies the control value for DSCP.
data *data-value*	Specifies the data value for DSCP.
special-frame	Configures special frames.
peer-wwn *pwwn-id*	Specifies the peer WWN for special frames.
switchport	Configures switchport parameters.
tcp-connections *number*	Specifies the number of TCP connection attempts. Valid values are 1 or 2.
time-stamp	Configures the time stamp.
acceptable-diff *number*	(Optional) Specifies the acceptable time difference for time stamps. The range is 1 to 60000.
use-profile *profile-id*	Specifies the interface using an existing profile ID. The range is 1 to 255.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.1(1)	This command was introduced.
1.3(1)	Added the **ficon portnumber** subcommand.
2.0(x)	Added the **qos** subcommand.

Usage Guidelines

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

interface **fcip1***space-space***5***space*,*space***fcip10***space-space***12***space*

Examples

The following example selects an FCIP interface and enters interface configuration submode:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface fcip 1
switch(config-if)#
```

The following example assigns the FICON port number to the selected FCIP interface:

```
switch# config terminal
```

```
switch(config)# interface fcip 51
switch(config-if)# ficon portnumber 234
```

Related Commands

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

interface fc-tunnel

To configure a Fibre Channel tunnel and facilitate RSPAN traffic, use the **interface fc-tunnel** command. To remove a configured tunnel or revert to factory defaults, use the **no** form of the command.

interface fc-tunnel {*number* **destination** *ip-address*|**explicit-path** *path-name* **source** *ip-address*}
nointerface fc-tunnel {*number* **destination** *ip-address*|**explicit-path** *path-name* **source** *ip-address*}

Syntax Description

number	Specifies a tunnel ID range from 1 to 255.
destination *ip-address*	Maps the IP address of the destination switch.
explicit-path *path-name*	Specifies a name for the explicit path. Maximum length is 16 alphanumeric characters.
source *ip-address*	Maps the IP address of the source switch.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example initiates the FC tunnel (100) in the source switch (switch S):

```
switch(config)# config terminal
switch(config)# interface fc-tunnel 100
switch(config-if)#
```

The following example maps the IP address of the source switch (switch S) to the FC tunnel (100):

```
switchS(config-if)# source 209.165.200.226
```

The following example maps the IP address of the destination switch (switch D) to the FC tunnel (100):

```
switch(config-if)# destination 209.165.200.227
```

The following example enables traffic flow through this interface:

```
switch(config-if)# no shutdown
```

The following example references the configured path in the source switch (switch S):

```
switch# config t
```

```
switch(config)# interface fc-tunnel 100
switch(config)# explicit-path Path1
```

Related Commands

Command	Description
fc-tunnel explicit-path	Configures a new or existing next-hop path.
show interface fc-tunnel	Displays an FC tunnel interface configuration for a specified interface.

interface gigabitethernet

To configure an Gigabit Ethernet interface, use the **interface gigabitethernet** command. To revert to the default values, use the **no** form of the command.

interface gigabitethernet *slot/port* **cdp enable channel-group** *group-id* **[force] isns** *profile-name*
nointerfacegigabitethernet *slot/port* **cdp enable channel-group isns** *profile-name*

Syntax Description

slot/*port*	Specifies a slot number and port number.
cdp enable	Enables Cisco Discovery Protocol (CDP) configuration parameters.
channel-group *group-id*	Adds to or removes from a PortChannel. The range is 1 to 128.
force	(Optional) Forcefully adds a port.
isns *profile-name*	Specifies the profile name to tag the interface. Maximum length is 64 characters.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(3a)	This command was introduced.
1.1(1a)	Added the **channel-group** subcommand.
1.3(1)	Added the **isns** subcommand.

Usage Guidelines

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

interfacegigabitethernet1/1*space-space***2***space*,*space* **gigabitethernet3/1***space-space***2**

Examples

The following example configures the Gigabit Ethernet interface at slot 4 port 1:

```
switch# config terminal
switch(config)# interface gigabitethernet 4/1
switch(config-if)#
```

The following example enters a IP address and subnet mask for the selected Gigabit Ethernet interface:

```
switch(config-if)# ip address 209.165.200.226 255.255.255.0
```

The following example changes the IP maximum transmission unit (MTU) value for the selected Gigabit Ethernet interface:

```
switch(config-if)# switchport mtu 3000
```

The following example creates a VR ID for the selected Gigabit Ethernet interface, configures the virtual IP address for the VR ID (VRRP group), and assigns a priority:

```
switch(config-if)# vrrp 100
switch(config-if-vrrp)# address 209.165.200.226
switch(config-if-vrrp)# priority 10
```

The following example adds the selected Gigabit Ethernet interface to a channel group. If the channel group does not exist, it is created, and the port is shut down:

```
switch(config-if)# channel-group 10

gigabitethernet 4/1 added to port-channel 10 and disabled
please do the same operation on the switch at the other end of the port-channel, then do
"no shutdown" at both ends to bring them up.
```

Related Commands

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

interface ioa

To configure an IOA interface, use the **interface ioa** command. To disable this feature, use the **no** form of the command.

interface ioa {*slot*/*port*}
no interface ioa {*slot*/*port*}

Syntax Description

slot /port	Specifies IOA slot or port number. The range is from 1 to 16 for the slot and for the port. The range is from 1 to 4.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure an IOA interface for a specific cluster:

```
switch(config)# interface ioa2/1

2009 May 19 18:33:08 sjc-sw2 %IOA-2-LOG_LIBBASE_SVC_LICENSE_ON_GRACE_PERIOD: (pid=8582) No
 license. Feature will be shut down after a grace period of approximately 107 days

switch(config-if)# no shutdown
```

Related Commands

Command	Description
show ioa cluster summary	Displays the summary of all the IOA cluster.

interface iscsi

To configure an iSCSI interface, use the **interface iscsi** command. To revert to default values, use the **no** form of the command.

interface iscsi *slot/port* **mode** {**pass-thru|store-and-forward|cut-thru**} **tcp qos** *value*
nointerface iscsi *slot/port* **mode** {**pass-thru|store-and-forward|cut-thru**} **tcp qos** *value*

slot/port	Specifies a slot number and port number.
mode	Configures a forwarding mode.
pass-thru	Forwards one frame at a time.
store-and-forward	Forwards data in one assembled unit (default).
cut-thru	Forwards one frame at a time without waiting for the exchange to complete.
tcp qos *value*	Configures the differentiated services code point (DSCP) value to apply to all outgoing IP packets. The range is 0 to 63.

Command Default

Disabled.

The TCP QoS default is 0.

The forwarding mode default is store-and-forward.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.1(1)	Added the **cut-thru** option for the **mode** subcommand.

Usage Guidelines

To configure iSCSI interface, enable iSCSI using the **iscsi enable** command.

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

interface iscsi *space* fc1/1*space* -*space* 5*space* ,*space* fc2/5*space* -*space* 7

Examples

The following example enables the iSCSI feature:

```
switch# config t
switch(config)# iscsi enable
```

The following example enables the store-and-forward mode for iSCSI interfaces 9/1 to 9/4:

```
switch(config)# interface iscsi 9/1 - 4
switch(config-if)# mode store-and-forward
```

The following example reverts to using the default pass-thru mode for iSCSI interface 9/1:

```
switch(config)# interface iscsi 9/1
switch(config-if)# mode pass-thru
```

Related Commands

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

interface mgmt

To configure a management interface, use the **interface mgmt** command in configuration mode.

interface mgmt *number*

Syntax Description

number	Specifies the management interface number which is 0.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

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 configures the management interface, displays the options available for the configured interface, and exits to configuration mode:

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

The following example shuts down the interface without using the **force** option:

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

The following example shuts down the interface using the **force** option:

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

Related Commands

Command	Description
show interface mgmt	Displays interface configuration for specified interface.

interface port-channel

To configure a PortChannel interface, use the **interface port-channel** command. To remove this configuration, use the **no** form of the command.

interface port-channel *number* **channel mode active fcdomain rcf-reject vsan** *vsan-id* **fspf** [{**cost** *link_cost*|**dead-interval** *seconds*|**ficon portnumber** *portnumber*|**hello-interval** *seconds*|**isns** *profile-name*|**passive**|**retransmit-interval** *seconds*}]
no interface port-channel *number*

Syntax Description

number	Specifies the PortChannel number. The range is 1 to 128.
channel mode active	Configures the channel mode for the PortChannel interface.
fcdomain	Specifies the interface submode.
rcf-reject	Configures the rcf-reject flag.
vsan	Specifies the VSAN range.
vsan-id	Specifies the ID of the VSAN is from 1 to 4093.
fspf	Configures the FSPF parameters.
cost	(Optional) Configures the FSPF link cost.
link_cost	Specifies the FSPF link cost which is 1-30000.
dead-interval	(Optional) Configures the FSPF dead interval.
seconds	Specifies the dead interval (in seconds) from 2-65535.
ficon	(Optional) Configures the FICON parameters.
portnumber *portnumber*	(Optional) Configures the FICON port number for this interface.
hello-interval	(Optional) Configures FSPF hello-interval.
seconds	Specifies the hello interval (in seconds) from 1-65535.
isns	(Optional) Tags this interface to the Internet Storage Name Service (iSNS) profile.
profile-name	Specifies the profile name to tag the interface.
passive	(Optional) Enable/disable FSPF on the interface.
retransmit-interval	(Optional) Configures FSPF retransmit interface.
seconds	Specifies the retransmit interval (in seconds) from 1-65535.

Command Default

Prior to Cisco MDS NX-OS Release 8.3(1), the CLI and the Device Manager create the PortChannel in On mode in the NPIV core switches and Active mode on the NPV switches. DCNM-SAN creates all PortChannels in Active mode.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
1.3(1)	Added **channel mode active** subcommand.

Usage Guidelines

Prior to Cisco MDS NX-OS Release 8.3(1), the CLI and the Device Manager create the PortChannel in On mode in the NPIV core switches and Active mode on the NPV switches. DCNM-SAN creates all PortChannels in Active mode. We recommend that you create PortChannels in Active mode.

Examples

The following example enters configuration mode and configures a PortChannel interface:

```
switch# config terminal
switch(config)# interface port-channel 32
switch(config-if)#
```

The following example assigns the FICON port number to the selected PortChannel port:

```
switch# config terminal
switch(config)# interface Port-channel 1
switch(config-if)# ficon portnumber 234
```

Related Commands

Command	Description
show interface	Displays interface configuration for specified interface.

interface sme

To configure the Cisco SME interface on a switch, use the **interface sme** command. To remove the interface, use the **no** form of the command,

interface sme *slot* */port*
no interface sme *slot* */port*

Syntax Description

slot	Identifies the number of the MPS-18/4 module slot.
port	Identifies the number of the Cisco SME port.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

To use this command, clustering must be enabled using the **cluster enable** command and Cisco SME services must be activated using the sme enable command.

Once you have configured the interface, use the **no shutdown** command to enable the interface.

To delete the Cisco SME interface, you must first remove the switch from the cluster. Use the **no sme cluster** command to remove the switch from the cluster and then use the **no interface** command to delete the interface.

The interface commands are available in the **(config-if)** submode.

Examples

The following example configures and enables the Cisco SME interface on the MPS-18/4 module slot and the default Cisco SME port:

```
switch# config terminal
switch(config)# interface sme 3/1
switch(config-if)# no shutdown
```

Related Commands

Command	Description
show interface sme	Displays interface information.
shutdown	Enables or disables an interface.

interface sme (Cisco SME cluster node configuration submode)

To add Cisco SME interface from a local or a remote switch to a cluster, use the **interface sme** command. To delete the interface, use the **no** form of the command.

interface sme {*slot*/*port*} **[force]**
no interface sme {*slot*/*port*} **[force]**

Syntax Description

slot	Identifies the MPS-18/4 module slot.
port	Identifies the Cisco SME port.
force	(Optional) Forcibly clears the previous interface context in the interface.

Command Default

Disabled.

Command Modes

Cisco SME cluster node configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

You have to first configure a node using the **fabric-membership** command before this command can be executed.

To use this command, clustering must be enabled using the **cluster enable** command and Cisco SME services must be activated using the **sme enable** command.

To delete the Cisco SME interface, first remove the switch from the cluster. Use the **no sme cluster** command to remove the switch from the cluster and then use the **no interface** command to delete the interface.

Examples

The following example specifies the fabric to which the node belongs and then adds the Cisco SME interface (4/1) from a local switch using the force option:

```
switch# config terminal
switch(config)# sme cluster clustername1
switch(config-sme-cl)# node local
switch(config-sme-cl-node)# fabric-membership f1
switch(config-sme-cl-node)# interface sme 4/1 fabric sw-xyz
```

The following example specifies the fabric to which the node belongs and then adds the Cisco SME interface (4/1) from a remote switch using the force option:

```
switch# config terminal
switch(config)# sme cluster clustername1
switch(config-sme-cl)# node 171.71.23.33
switch(config-sme-cl-node)# fabric-membership f1
switch(config-sme-cl-node)# interface sme 4/1 fabric sw-xyz
```

Related Commands

Command	Description
fabric-membership	Adds the node to a fabric.
show interface	Displays Cisco SME interface details.

interface vsan

To configure a VSAN interface, use the **interface vsan** command. To remove a VSAN interface, use the **no** form of the command.

interface vsan *vsan-id*
no interface vsan *vsan-id*

Syntax Description

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

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example selects a VSAN interface and enters interface configuration submode:

```
switch# config terminal
switch(config)# interface vsan 1
switch(config-if)#
```

Related Commands

Command	Description
show interface	Displays interface configuration for specified interface.

ioa cluster

To configure an IOA cluster, use the **ioa cluster** command. To disable this feature, use the **no** form of the command.

ioa cluster {*cluster name*}
no ioa cluster {*cluster name*}

Syntax Description

cluster name	Specifies an IOA cluster name.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure an IOA cluster:

```
switch(config)# ioa cluster tape_vault
switch#(config-ioa-cl)#
```

Related Commands

Command	Description
show ioa cluster	Displays detailed information of all the IOA cluster.

ioa site-local

To configure an IOA site, use the **ioa site-local** command. To disable this feature, use the **no** form of the command.

ioa site-local {*site name*}
no ioa site-local {*site name*}

Syntax Description

site name	Specifies an IOA site name. The maximum name length is restricted to 31 alphabetical characters.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure an IOA local site:

```
switch# config t
switch(config)# ioa site-local SJC
switch#(config)#
```

Related Commands

Command	Description
ioa enable	Enables or disables the I/O Accelerator.

ioa-ping

To validate the connectivity between the master switch and the specified target device (for a specific flow), use the **ioa-ping** command.

ioa-ping host *hpwwn* **target** *tpwwn* **vsan** *vid* **interface** *if0*

Syntax Description

host	Specifies the host address.
hpwwn	Specifies the host PWWN for the flow.
target	Specifies the target address.
tpwwn	Specifies the target PWWN for the flow.
vsan	Specifies the VSAN.
vid	Specifies the VSAN ID. The range is from 1 to 4093.
interface	Specifies the interface associated with the flow.
if0	Specifies the ioa interface for the flow over which the test unit ready commands will be sent.

Command Default

Prompts for user input.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 6.2(5)	This command was introduced.

Usage Guidelines

None.

Note **ioa-ping** will work from 6.2(5) onwards and the command has to be executed from IOA master switch only.

Examples

The following example shows how to validate the connectivity between the master switch and the specified target device:

```
switch# ioa-ping host 10:00:00:00:11:a1:01:0a target 50:0a:09:80:11:4b:01:0a vsan 11 interface
 ioa 1/1

1: Round Trip Time  inf msec Device status 0
2: Round Trip Time  inf msec Device status 0
3: Round Trip Time  inf msec Device status 0
4: Round Trip Time  inf msec Device status 0
5: Round Trip Time  inf msec Device status 0
```

```
5 transmitted, 5 received ,rtt min/avg/max =  inf/ inf/ inf (msec)
switch#
```

Related Commands

Command	Description
show ioa cluster	Displays detailed information of all the IOA cluster.

ip access-group

To apply an access list to an interface, use the **ip access-group** command in interface mode. Use the **no** form of this command to negate a previously issued command or revert to factory defaults.

ip access-group *access-list-name* [{**in**|**out**}]

Syntax Description

access-list-name	Specifies the IP access list name. The maximum length is 64 alphanumeric characters and the text is case insensitive.
in	(Optional) Specifies that the group is for ingress traffic.
out	(Optional) Specifies that the group is for egress traffic.

Command Default

The access list is applied to both ingress and egress traffic.

Command Modes

Interface mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

The **ip access-group** command controls access to an interface. Each interface can only be associated with one access list. The access group becomes active immediately.

We recommend creating all rules in an access list, before creating the access group that uses that access list.

If you create an access group before an access list, the access list is created and all packets in that interface are dropped, because the access list is empty.

The access-group configuration for the ingress traffic applies to both local and remote traffic. The access-group configuration for the egress traffic applies only to local traffic. You can apply a different access list for each type of traffic.

Examples

The following example creates an access group called aclPermit for both the ingress and egress traffic (default):

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list aclPermit permit ip any any
switch(config)# interface Gigabitethernet 3/1
switch(config-if)# ip access-group aclPermit
```

The following example deletes the access group called aclPermit:

```
switch(config-if)# no ip access-group aclPermit
```

The following example creates an access group called aclDenyTcp (if it does not already exist) for ingress traffic:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list aclDenyTcp deny tcp any any
switch(config)# interface gigabitethernet 3/1
switch(config-if)# ip access-group aclDenyTcp in
```

The following example deletes the access group called aclDenyTcp for ingress traffic:

```
switch(config-if)# no ip access-group aclDenyTcp in
```

The following example creates an access list called aclPermitUdp (if it does not already exist) for local egress traffic:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list aclPermitUdp permit udp 192.168.32.0 0.0.7.255 any
switch(config)# interface gigabitethernet 3/1
switch(config-if)# ip access-group aclPermitUdp out
```

The following example removes the access list called aclPermitUdp for local egress traffic:

```
switch(config-if)# no ip access-group aclPermitUdp out
```

Related Commands

Command	Description
ip access-list	Configures IP access control lists.
show ip access-list	Displays the IP-ACL configuration information.

ip access-list

To configure IPv4 access control lists (ACLs), use the **ip access-list** command. To remove the configuration, use the **no** form of this command.

ip access-list *name* {**permit** | **deny**} {**icmp** | **ip** | **tcp** |[**flags** {{**[ack]**} {**[fin]**} {**[psh]**} {**[rst]**} {**[syn]**} {**[urg]**} | **all**}]| **udp** | *protocol-num*} {**any** |*src-ip src-mask*} [{**eq port** {{**dns** | **ftp** | **ftp-data** | **http** | **ntp** | **radius** | **sftp** | **smtp** | **snmp** | **snmp-trap** | **ssh** | **syslog** | **tacacs-ds** | **tacacs-plus** | **telnet** | **tftp** | **www** | **wbem-http** | **wbem-https**} | *src-port-num*} | **gt port** *src-port-num-low* | **lt port** *src-port-num-high* | **range port** *src-port-num-low src-port-num-high*}] {**any2** | *dst-ip dst-mask*} [{**eq2 port2** {{**dst_dns** | **dst_ftp** | **dst_ftp-data** | **dst_http** | **dst_ntp** | **dst_radius** | **dst_sftp** | **dst_smtp** | **dst_snmp** | **dst_snmp-trap** | **dst_ssh** | **dst_syslog** | **dst_tacacs-ds** | **dst_tacacs-plus** | **dst_telnet** | **dst_tftp** | **dst_www** | **dst_wbem-http** | **dst_wbem-https**} *dst-port-num*} |**gt2 port2** *dst-port-num-low* | **lt2 port2** *dst-port-num-high* | **range2 port2** *dst-port-num-low dst-port-num-high*}] [{**established** | **icmp-type** {{**echo** | **echo-reply** | **redirect** | **time-exceeded** | **unreachable** | **traceroute**} | *icmp-msg-num*} [**icmp-code** *icmp-code-num*] | **icmp-type traceroute**}] [**tos** {**delay** | **throughput** | **reliability** | **monetary-cost** | **normal-service**}] **[log-deny]**
no ip access-list *name* {**permit** | **deny**} {**icmp** | **ip** | **tcp** |[**flags** {{**[ack]**} {**[fin]**} {**[psh]**} {**[rst]**} {**[syn]**} {**[urg]**} | **all**}] | **udp** | *protocol-num*} {**any** |*src-ip src-mask*} [{**eq port** {{**dns** | **ftp** | **ftp-data** | **http** | **ntp** | **radius** | **sftp** | **smtp** | **snmp** | **snmp-trap** | **ssh** | **syslog** | **tacacs-ds** | **tacacs-plus** | **telnet** | **tftp** | **www** | **wbem-http** | **wbem-https**} | *src-port-num*} | **gt port** *src-port-num-low* | **lt port** *src-port-num-high* | **range port** *src-port-num-low src-port-num-high*}] {**any2** |*dst-ip dst-mask*} [{**eq2 port2** {{**dst_dns** | **dst_ftp** | **dst_ftp-data** | **dst_http** | **dst_ntp** | **dst_radius** | **dst_sftp** | **dst_smtp** | **dst_snmp** | **dst_snmp-trap** | **dst_ssh** | **dst_syslog** | **dst_tacacs-ds** | **dst_tacacs-plus** | **dst_telnet** | **dst_tftp** | **dst_www** | **dst_wbem-http** | **dst_wbem-https** } *dst-port-num*} | **gt2 port2** *dst-port-num-low* | **lt2 port2** *dst-port-num-high* | **range2 port2** *dst-port-num-low dst-port-num-high*}] [{**established** | **icmp-type** {{**echo** | **echo-reply** | **redirect** | **time-exceeded** | **unreachable** | **traceroute**} | *icmp-msg-num*} [**icmp-code** *icmp-code-num*] | **icmp-type traceroute**}] [**tos** {**delay** | **throughput** | **reliability** | **monetary-cost** | **normal-service**}] **[log-deny]**

Syntax Description

name	Specifies an access list name. The maximum length is 28 alphanumeric characters.
deny	Denies access if the conditions match.
permit	Allows access if the conditions match.

ip-protocol	Specifies the name or number (integer range from 0 to 255) of an IP protocol. The IP protocol name can be **icmp**, **ip**, **tcp**, or **udp**. The following TCP flags options are available: • ack • all • any • fin • psh • rst • syn • urg
source-address	Specifies the network from which the packet is sent. There are two ways to specify the source address: • IPv4 address • The **any** keyword used as an abbreviation for the source address 0.0.0.0 and source-wildcard address 255.255.255.255
source-wildcard	Applies the wildcard bits to the source address.
destination-address	Specifies the network to which the packet is to be sent. You can specify the destination using the following options: • IPv4 address • The **any** keyword used as an abbreviation for the source address 0.0.0.0 and source-wildcard address 255.255.255.255 • The **eq** keyword compares equal source ports. • The **gt** keyword compares ports that are greater than and including source ports. • The **lt** keyword compares ports that are less than and including source ports. • The **range** keyword compares a range of source ports.
destination-wildcard	Applies the wildcard bits to the destination address.

operator	Compares source or destination ports to the packet and has the following options: • **any** = Any destination IP • **eq** = Equal source port • **gt** = Greater than and including source port • **lt** = Less than and including source port • **range** = Source port range port-value
port *port-value*	Specifies the decimal number (ranging from 0 to 65535) or one of the following names to indicate a TCP or UDP port. • TCP port names—dns, ftp, ftp-data, http, ntp, radius, sftp, smtp, snmp, snmp-trap, ssh, syslog, tacacs-ds, tacacs-plus, telnet, tftp, wbem-http, wbem-https, and www. • UDP port names—dns, ftp, ftp-data, http, ntp, radius, sftp, smtp, snmp, snmp-trap, ssh, syslog, tacacs-ds, tacacs-plus, telnet, tftp, wbem-http, wbem-https, and www.
icmp-type *icmp-value*	(Optional) Filters ICMP packets by ICMP message type. The range is 0 to 255. The ICMP types include echo (8), echo-reply (0), redirect (5), time-exceeded (11), traceroute (30), and unreachable (3).
established	(Optional) Indicates an established connection for the TCP protocol. A match occurs if the TCP datagram has the ACK, FIN, PSH, RST, SYN, or URG control bits set. The non-matching case is that of the initial TCP datagram to form a connection.
tos *tos-value*	(Optional) Filters packets by the following type of service level: normal-service (0), monetary-cost (1), reliability (2), throughput (4), and delay (8).
log-deny	(Optional) Sends an information logging message to the console about the packet that is denied entries.

Command Default

IP access list is not configured.

Command Modes

Configuration mode (config)

Command History

Release	Modification
4.1(1b)	Added a note information for the usage section.
1.2(1)	This command was introduced.

Usage Guidelines

Using the **log-deny** option at the end of the individual ACL entries shows the ACL number and whether the packet was permitted or denied, in addition to port-specific information. This option causes an information logging message about the packet that matches the dropped entry (or entries).

Table 2: Unsupported Keywords in Protocols

Protocol	Unsupported Keywords
IP	**eq port**, **established**, **gt**, **lt**, **range**, **icmp-type**, and **log-deny**
ICMP	**eq port**, **established**, **gt**, **lt**, and **range**
UPD	**established**, **icmp-type**, and **log-deny**
TCP	**icmp-type** and **log-deny**

Examples

The following example configures an IP-ACL called aclPermit and permits IP traffic from any source address to any destination address:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list aclPermit permit ip any any
```

The following example removes the IP-ACL called aclPermit:

```
switch(config-if)# no ip access-group aclPermit
```

The following example updates that are aclPermit to deny TCP traffic from any source address to any destination address:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list aclPermit deny tcp any any
```

The following example defines an IP-ACL that permits this network. Subtracting 255.255.248.0 (normal mask) from 255.255.255.255 yields 0.0.7.255:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list aclPermitUdp permit udp 192.168.32.0 0.0.7.255 any
```

The following example permits all IP traffic from and to the specified networks:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip access-list aclPermitIpToServer permit ip 10.1.1.0 0.0.0.255 172.16.1.0
 0.0.0.255
```

The following example denies TCP traffic from 1.2.3.0 through source port 5 to any destination:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/
switch(config)# ip access-list aclDenyTcpIpPrt5 deny tcp 1.2.3.0 0.0.0.255 eq port 5 any
```

The following example removes this entry from the IP-ACL:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/
```

```
switch(config)# no ip access-list aclDenyTcpIpPrt5 deny tcp 1.2.3.0 0.0.0.255 eq port 5 any
```

Related Commands

Command	Description
show ip access-list	Displays the IP ACL configuration information.

ip address (FCIP profile configuration submode)

To assign the local IP address of a Gigabit Ethernet interface to the FCIP profile, use the **ip address** command. To remove the IP address, use the **no** form of the command.

ip address *address*
no ip address *address*

Syntax Description

address	Specifies the IP address.

Command Default

Disabled.

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

To create a FCIP profile, you must assign a local IP address of a Gigabit Ethernet interface to the FCIP profile.

Examples

The following example assigns the local IP address of a Gigabit Ethernet interface to the FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)# ip address 209.165.200.226
```

Related Commands

Command	Description
interface fcip interface_number use-profile profile-id	Configures the interface using an existing profile ID from 1 to 255.
show fcip profile	Displays information about the FCIP profile.

ip address (interface configuration)

To assign an IP address to a Gigabit Ethernet interface, use the **ip address** command in interface configuration submode. To remove the IP address, us the **no** form of the command.

ip address *address netmask*
no ip address *address netmask*

Syntax Description

address	Specifies the IP address.
netmask	Specifies the network mask.

Command Default

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example assigns an IP address to a Gigabit Ethernet interface:

```
switch# config terminal
switch(config)# interface gigabitethernet 1/2
switch(config-profile)# ip address 10.5.1.1 255.255.0.0
```

Related Commands

Command	Description
interface fcip interface_number use-profile profile-id	Configures the interface using an existing profile ID from 1 to 255.
show fcip profile	Displays information about the FCIP profile.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

ip default-gateway

To configure the IP address of the default gateway, use the **ip default-gateway** command. To disable the IP address of the default gateway, use the **no** form of the command.

ip default-gateway *destination-ip-address* [**interface cpp** *slot_number/processor-number/vsan-id*]
no ip default-gateway *destination-ip-address* [**interface cpp** *slot_number/processor-number/vsan-id*]

Syntax Description

destination-ip-address	Specifies the IP address,
interface	(Optional) Configures an interface.
cpp	(Optional) Specifies a virtualization IPFC interface.
slot	(Optional) Specifies a slot number of the ASM.
processor-number	(Optional) Specifies the processor number for the IPFC interface. The current processor number is always 1.
vsan-id	(Optional) Specifies the ID of the management VSAN. The range 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures the IP default gateway to 1.1.1.4:

```
switch# config terminal
switch(config)# ip default-gateway 1.1.1.4
```

Related Commands

Command	Description
show ip route	Displays the IP address of the default gateway.

ip default-network

To configure the IP address of the default network, use the **ip default-network** command in configuration mode. To disable the IP address of the default network, use the **no** form of the command.

ip default-network *ip-address*
no ip default-network *ip-address*

Syntax Description

ip-address	Specifies the IP address of the default network.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures the IP address of the default network to 1.1.1.4:

```
switch# config terminal
switch(config)# ip default-network 209.165.200.226
switch(config)# ip default-gateway 209.165.200.227
```

Related Commands

Command	Description
show ip route	Displays the IP address of the default gateway.

ip domain-list

To configure or un-configure one or more domain names, use the **ip domain-list** command in configuration mode. To disable the IP domain list, use the **no** form of the command.

ip domain-list *domain-name*
no ip domain-list *domain-name*

Syntax Description

domain-name	Specifies the domain name for the IP domain list. Maximum length is 80 characters.

Command Default

If there is a domain list, the default domain name is not used.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

When “ping dino” is initiated, IP stack will append dino.cisco.com (whatever configured in domain-name) first for Name resolution. If that doesn’t succeed, it will try with domain-list.

Note If there is no domain list, the domain name that you specified with the **ip domain-name** global configuration command is used. More than one "**ip domain-list** "command can be entered and they will be tried in order.

Examples

The following example configures the IP domain list:

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

Related Commands

Command	Description
ip domain-lookup	Enables the DNS hostname to address translation.
ip name-server	Configures a list of name servers.
show ip route	Displays the IP address of the default gateway.

ip domain-lookup

To enable the DNS hostname to address translation, use the **ip domain-lookup** command in configuration mode. Use the **no** form of this command to disable this feature.

ip domain-lookup
no ip domain-lookup

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Instead of IP addresses, you can configure the switch using meaningful names. When names are configured the switch automatically looks up the name to get its corresponding IP address.

Note In addition to **ip domain-lookup**, other commands need to be entered as well such as "**ip name-server**" and optionally, "**ip domain-name**" and "**ip domain-list**".

Examples

The following example configures a DNS server lookup feature:

```
switch# config terminal
switch(config)# ip domain-lookup
```

Related Commands

Command	Description
show ip route	Displays the IP address of the default gateway.
ip name-server	Configures a list of name servers.

ip domain-name

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

ip domain-name *domain-name*
no ip domain-name *domain-name*

Syntax Description

domain-name	Specifies the domain name.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

When "**ping dino**" is initiated, IP stack will append dino.cisco.com (whatever configured in domain-name) first for name resolution. If that doesn't succeed, it will try with **domain-list**.

Examples

The following example configures a domain name:

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

Related Commands

Command	Description
ip-name server	Configures one or more IP name servers.
ip domain-list	Configure or un-configure one or more domain names.
ip domain-lookup	Enables the DNS hostname to address translation.
show ip route	Displays the IP address of the default gateway.

ip name-server

To configure one or more IP name servers, use the **ip name-server** command in configuration mode. To disable this feature, use the **no** form of the command.

ip name-server *ip-address*
no ip name-server *ip-address*

Syntax Description

ip-address	Specifies the IP address for the name server.

Command Default

The default is no name servers are configured and no IP name resolution is performed.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can configures a maximum of six servers. By default, no server is configured.

Examples

The following example configure a name server with an IP address of 209.165.200.226:

```
switch# config terminal
switch(config)# ip name-server 209.165.200.226
```

The following example specifies the first address (209.165.200.226) as the primary server and the second address (209.165.200.227) as the secondary sever:

```
switch(config)# ip name-server 209.165.200.226 209.165.200.227
```

The following example deletes the configured server(s) and reverts to factory default:

```
switch(config)# no ip name-server
```

Related Commands

Command	Description
ip domain-lookup	Enables the DNS hostname to address translation.
ip domain-list	Configure or un-configure one or more domain names.
ip name-server	Configures one or more IP name servers.
show ip route	Displays the IP address of the default gateway.

ip route

To configure a static route, use the **ip route** command in configuration mode.

ip route *ip-address subnet-mask* [*nexthop_ip-address*] [{**interface** {**gigabitethernet** *slot /port*|**mgmt 0**|**port-channel** *channel-id*|**vsan** *vsan-id*}|**distance** *distance-number*}]
no ip route *ip-address subnet-mask* [*nexthop_ip-address*] [{**interface** {**gigabitethernet** *slot /port*|**mgmt 0**|**port-channel** *channel-id*|**vsan** *vsan-id*}|**distance** *distance-number*}]

Syntax Description

ip-address	Specifies the IP address for the route.
subnet-mask	Specifies the subnet mask for the route.
nexthop_ip-address	(Optional) Specifies the IP address of the next hop switch.
interface	(Optional) Configures the interface associated with the route.
gigabitethernet *slot /port*	Specifies a Gigabit Ethernet interface at a port and slot.
mgmt 0	Specifies the managment interface (mgmt 0).
port-channel *channel-id*	Specifies a PortChannel interface. The range is 1 to 128.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
distance *distance-number*	(Optional) Specifies the distance metric for this route. It can be from 0 to 32766.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure a static route:

```
switch# config terminal
switch(config)# IP route 10.0.0.0 255.0.0.0 20.20.20.10 distance 10 interface vsan 1
```

Related Commands

Command	Description
show ip route	Displays the IP address routes configured in the system.

ip routing

To enable the IP forwarding feature, use the **ip routing** command in configuration mode. To disable this feature, use the **no** form of the command.

ip routing
no ip routing

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example enables the IP forwarding feature:

```
switch# config terminal
switch(config)# ip routing
```

Related Commands

Command	Description
show ip routing	Displays the IP routing state.

ip-compression

To enable compression on the FCIP link, use the **ip-compression** command in interface configuration submode. To disable compression, use the **no** form of the command.

ip-compression [{**auto**|**mode1**|**mode2**|**mode3**}]
no ip-compression [{**auto**|**mode1**|**mode2**|**mode3**}]

Syntax Description

auto	(Optional) Enables the automatic compression setting.
mode1	(Optional) Enables fast compression for the following high bandwidth links: PS-4 and IPS-8, less then 100 Mbps MPS-14/2, up to 1 Gbps
mode2	(Optional) Enables moderate compression for medium bandwidth links less than 25 Mbps.
mode3	(Optional) Enables compression for bandwidth links less than 10 Mbps.

Command Default

Disabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(x)	Changed the keywords from **high-throughput** and **high-comp-ratio** to **mode1**, **mode2**, and **mode3**.

Usage Guidelines

When no compression mode is entered in the command, the default is **auto**.

The FCIP compression feature introduced in Cisco SAN-OS Release 1.3 allows IP packets to be compressed on the FCIP link if this feature is enabled on that link. By default the FCIP compression is disabled. When enabled, the software defaults to using the auto mode (if a mode is not specified).

With Cisco SAN-OS Release 2.0(1b) and later, you can configure FCIP compression using one of the following modes:

- **mode1** is a fast compression mode for high bandwidth links (> 25 Mbps).
- **mode2** is a moderate compression mode for moderately low bandwidth links (between 10 and 25 Mbps).
- **mode3** is a high compression mode for low bandwidth links (< 10 Mbps).
- **auto** (default) mode determines the appropriate compression scheme based on the bandwidth of the link (the bandwidth of the link configured in the FCIP profile's TCP parameters).

The IP compression feature behavior differs between the IPS module(s) and the MPS-14/2 module. While **mode2** and **mode3** perform software compression in both modules, **mode1** performs hardware-based compression in MPS-14/2 modules, and software compression in IPS-4 and IPS-8 modules.

In Cisco MDS SAN-OS Release 2.1(1a) and later, the **auto** mode option uses a combination of compression modes to effectively utilize the WAN bandwidth. The compression modes change dynamically to maximize the WAN bandwidth utilization.

Examples

The following example enables faster compression:

```
switch# config terminal
switch(config) interface fcip 1
switch(config-if)# ip-compression mode1
```

The following example enables automatic compression by default:

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

The following example disables compression:

```
switch(config-if)# no ip-compression
```

Related Commands

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

ips netsim delay-ms

To delay packets that arrive at a specified Gigabit Ethernet interface specifying milliseconds, use the **ips netsim delay** command in SAN extension tuner configuration submode.

ips netsim delay-ms *milliseconds* **ingress gigabitethernet** *slot*/*port*

Syntax Description

milliseconds	Specifies the delay in milliseconds. The range is 0 to 150.
ingress	Specifies the ingress direction.
gigabitethernet*slot*/*port*	Specifies the the slot and port number of the Gigabit Ethernet interface.

Command Default

Disabled.

Command Modes

SAN extension tuner configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the IP Network Simulator using the **ips netsim enable** command.

This command introduces a delay for all packets entering the Gigabit Ethernet interface. Delay is unidirectional. To introduce delay in the opposite direction, use the slot and port number of the adjacent interface.

Examples

The following example shows how to configure a delay of 50 milliseconds for packets entering Gigabit Ethernet interface 2/3:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
switch(config)# exit
switch#
switch# ips netsim delay-ms 50 ingress gigabitethernet 2/3
```

Related Commands

Command	Description
show ips netsim	Displays a summary of the interfaces that are currently operating in network simulation mode.
ips netsim enable	Enables the IP Network Simulator.

ips netsim delay-us

To delay packets that arrive at a specified Gigabit Ethernet interface specifying microseconds, use the **ips netsim delay** command in SAN extension tuner configuration submode.

ipsnetsimdelay-us*microseconds***ingressgigabitethernet***slot*/*port*

Syntax Description

microseconds	Specifies the delay in microseconds. The range is 0 to 150000.
ingress	Specifies the ingress direction.
gigabitethernet*slot*/*port*	Specifies the the slot and port number of the Gigabit Ethernet interface.

Command Default

Disabled.

Command Modes

SAN extension tuner configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the IP Network Simulator using the **ips netsim enable** command.

This command introduces a delay for all packets entering the Gigabit Ethernet interface. Delay is unidirectional. To introduce delay in the opposite direction, use the slot and port number of the adjacent interface.

Examples

The following example shows how to configure a delay of 50 microseconds for packets entering Gigabit Ethernet interface 2/3:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
switch(config)# exit
switch#
switch# ips netsim delay-us 50 ingress gigabitethernet 2/3
```

Related Commands

Command	Description
ips netsim enable	Enables the IP Network Simulator.
show ips netsim	Displays a summary of the interfaces that are currently operating in network simulation mode.

ips netsim drop nth

To drop packets every nth packet at a specified Gigabit Ethernet interface, use the **ips netsim drop nth** command in SAN extension tuner configuration submode.

ips netsim drop nth *packet* {**burst** *burst-size* **ingress gigabitethernet** *slot*/*port*|**ingress gigabitethernet** *slot*/*port*}

Syntax Description

packet	Specifies a specific packet to drop. The range is 0 to 10,000.
burst *burst-size*	Specifies the packet burst size. The range is 1 to 100.
ingress	Specifies the ingress direction.
gigabitethernet*slot*/ *port*	Specifies the the slot and port number of the Gigabit Ethernet interface.

Command Default

Disabled.

Command Modes

SAN extension tuner configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the IP Network Simulator using the **ips netsim enable** command.

You can configure the IP Network Simulator to simulate packet drops (even when the queue is not full) randomly (specified as a percentage) or every Nth packet. Percentage is represented as the number of packets in 10,000. For example, if you want to drop one percent of packets, then specify it as 100 packets in 10,000. To simulate a realistic scenario for IP networks using random drops, the drop percentage should be between zero and one percent of packet drops in the specified traffic direction.

If you use the optional burst parameter, then a specified number of packets are dropped. If you do not specify the burst parameter, then only one packet is dropped. The burst limit for either random or Nth drops is 1 to 100 packets. Take the burst parameter into account when specifying the percentage of packets dropped. For example, if you select a random drop of 100 packets in 10,000 (or one percent) with a burst of 2, 200 packets (or two percent) in every 10,000 packets are dropped. Specifying 2 for burst doubles the packet drop.

Examples

The following example shows how to configure an interface to drop every 100th packet, 2 packets at a time:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
switch(config)# exit
switch#
switch# ips netsim drop nth 100 burst 2 ingress gigabitethernet 2/3
```

Related Commands

Command	Description
ips netsim enable	Enables the IP Network Simulator.
show ips netsim	Displays a summary of the interfaces that are currently operating in network simulation mode.

ips netsim drop random

To drop packets randomly at a specified Gigabit Ethernet interface, use the **ips netsim drop random** command in SAN extension tuner configuration submode.

ips netsim drop random *packet-percentage* {**burst** *burst-size* **ingress gigabitethernet** *slot*/*port*|**ingress gigabitethernet** *slot*/*port*}

Syntax Description

packet-percentage	Specifies the percentage of packets dropped. The range is 0 to 10000.
burst *burst-size*	Specifies the packet burst size. The range is 1 to 100.
ingress	Specifies the ingress direction.
gigabitethernet*slot /port*	Specifies the the slot and port number of the Gigabit Ethernet interface.

Command Default

Disabled.

Command Modes

SAN extension tuner configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the IP Network Simulator using the **ips netsim enable** command.

You can configure the IP Network Simulator to simulate packet drops (even when the queue is not full) randomly (specified as a percentage) or every Nth packet. Percentage is represented as the number of packets in 10,000. For example, if you want to drop one percent of packets, then specify it as 100 packets in 10,000. To simulate a realistic scenario for IP networks using random drops, the drop percentage should be between zero and one percent of packet drops in the specified traffic direction.

If you use the optional burst parameter, then a specified number of packets are dropped. If you do not specify the burst parameter, then only one packet is dropped. The burst limit for either random or Nth drops is 1 to 100 packets. Take the burst parameter into account when specifying the percentage of packets dropped. For example, if you select a random drop of 100 packets in 10,000 (or one percent) with a burst of 2, 200 packets (or two percent) in every 10,000 packets are dropped. Specifying 2 for burst doubles the packet drop.

Examples

The following example shows how to configure an interface to drop one percent of packets:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
switch(config)# exit
switch#
switch# ips netsim drop random 100 burst 1 ingress gigabitethernet 2/3
```

Related Commands

Command	Description
show ips netsim	Displays a summary of the interfaces that are currently operating in network simulation mode.
ips netsim enable	Enables the IP Network Simulator.

ips netsim enable

To enable two Gigabit Ethernet interfaces to operate in the network simulation mode, enter the **ips netsim enable** command in SAN extension tuner configuration submode. To disable this feature, use the **no** form of the command.

ips netsim enable interface gigabitethernet *slot/port* **gigabitethernet** *slot/port*
no ips netsim enable interface gigabitethernet *slot/port* **gigabitethernet** *slot/port*

Syntax Description

interface	Specifies that interfaces are enabled.
gigabitethernet*slot/port*	Specifies the the slot and port number of the Gigabit Ethernet interface.

Command Default

Disabled.

Command Modes

SAN extension tuner configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This command enables two Gigabit Ethernet interfaces to simulate network characteristics. The first interface specified is the ingress port and the second interface specified is the egress port. Ports must be adjacent and the ingress interface must be an odd-numbered port.

Interfaces configured with this command can no longer be used for FCIP or iSCSI. When the SAN extension tuner configuration submode is turned off, any interface configured for network simulation reverts back to normal operation.

Examples

The following example enables the IP Network Simulator and configures interfaces 2/3 and 2/4 for network simulation:

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

Related Commands

Command	Description
show ips netsim	Displays a summary of the interfaces that are currently operating in network simulation mode.

ips netsim max-bandwidth-kbps

To limit the bandwidth in kilobytes per second of a specified Gigabit Ethernet interface, use the **ips netsim max-bandwidth-kbps** command in SAN extension tuner configuration submode.

ips netsim max-bandwidth-kbps *bandwidth* **ingress gigabitethernet** *slot/port*

Syntax Description

bandwidth	Specifies the bandwidth in kilobytes per second. The range is 1000 to 1000000.
ingress	Specifies the ingress direction.
gigabitethernet*slot/port*	Specifies the the slot and port number of the Gigabit Ethernet interface.

Command Default

Disabled.

Command Modes

SAN extension tuner configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the IP Network Simulator using the **ips netsim enable** command.

Examples

The following example shows how to limit the interface bandwidth to 4500 Kbps:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
switch(config)# exit
switch#
switch# ips netsim max-bandwidth-kbps 4500 ingress gigabitethernet 2/3
```

Related Commands

Command	Description
ips netsim enable	Enables the IP Network Simulator.
show ips netsim	Displays a summary of the interfaces that are currently operating in network simulation mode.

ips netsim max-bandwidth-mbps

To limit the bandwidth in megabytes per second of a specified Gigabit Ethernet interface, use the **ips netsim max-bandwidth-mbps** command in SAN extension tuner configuration submode.

ips netsim max-bandwidth-mbps *bandwidth* **ingress gigabitethernet** *slot/port*

Syntax Description

bandwidth	Specifies the bandwidth in megabytes per second. The range is 1 to 1000.
ingress	Specifies the ingress direction.
gigabitethernet*slot/port*	Specifies the the slot and port number of the Gigabit Ethernet interface.

Command Default

Disabled.

Command Modes

SAN extension tuner configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the IP Network Simulator using the **ips netsim enable** command.

Examples

The following example shows how to limit the interface bandwidth to 45 Mbps:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
switch(config)# exit
switch#
switch# ips netsim max-bandwidth-mbps 45 ingress gigabitethernet 2/3
```

Related Commands

Command	Description
ips netsim enable	Enables the IP Network Simulator.
show ips netsim	Displays a summary of the interfaces that are currently operating in network simulation mode.

ips netsim qsize

To limit the size of the queue on a specified Gigabit Ethernet interface, use the **ips netsim qsize** command in SAN extension tuner configuration submode.

ips netsim qsize *queue-size* **ingress gigabitethernet** *slot/port*

Syntax Description

queue-size	Specifies the queue size. The range is 0 to 1000000.
ingress	Specifies the ingress direction.
gigabitethernet*slot /port*	Specifies the the slot and port number of the Gigabit Ethernet interface.

Command Default

Disabled.

Command Modes

SAN extension tuner configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the IP Network Simulator using the **ips netsim enable** command.

This command rate limits the size of the queue on a specified Gigabit Ethernet port. The recommended queue size for network simulation is 50000 to 150000. If the queue becomes full, packets are dropped.

Examples

The following example shows how to limit the queue size to 75 KB:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
switch(config)# exit
switch#
switch# ips netsim qsize 75 ingress gigabitethernet 2/3
```

Related Commands

Command	Description
ips netsim enable	Enables the IP Network Simulator.
show ips netsim	Displays a summary of the interfaces that are currently operating in network simulation mode.

ips netsim reorder

To reorder packets entering a specified Gigabit Ethernet interface, use the **ips netsim reorder** command in SAN extension tuner configuration submode.

ipsnetsimreorder{**nth** *packet***distance** *dist-packet* **ingress gigabitethernet***slot*/*port*|**nth** *packet* **ingress gigabitethernet***slot*/*port*}
|{**random** *percent* **distance** *dist-packet* **ingress gigabitethernet** *slot*/*port*
|**random** *percent* **ingress gigabitethernet** *slot*/*port*}

Syntax Description

nth *packet*	Specifies a specific packet reordered. The range is 0 to 10,000.
distance *dist-packet*	Specifies the distance between the packet to be reordered and the packet at the head of the queue. The range is 1 to 10.
ingress	Specifies the ingress direction.
gigabitethernet*slot*/*port*	Specifies the the slot and port number of the Gigabit Ethernet interface.
random percent	Specifies the percentage of packets passed before a reorder. The range is 0 to 10,000.

Command Default

Disabled.

Command Modes

SAN extension tuner configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

To use this command, you must enable the IP Network Simulator using the **ips netsim enable** command.

You can configure network simulator to reorder packets (even when the queue is not full) randomly (specified as a percentage) or every Nth packet. Percentage is represented as the number of packets in 10,000. For example, if you want to reorder one percent of packets, then specify it as 100 packets in 10,000. To simulate a realistic scenario for IP networks using random reordering, the percentage should be between zero and one percent of packet reordered in the specified traffic direction.

If you use the optional burst parameter, then the specified number of packets will be reordered. If you do not specify the burst parameter, then only one packet is reordered.

Examples

The following example shows reordering at 50 percent with a distance limit of 5:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
```

```
switch(config)# exit
switch#
switch# ips netsim reorder random 50 distance 5 ingress gigabitethernet 2/3
```

The following example shows reordering of every 50th packet with a distance limit of 5:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
switch(config)# exit
switch#
switch# ips netsim reorder nth 50 distance 5 ingress gigabitethernet 2/3
```

Related Commands

Command	Description
ips netsim enable	Enables the IP Network Simulator.
show ips netsim	Displays a summary of the interfaces that are currently operating in network simulation mode.

ipv6 access-list

To configure an IPv6 access control list (ACL) and enter IPv6-ACL configuration submode, use the **ipv6 access-list** command in configuration mode. To discard an IPv6 ACL, use the **no** form of the command.

ipv6 access-list *list-name*
no ipv6 access-list *list-name*

Syntax Description

list-name	Specifies an IP access control list name. The maximum size is 64.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Before using the **ipv6 access-list** command to configure an IPv6 ACL on a switch, become familiar with the features of IPv6 and its extended addressing capabilities. In particular, it is important to understand the different types of IPv6 address formats, the IPv6 address prefix format, and the different IPv6 address types. For detailed information about IPv6.

Examples

The following example configures an IPv6 access list called List1 and enters IPv6-ACL configuration submode:

```
switch # config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ipv6 access-list List1
switch(config-ipv6-acl)#
```

The following example removes the IPv6 access list called List1 and all of its entries:

```
switch(config)# no ipv6 access-list List1
switch(config)#
```

Related Commands

ipv6 route	Configures an IPv6 static route.
ipv6 routing	Enables IPv6 unicast routing.
show ipv6 access-list	Displays a summary of ACLs.
show ipv6 route	Displays the IPv6 static routes configured on the switch.
show ipv6 routing	Displays the IPv6 unicast routing configured on the switch.

ipv6 address

To enable IPv6 processing and configure an IPv6 address on the interface, use the **ipv6 address** command in interface configuration submode. To remove an IPv6 address, use the **no** form of the command.

ipv6 address *ipv6-address-prefix*
no ipv6 address *ipv6-address-prefix*

Syntax Description

ipv6-address-prefix	Specifies the IPv6 address prefix. The format is *X:X:X::X/n* .

Command Default

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can use the **ipv6 address** command to enable IPv6 processing and configure the IPv6 address on the interface. An IPv6 a ddress must be configured on an interface for the interface to forward IPv6 traffic.

Assigning a unicast address generates a link local address and implicitly enables IPv6.

Note The *ipv6-address-prefix* argument in the **ipv6 address** command must be in the form documented in R FC 2373, where the address is specified in hexadecimal using 16-bit values between colons. A slash mark (/) precedes a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

Examples

The following example assigns a unicast IPv6 address to the interface and enables IPv6 processing on the interface:

```
switch#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#interface gigabitethernet 2/2
switch(config-if)#ipv6 address 2001:0DB8:800:200C::417A/64
```

Related Commands

ipv6 enable	Enables IPv6 processing on the interface.
ipv6 nd	Configures IPv6 neighbor discovery commands on the interface.
ipv6 traffic-filter	Configures IPv6 ACLs to filter traffic for packets on the interface.
show interface	Displays interface configuration information.

ipv6 enable

To enable IPv6 processing and configure an IPv6 link-local address on the interface, use the **ipv6 enable** command in interface configuration submode. To disable IPv6 processing and remove the link-local address, use the **no** form of the command.

ipv6 enable
no ipv6 enable

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

When you enable IPv6 on an interface, a link local address is automatically assigned. This address is used for communication on the switch:

Examples

The following example enables IPv6 processing on the interface:

```
switch#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#interface gigabitethernet 2/2
switch(config-if)#ipv6 enable
```

The following example disables IPv6 processing on the interface:

```
switch(config-if)# no ipv6 enable
```

Related Commands

ipv6 address	Configures the IPv6 address and enables IPv6 processing.
ipv6 nd	Configures IPv6 neighbor discovery commands on the interface.
ipv6 traffic-filter	Configures IPv6 ACLs to filter traffic for packets on the interface.
show interface	Displays interface configuration information.

ipv6 nd

To configure IPv6 neighbor discovery commands on the interface, use the **ipv6 nd** command in interface configuration submode. To remove IPv6 neighbor discovery configuration commands, use the **no** form of the command.

ipv6 nd {**dad attempts** *number*|**reachable-time** *time*|**retransmission-time** *time*}
no ipv6 nd {**dad attempts** *number*|**reachable-time** *time*|**retransmission-time** *time*}

Syntax Description

dad attempts *number*	Configures duplicate address detection (DAD) attempts. The range is 0 to 15.
reachable-time *time*	Configures reachability time. Specifies the reachability time in milliseconds. The range is 1000 to 3600000.
retransmission-time *time*	Configures the retransmission timer. Specifies the retransmission time in milliseconds. The range is 1000 to 3600000.

Command Default

DAD attempts: 0.

Reachable-time: 30000 milliseconds.

Retransmission-time: 1000 milliseconds.

Command Modes

Interface configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

A router must be able to determine the link-local address for each of its neighboring routers in order to ensure that the target address (the final destination) in a redirect message identifies the neighbor router by its link-local address. For static routing, the address of the next-hop router should be specified using the link-local address of the router; for dynamic routing, all IPv6 routing protocols must exchange the link-local addresses of neighboring routers.

Note A high number of DAD attempts (greater than 2) can delay address assignment.

For complete information about IPv6 neighbor discovery.

Examples

The following example sets the duplicate address detection attempts count to 2:

```
switch# config terminal
switch(config)# interface gigabitethernet 2/2
switch(config-if)# ipv6 nd dad attempts 2
```

The following example sets the reachability time to 10000 milliseconds:

```
switch(config-if)# ipv6 nd reachability-time 10000
```

The following example sets the retransmission time to 20000 milliseconds:

```
switch(config-if)# ipv6 nd retransmission-time 20000
```

Related Commands

ipv6 address	Configures the IPv6 address and enables IPv6 processing.
ipv6 enable	Enables IPv6 processing on the interface.
ipv6 traffic-filter	Configures IPv6 ACLs to filter traffic for packets on the interface.
show interface	Displays interface configuration information.

ipv6 route

To configure an IPv6 static route, use the **ipv6 route** command in configuration mode. To remove or disable an IPv6 static route, use the **no** form of the command.

ipv6 route *destination-address-prefix next-hop-address* [{**distance** *distance-metric*|**interface** {**gigabitethernet** *slot/port*|**mgmt** *number*|**port-channel** *number*|**vsan** *vsan-id*}}] [**distance** *distance-metric*]
no ipv6 route *destination-address-prefix next-hop-address* [{**distance** *distance-metric*|**interface** {**gigabitethernet** *slot/port*|**mgmt** *number*|**port-channel** *number*|**vsan** *vsan-id*}}] [**distance** *distance-metric*]

Syntax Description

destination-address-prefix	Specifies the IPv6 destination address prefix. The format is *X:X:X::X/n* .
next-hop-address	Specifies the next hop IPv6 address. The format is *X:X:X::X* .
distance	(Optional) Configures an IPv6 route metric.
distance-metric	Specifies a distance metric for the specified route. The range is 0 to 32766.
interface	(Optional) Configures a next hop IPv6 address.
gigabitethernet*slot/port*	(Optional) Specifies a Gigabit Ethernet slot and port number.
mgmt *number*	(Optional) Specifies the management interface.
port-channel *number*	(Optional) Specifies a PortChannel number. The range is 1 to 128
vsan *vsan-id*	(Optional) Specifies an IPFC VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Before using the **ipv6 route** command to configure IPv6 features on a switch, become familiar with the features of IPv6 and its extended addressing capabilities. In particular, it is important to understand the different types of IPv6 address formats, the IPv6 address prefix format, and the different IPv6 address types.

Examples

The following example configures a static default IPv6 route on a Gigabit Ethernet interface:

```
switch # config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ipv6 route ::/0 gigabitethernet 3/1
```

The following example configures a fully specified static route on a Gigabit Ethernet interface:

```
switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet 3/2
```

The following example configures a recursive static route to a specified next hop address:

```
switch(config)# ipv6 route 2001:0DB8::/32 2001:0DB8:2002::1
```

The following example configures a recursive static route to a specified next hop address, from which the output interface is automatically derived, and to a specified interface:

```
switch(config)# ipv6 route 2001:0DB8::/32 2001:0DB8:2002::1 gigabitethernet 3/2
```

The following example configures a static IPv6 route with an administrative distance of 20.

```
switch(config)# ipv6 route 2001:0DB8::/32 interface gigabitethernet 2/0 distance 20
```

Related Commands

ipv6 access-list	Configures an IPv6 access control list (ACL) and enters IPv6-ACL configuration submode.
ipv6 routing	Enables IPv6 unicast routing.
show ipv6 access-list	Displays a summary of ACLs.
show ipv6 route	Displays the static IPv6 routes configured on the switch.
show ipv6 routing	Displays the IPv6 unicast routing configured on the switch.

ipv6 routing

To enable IPv6 unicast routing, use the **ipv6 routing** command in configuration mode. To disable IPv6 unicast routing, use the **no** form of the command.

ipv6 routing
no ipv6 routing

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Before using the **ipv6 routing** command to configure IPv6 features on a switch, become familiar with the features of IPv6 and its extended addressing capabilities. In particular, it is important to understand the different types of IPv6 address formats, the IPv6 address prefix format, and the different IPv6 address types.

Examples

The following example enables IPv6 routing:

```
switch # config terminal
switch(config)# ipv6 routing
```

The following example disables IPv6 routing:

```
switch(config)# no ipv6 routing
```

Related Commands

ipv6 access-list	Configures an IPv6 access control list (ACL) and enters IPv6-ACL configuration submode.
ipv6 route	Configures a static IPv6 route.
show ipv6 access-list	Displays a summary of ACLs.
show ipv6 route	Displays the static IPv6 routes configured on the switch.
show ipv6 routing	Displays the IPv6 unicast routing configured on the switch.

ipv6 traffic-filter

To configure IPv6 access control lists (ACLs) to filter traffic for packets on the interface, use the **ipv6 traffic-filter** command in interface configuration submode. To remove an IPv6-ACL traffic filter on the switch, use the **no** form of the command.

ipv6 traffic-filter *access-list-name* {**in**|**out**}
no ipv6 traffic-filter *access-list-name* {**in**|**out**}

Syntax Description

access-list-name	Specifies the name of an access control list for packets. The maximum size is 64 characters.
in	Configures inbound packets.
out	Configures outbound packets.

Command Default

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures a traffic filter, called testfilter, for inbound packets:

```
switch# config terminal
switch(config)# interface gigabitethernet 2/2
switch(config-if)# ipv6 traffic-filter testfilter in
```

Related Commands

ipv6 address	Configures the IPv6 address and enables IPv6 processing.
ipv6 enable	Enables IPv6 processing on the interface.
ipv6 nd	Configures IPv6 ACLs to filter traffic for packets on the interface.
show interface	Displays interface configuration information.

iscsi authentication

To configure the default authentication method for iSCSI, use the **iscsi authentication** command. To revert to the default, use the **no** form of the command.

iscsi authentication {**chap**|**chap-none**|**none**|**username** *username* **password** [{**0**|**7**}] *password*}
no iscsi authentication {**chap**|**chap-none**|**none**|**username**}

Syntax Description

chap-none	Configures either the CHAP or no authentication.
chap	Configures the Challenge Handshake Authentication Protocol (CHAP) authentication method.
none	Specifies that no authentication is required for the selected interface
username *username*	Assigns CHAP username to be used when switch is authenticated.
password	Configures the password for the username.
0	(Optional) Specifies that the password is a cleartext CHAP password.
7	(Optional) Specifies that the password is an encrypted CHAP password.
password	Specifies a password for the username.

Command Default

chap-none.

The default password is a cleartext password.

Command Modes

Configuration mode.

Command History

Release	Modification
1.1(1)	This command was introduced.
2.0(x)	Added the **username** option.

Usage Guidelines

By default, the Cisco MDS 9000 Family switch accepts an iSCSI initiator with either no authentication or CHAP authentication. If CHAP authentication is always required, use the **iscsi authentication chap** command. If no authentication is always required, use the **iscsi authentication none** command.

Use the **chap-none** option to override the global configuration which might have been configured to allow only one option either CHAP or none but not both.

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 configures CHAP only for ISCSI authentication:

```
switch# config terminal
switch(config)# iscsi authentication chap
```

Related Commands

Command	Description
show iscsi global	Displays all iSCSI initiators configured by the user.

iscsi duplicate-wwn-check

To check the current running configuration for conflicts between iSCSI initiators' static WWN allocation and what the system thinks is available in its WWN pool, use the **iscsi duplicate-wwn-check** command in configuration mode.

iscsi duplicate-wwn-check

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

Prior to Cisco MDS SAN-OS Release 2.1(2), WWNs assigned to static iSCSI initiators by the system can be inadvertently returned to the system when an upgrade fails or the system software is manually downgraded (that is, when you manually boot up an older Cisco MDS SAN-OS release without using the **install all** command). In these instances, the system can later assign those WWNs to other iSCSI initiators (dynamic or static) and cause conflicts.

As of Cisco MDS SAN-OS Release 2.1(2), you can use the **iscsi duplicate-wwn-check** command to check for and remove any configured WWNs that belong to the system.

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 check the current running configuration for conflicts between iSCSI initiators' static WWN allocation and what the system thinks is available in its WWN pool:

```
switch# config terminal
Enter configuration command, one per line. End with CNTL/Z.
switch(config)# iscsi duplicate-wwn-check

List of Potential WWN Conflicts:
-------------------------------
Node : iqn.test-local-nwnn:1-local-pwwn:1
nWWN : 22:03:00:0d:ec:02:cb:02
pWWN : 22:04:00:0d:ec:02:cb:02
```

The following example shows how to remove the conflicting nWWN and pWWN:

```
switch(config)# iscsi initiator name iqn.test-local-nwwn:1-local-pwwn:1
switch(config-iscsi-init)# no static nWWN  22:03:00:0d:ec:02:cb:02
switch(config-iscsi-init)# no static pWWN  22:04:00:0d:ec:02:cb:02
```

Related Commands

Command	Description
iscsi initiator name	Assigns an iSCSI name and changes to iSCSI initiator configuration submode.
static	Assigns persistent WWNs to an iSCSI initiator in iSCSI initiator configuration submode.
show iscsi initiator	Displays information about configured iSCSI initiators.

iscsi dynamic initiator

To configure dynamic initiator modes, use the **iscsi dynamic initiator** command in configuration mode. To revert to the default mode, use the **no** form of the command.

iscsi dynamic initiator {**deny**|**islb**}
no dynamic initiator {**deny**|**islb**}

Syntax Description

deny	Specifies that dynamic initiators are denied from logging on to the MDS switch.
islb	Specifies iSLB dynamic initiator mode.

Command Default

iSCSI.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Three dynamic initiator modes are supported:

- iSCSI—Dynamic initiators are treated as iSCSI initiators and can access dynamic virtual targets and configured iSCSI virtual targets.
- iSLB—Dynamic initiators are treated as iSLB initiators and can access dynamic virtual targets.
- Deny—Dynamic initiators are not allowed to log in to the MDS switch.

iSCSI dynamic initiator is the default mode of operation. This configuration is distributed using CFS.

Note Configuring dynamic initiator modes is supported only through the CLI, not through Device Manager or Fabric Manager.

A dynamic iSCSI initiator can be converted to a static iSCSI initiator and its WWNs can be made persistent.

A dynamic iSLB initiator can be converted to a static iSLB initiator and its WWNs can be made persistent.

Note You cannot convert a dynamic iSCSI initiator to a static iSLB initiator, or a dynamic iSLB initiator to a static iSCSI initiator.

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 command configures the dynamic initiator mode as iSLB:

```
switch(config)# iscsi dynamic initiator islb
```

The following command configures the dynamic initiator mode as deny:

```
switch(config)# iscsi dynamic initiator deny
```

The following command reverts to the default dynamic initiator mode of iSCSI:

```
switch(config)# no iscsi dynamic initiator deny
```

Related Commands

Command	Description
iscsi save-initiator	Permanently saves the automatically assigned nWWN or pWWN mapping.
show iscsi global	Displays global iSCSI configured information.

iscsi enable

To enable the iSCSI feature in any Cisco MDS switch, use the **iscsi enable** command. To disable this feature, use the **no** form of the command.

iscsi enable
no iscsi enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.2(2c)	Updated the example command.
NX-OS 4.1(1)	This command was deprecated.

Usage Guidelines

The configuration and verification commands for the iSCSI feature are only available when iSCSI is enabled on a switch. When you disable this feature, all related configurations are automatically discarded.

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 command enables the iSCSI feature:

```
switch(config)# iscsi enable
switch(config)# iscsi enable module 8
switch(config)# int iscsi 2/1
switch(config-if)#
switch(config)# no shutdown
```

The following command disables the iSCSI feature (default):

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

iscsi enable module

To enable iSCSI features for each IPS linecard to create corresponding iSCSI interfaces, use the **iscsi enable module** command.

iscsi enable module *module-num*

Syntax Description

module-num	Specifies the desired IPS linecard module number on which iSCSI interfaces need to be enabled.

Command Default

iSCSI interfaces are disabled on IPS linecards by default.

Command Modes

Configuration mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable the iSCSI interface on a desired module number on the switch:

```
switch# config terminal
switch(config)# iscsi enable module 1
```

Note The iSCSI feature must be enabled before executing this command.

Related Commands

Command	Description
iscsi enable	Enables the iSCSI features but does not create the interfaces.

iscsi import target fc

To allow dynamic mapping of Fibre Channel targets, use the **iscsi import target fc** command. To disable this feature, use the **no** form of the command.

iscsi import target fc
no iscsi import target fc

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command directs iSCSI to dynamically import all Fibre Channel targets into iSCSI.

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 allows dynamic mapping of Fibre Channel targets:

```
switch# config terminal
switch(config)# iscsi import target fc
```

The following example disables dynamic mapping of Fibre Channel targets:

```
switch(config)# no iscsi import target fc
```

Related Commands

Command	Description
show iscsi global	Displays all iSCSI initiators configured by the user.

iscsi initiator idle-timeout

To configure the iSCSI initiator idle timeout, use the **iscsi initiator idle-timeout** command. To revert to the default, use the **no** form of the command.

iscsi initiator idle-timeout *seconds*
no iscsi initiator idle-timeout *seconds*

Syntax Description

seconds	Specifies the timeout in seconds. The range is 0 to 3600.

Command Default

300 seconds.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3	This command was introduced.

Usage Guidelines

When the idle timeout value is set to 0, the initiator information is cleared immediately after the last session from the initiator terminates.

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 configures the iSCSI initiator idle timeout to 180 seconds:

```
switch# config terminal
switch(config)# iscsi initiator idle-timeout 180
```

The following example reverts the default value of 300 seconds:

```
switch# config terminal
switch(config)# no iscsi initiator idle-timeout 240
```

Related Commands

Command	Description
show iscsi global	Displays global iSCSI configuration information.

iscsi initiator ip-address

To assign persistent WWNs to an iSCSI initiator or assign an iSCSI initiator into VSANs other than the default VSAN, use the **iscsi initiator ip-address** command. To revert to the default, use the **no** form of the command.

iscsi initiator ip-address *ipaddress* **static** {**nwwn**|**pwwn**} {*wwn-id*|**system-assign** *number*} **vsan** *vsan-id*
no iscsi initiator ip-address *ipaddress* **static** {**nwwn**|**pwwn**} {*wwn-id*|**system-assign** *number*} **vsan** *vsan-id*

Syntax Description

ipaddress	Specifies the initiator IP address.
nwwn	Configures the inititiator node WWN hex value.
pwwn	Configures the peer WWN for special frames.
wwn-id	Enters the pWWN or nWWN ID.
system-assign *number*	Generates the nWWN value automatically. The number ranges from 1 to 64.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Under a circumstance where an iSCSI initiator needs to have a persistent binding to FC WWNs, this command should be used. Also, an iSCSI initiator can be put into multiple VSANs. An iSCSI host can become a member of one or more VSANs.

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 command configures an iSCSI initiator. using the IP address of the initiator node:

```
switch(config)# iscsi initiator ip address 209.165.200.226
```

The following command deletes the configured iSCSI initiator.

```
switch(config)# no iscsi initiator ip address 209.165.200.226
```

The following command uses the switch's WWN pool to allocate the nWWN for this iSCSI initiator and keeps it persistent:

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

The following command assigns the user provided WWN as nWWN for the iSCSI initiator. You can only specify one nWWN for each iSCSI node:

```
switch(config-(iscsi-init))# nWWN 20:00:00:05:30:00:59:11
```

The following command uses the switch's WWN pool to allocate two pWWNs for this iSCSI initiator and keeps it persistent:

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

The following command assigns the user provided WWN as pWWN for the iSCSI initiator:

```
switch(config-(iscsi-init))# pWWN 21:00:00:20:37:73:3b:20
```

Related Commands

Command	Description
show iscsi initiator	Displays information about configured iSCSI initiators.

iscsi initiator name

To configure an iSCSI initiator name and change to iSCSI configuration mode, use the **iscsi initiator name** command. To revert to factory defaults, use the **no** form of the command.

iscsi initiator name *name*
no iscsi initiator name *name*

Syntax Description

name	Enters the initiator name to be used. The minimum length is 16 characters and maximum is 223 characters.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(2)	This command was introduced.

Usage Guidelines

Under a circumstance where an iSCSI initiator needs to have a persistent binding to FC WWNs, this command should be used. Also, an iSCSI initiator can be put into multiple VSANs. An iSCSI host can become a member of one or more VSANs.

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 configures an iSCSI initiator using the iSCSI name of the initiator node:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# iscsi initiator name iqn.1987-02.com.cisco.initiator
```

Related Commands

Command	Description
show iscsi initiator	Displays information about configured iSCSI initiators.

iscsi interface vsan-membership

To configure VSAN membership for iSCSI interfaces, use the **iscsi interface vsan-membership** command. Use the **no** form of this command to disable this feature or to revert to factory defaults.

iscsi interface vsan-membership
no iscsi interface vsan-membership

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

If the **iscsi interface vsan-membership** command is disabled, you will not be able to configure iSCSI VSAN membership.

Caution Changing the VSAN membership, the forwarding mode, and the authentication of an iSCSI interface that is part of an iSLB VRRP group impacts load balancing on the interface.

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 command enables the iSCSI interface VSAN membership:

```
switch# config terminal
switch(config)# iscsi interface vsan-membership
```

The following command disables the iSCSI interface VSAN membership (default):

```
switch(config)# no iscsi interface vsan-membership
```

Related Commands

Command	Description
show iscsi initiator	Displays information about configured iSCSI initiators.

iscsi save-initiator

To permanently save the automatically assigned nWWN and pWWN mapping, use the **iscsi save-initiator** command.

iscsi save-initiator [{**ip-address** *ip-address*|**name** *name*}]

Syntax Description

ip-address *ip-address*	(Optional) Specifies the initiator IP address.
name *name*	(Optional) Specifies the initiator name to be used from 1 to 255 characters. The minimum length is 16 characters.

Command Default

If initiator name or IP address is not specified, the nWWN and pWWN mapping for all initiators becomes permanent.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

After executing the **iscsi save-initiator** command, issue the **copy running-config startup-config** to save the nWWN and pWWN mapping across switch reboots.

After a dynamic iSCSI initiator has logged in, you may decide to permanently save the automatically assigned nWWN and pWWN mapping so this initiator uses the same mapping the next time it logs in.

You can convert a dynamic iSCSI initiator to static iSCSI initiator and make its WWNs persistent.

Note You cannot convert a dynamic iSCSI initiator to a static iSLB initiator or a dynamic iSLB initiator to a static iSCSI initiator.

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 save the nWWN and pWWN mapping for all the initiators:

```
switch(config)# iscsi save-initiator
```

The following example shows how to save the nWWN and pWWN mapping for an initiator named iqn.1987-02.com.cisco.initiator:

```
switch(config)# iscsi save-initiator name iqn.1987-02.com.cisco.initiator
```

Related Commands

Command	Description
iscsi initiator	Configures an iSCSI initiator.
show iscsi initiator	Displays information about configured iSCSI initiators.

iscsi virtual-target name

To create a static iSCSI virtual target, use the **iscsi virtual-target** command. To revert to the default values, use the **no** form of the command.

iscsi virtual-target name *name* **advertise interface** {**gigabitethernet** *slot*/*port* [*.subinterface*]|**port-channel** *channel-id* [*.subinterface*]} **all-initiator-permit initiator** {**initiator-name**|**ip-address** *ipaddress* [*netmask*]} **permit pwwn** *pwwn-id* [{**fc-lun** *number* **iscsi-lun** *number* [**secondary-pwwn** *pwwn-id* [**sec-lun** *number*]]|**secondary-pwwn** *pwwn-id*}] **revert-primary-port trespass**
no iscsi virtual-target name *name* **advertise interface** {**gigabitethernet** *slot*/*port* [*.subinterface*]|**port-channel** *channel-id* [*.subinterface*]} **all-initiator-permit initiator** {**initiator-name**|**ip-address** *ipaddress* [*netmask*]} **permit pwwn** *pwwn-id* [{**fc-lun** *number* **iscsi-lun** *number* [**secondary-pwwn** *pwwn-id* [**sec-lun** *number*]]|**secondary-pwwn** *pwwn-id*}] **revert-primary-port trespass**

Syntax Description

name	Enters the virtual target name to be used. The minimum length is 16 characters and maximum of 223 bytes.
advertise interface	Advertises the virtual target name on the specified interface.
gigabitethernet *slot*/*port subinterface*	Selects the Gigabit Ethernet interface or subinterface to configure.
port-channel *channel-id subinterface*	Selects the Port Channel interface or subinterface to configure.
all-initiator-permit	Enables all iSCSI initiator access to this target.
initiator	Configures specific iSCSI initiator access to this target.
initiator-name	Specifies the iSCSI initiator name to be used access a specified target. Maximum length is 255 characters.
ip-address *ip-address*	Specifies the iSCSI initiator IP address.
permit	Permits access to the specified target.
pwwn *pwwn-id*	Specifies the peer WWN ID for special frames.
secondary-pwwn *pwwn-id*	(Optional) Specifies the secondary pWWN ID.
fc-lun *number*	(Optional) Specifies the Fibre Channel Logical Unit Number (LUN).
iscsi-lun *number*	(Optional) Specifies the iSCSI virtual target number.
sec-lun *number*	(Optional) Specifies the secondary Fibre Channel LUN.
revert-primary-port trespass	Moves LUNs forcefully from one port to another.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.1(1)	This command was introduced.
1.3(1)	Added **revert-to-primary** and **trespass** subcommands.

Usage Guidelines

This command is used to configure a static iSCSI target for access by iSCSI initiators. A virtual target may contain a subset of LUs of an FC target or one whole FC target.

Do not specify the LUN if you want to map the whole Fibre Channel target to an iSCSI target. All Fibre Channel LUN targets are exposed to iSCSI.

Note The CLI interprets the LUN identifier value as a hexadecimal value whether or not the 0x prefix is included.

One iSCSI target cannot contain more than one Fibre Channel target.

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 creates a static virtual target and enters ISCSI target configuration submode:

```
switch# config terminal
switch(config)# iscsi virtual-target name 0123456789ABDEFGHI
switch(config-iscsi-tgt)#
```

The following command advertises the virtual target only on the specified interface. By default, it is advertised on all interfaces in all IPS modules.

```
switch(config-iscsi-tgt)# advertise interface gigabitethernet 4/1
```

The following command maps a virtual target node to a Fibre Channel target:

```
switch(config-iscsi-tgt)# pWWN 26:00:01:02:03:04:05:06
```

The following command enters the secondary pWWN for the virtual target node:

```
switch(config-iscsi-tgt)# pWWN 26:00:01:02:03:04:05:06 secondary-pwwn 66:00:01:02:03:04:05:02
```

Use the LUN option to map different Fibre Channel LUNs to different iSCSI virtual targets. If you have already mapped the whole Fibre Channel target, you will not be able to use this option.

```
switch(config-iscsi-tgt)# pWWN 26:00:01:02:03:04:05:06 fc-lun 0 iscsi-lun 0
```

The following command allows the specified iSCSI initiator node to access this virtual target. You can issue this command multiple times to allow multiple initiators.

```
switch(config-iscsi-tgt)# initiator iqn.1987-02.com.cisco.initiator1 permit
```

The following command prevents the specified initiator node from accessing virtual targets:

```
switch(config-iscsi-tgt)# no initiator iqn.1987-02.com.cisco.initiator1 permit
```

The following command allows the specified IP address to access this virtual target:

```
switch(config-iscsi-tgt)# initiator ip-address 209.165.200.226 permit
```

The following command prevents the specified IP address from accessing virtual targets:

```
switch(config-iscsi-tgt)# no initiator ip-address 209.165.200.226 permit
```

The following command allows all initiators in this subnetwork to access this virtual target:

```
switch(config-iscsi-tgt)# initiator ip-address 10.50.0.0 255.255.255.0 permit
```

The following command prevents all initiators in this subnetwork from accessing virtual targets:

```
switch(config-iscsi-tgt)# no initiator ip-address 10.50.0.0 255.255.255.0 permit
```

The following command allows all initiator nodes to access this virtual target:

```
switch(config-iscsi-tgt)# all-initiator-permit
```

The following command prevents any initiator node from accessing virtual targets:

```
switch(config-iscsi-tgt)# no all-initiator-permit
```

The following command configures a primary and secondary port and moves the LUNs from one port to the other using the **trespass** command:

```
switch# config terminal
switch(config)# iscsi virtual-target name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-tgt)# pwwn 50:00:00:a1:94:cc secondary-pwwn 50:00:00:a1:97:ac
switch(config-iscsi-tgt)# trespass
```

Related Commands

Command	Description
show iscsi virtual target	Displays information about iSCSI virtual targets.

islb abort

To discard a pending iSCSI Server Load Balancing (iSLB) configuration, use the **islb abort** command.

islb abort

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can use the **islb abort** command to discard the pending changes to the iSLB configuration and release the fabric lock. This action has no effect on the active configuration on any switch in the fabric.

The **islb abort** command can be issued only by the user who started the Cisco Fabric Services (CFS) session and only on the switch that started the CFS session.

Examples

The following example discards the pending iSLB configuration distribution:

```
switch# config t
switch(config)# islb abort
```

Related Commands

Command	Description
clear islb session	Clears a pending iSLB configuration. This command can be issued on any switch by a user with admin privileges.
islb commit	Commits the iSLB configuration distribution and releases the fabric lock.
show islb cfs-session status	Displays iSLB information.
show islb pending	Displays the pending configuration changes.
show islb pending-diff	Displays the differences between the pending configuration and the current configuration.

islb commit

To commit a pending iSCSI server load balancing (iSLB) configuration, use the **islb commit** command.

islb commit

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can use the **islb commit** command to commit the pending changes to the iSLB configuration and release the fabric lock. This action changes the active configuration on all Cisco MDS switches in the fabric.

The **islb commit** command can be issued only by the user who started the Cisco Fabric Services (CFS) session and only on the switch that started the CFS session.

Examples

The following example commits the pending iSLB configuration distribution:

```
switch# config t
switch(config)# islb commit
```

Related Commands

Command	Description
clear islb session	Clears a pending iSLB configuration. This command can be issued on any switch by a user with admin privileges.
islb abort	Discards the pending iSLB configuration distribution and releases the fabric lock.
islb distribute	Enables iSLB configuration distribution.
show islb cfs-session status	Displays iSLB information.
show islb pending	Displays the pending configuration changes.
show islb pending-diff	Displays the differences between the pending configuration and the current configuration.

islb distribute

To enable Cisco Fabric Services for iSCSI Server Load Balancing (iSLB) configuration, use the **islb distribute** command. To disable the iSLB configuration distribution, use the **no** form of the command

islb distribute
no islb distribute

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can use the **islb distribute** command to enable the distribution of iSLB configuration information to other Cisco MDS switches in the fabric using the Cisco Fabric Services (CFS) infrastructure. You can synchronize the iSLB configuration across the fabric from the console of a single MDS switch.

Note The only initiator configuration that is distributed throughout the fabric using CFS is a statically mapped, iSLB initiator configuration. Dynamically mapped and statically mapped iSCSI initiator configurations are not distributed. iSCSI initiator idle-timeout and global authentication parameters are also distributed.

If you are using both iSLB and inter-VSAN routing (IVR), ensure that the following conditions are satisfied; otherwise, traffic may be disrupted in the fabric.

- You must enable both features on at least one switch in the fabric.
- You must configure and activate zoning from the switch for normal zones, IVR zones, and and iSLB zones.

Examples

The following example enables iSLB configuration distribution:

```
switch# config t
switch(config)# islb distribute
```

The following example disables iSLB configuration distribution:

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

Related Commands

Command	Description
clear islb session	Clears a pending iSLB configuration. This command can be issued on any switch by a user with admin privileges.

Command	Description
islb abort	Discards the pending iSLB configuration distribution and releases the fabric lock.
islb commit	Commits the iSLB configuration distribution and releases the fabric lock.

islb initiator

To configure the iSCSI server load balancing (iSLB) initiator and enter iSLB initiator configuration submode, use the **islb initiator** command. To delete the configured ISLB initiator, use the **no** form of the command.

islb initiator {**ip-address** {*ip-addressipv6-address*}|**name** *name*}
no islb initiator name *name*

Syntax Description

ip-address	Specifies the iSLB initiator node IP address.
ip-address	Specifies the initiator IPv4 address.
ipv6-address	Specifies the initiator IPv6 address.
name *name*	Specifies the iSLB initiator node name. The maximum size is 223.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can use the **islb initiator** command to enter iSLB initiator configuration submode to configure static mapping for an iSLB initiator.

Examples

The following example enters iSLB initiator configuration submode to configure static mapping (using the IPv4 ip-address option) for an iSLB initiator:

```
switch# config t
switch(config)# islb initiator ipaddress 10.1.2.3
switch(config-islb-init)#
```

The following example deletes the configured iSLB initiator:

```
switch(config)# no islb initiator ipaddress 10.1.2.3
```

The following example enters iSLB initiator configuration submode to configure static mapping (using the IPv6 option) for an iSLB initiator:

```
switch# config t
switch(config)# islb initiator ipaddress 1111.2222.3333.4::5
switch(config-islb-init)#
```

The following example deletes the configured iSLB initiator:

```
switch(config)# no islb initiator ipaddress 1111.2222.3333.4::5
```

The following example enters iSLB initiator configuration submode to configure static mapping (using the name option) for an iSLB initiator:

```
switch# config t
switch(config)# islb initiator name iqn.1987-02.co..cisco.initiator
switch(config-islb-init)#
```

The following example deletes the configured iSLB initiator:

```
switch(config)# no islb initiator ipaddress name iqn.1987-02.co..cisco.initiator
```

Related Commands

Command	Description
show islb initiator configured	Displays iSLB initiator configuration information.
show islb initiator detail	Displays more detailed information about the iSLB configuration.
show islb initiator iscsi-session	Displays iSLB session details.
show islb initiator summary	Displays iSLB initiator summary information.

islb save-initiator

To permanently save the automatically assigned nWWN and pWWN mapping for the iSLB initiator, use the **islb save-initiator** command.

islb save-initiator [{**ip-address** *ip-address*|**name** *name*}]

Syntax Description

ip-address *ip-address*	(Optional) Specifies the initiator IP address. The format is *A.B.C.D* or *X:X:X::X* .
name *name*	(Optional) Specifies the initiator name to be used from 1 to 223 characters.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Saving the automatically assigned nWWN and pWWN mapping allows the initiator to use the same mapping the next time it logs in.

You can convert a dynamic iSLB initiator to a static iSLB initiator and make its WWNs persistent.

Note You cannot convert a dynamic iSCSI initiator to a static iSLB initiator or a dynamic iSLB initiator to a static iSCSI initiator.

Note Making the dynamic mapping for iSLB initiators static is the same as for iSCSI.

Note Only a statically mapped iSLB initiator configuration is distributed throughout the fabric using CFS. Dynamically and statically configured iSCSI initiator configurations are not distributed.

Examples

The following example saves the nWWNs and pWWNs that have automatically been assigned to the iSLB initiator whose name is specified:

```
switch# config t
switch(config)# islb save-initiator name iqn.1987-02.com.cisco.initiator
```

The following example saves the nWWNs and pWWNs that have automatically been assigned to the iSLB initiator whose IPv4 address is specified:

```
switch(config)# islb save-initiator ip-address 10.10.100.11
```

The following example saves the nWWNs and pWWNs that have automatically been assigned to all the iSLB initiators:

```
switch(config)# islb save-initiator

Please execute "copy run start" to keep the WWNs persistent across switch reboots
```

Related Commands

Command	Description
show islb session	Displays detailed iSLB session information.

islb virtual-target name

To configure an iSLB virtual target and enter iSLB target configuration submode, use the **islb virtual-target name** command. To revert to the default values, use the **no** form of the command.

islb virtual-target name *name* {**all-initiator-permit**|**initiator** {*initiator-name* **permit**|**ip address** {*A.B.C.D* **permit**|*X*:*X*:*X*:*X*:*X* **permit**}}|**pWWN permit**|**revert-primary-port permit**|**trespass permit**}
no islb virtual-target name *name* {**all-initiator-permit**|**initiator** {*initiator-name* **permit**|**ip address** {*A.B.C.D* **permit**|*X*:*X*:*X*:*X*:*X* **permit**}}|**pWWN permit**|**revert-primary-port permit**|**trespass permit**}

Syntax Description

name	Specifies the virtual target name to be used. The minimum length is 16 bytes and the maximum length is 223 bytes.
all-initiator-permit	Configures all iSLB initiators to access the target.
initiator	Configures the iSLB initiator to access the target.
initiator-name	Specifies the initiator name. The minimum length is 16 bytes and the maximum length is 223 bytes.
X:X:X::X **permit**	Permits access to the specified target.
ip address	Specifies the initiator IP address. The format is *A.B.C.D* or *X:X:X::X* .
pWWN permit	Specifies the pWWN of the Fibre Channel target. The format is *hh:hh:hh:hh:hh:hh:hh:hh* .
revert-primary-port permit	Reverts to the primary port when it becomes active again.
trespass permit	Enables trespass support.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command is used to configure a static target for access by iSLB initiators.

Examples

The following example creates a static virtual target and enters iSLB target configuration submode:

```
switch# config terminal
switch(config)# islb virtual-target name ABCDEFGHIJ1234567890
ips-hac1(config-islb-tgt)#
```

The following example allows all iSLB initiators to access the target:

```
ips-hac1(config-islb-tgt)# all-initiator-permit
```

The following command allows the specified IP address to access this virtual target:

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

The following example prevents the specified IP address from accessing virtual targets:

```
switch(config-islb-tgt)# no initiator ip-address 209.165.200.226 permit
```

The following example allows all initiators in this subnetwork to access this virtual target:

```
switch(config-islb-tgt)# initiator ip-address 10.50.0.0 255.255.255.0 permit
```

The following example prevents all initiators in this subnetwork from accessing virtual targets:

```
switch(config-islb-tgt)# no initiator ip-address 10.50.0.0 255.255.255.0 permit
```

The following example maps a pWWN to a Fibre Channel target:

```
ips-hac1(config-islb-tgt)# pwwn 26:00:01:02:03:04:05:06
```

Related Commands

Command	Description
show islb virtual-target	Displays information about iSLB virtual targets.

islb vrrp

To configure iSCSI server load balancing (iSLB) on a Virtual Router Redundancy Protocol (VRRP) group, use the **islb vrrp** command. To disable the iSLB configuration on the VRRP group, use the **no** form of the command.

islb vrrp {*group-number* **load-balance**|**ipv6** *group-number* **load-balance**}
no islb vrrp {*group-number* **load-balance**|**ipv6** *group-number* **load-balance**}

Syntax Description

group-number	Specifies an IPv4 Virtual Router group number. The range is 1 to 255.
load-balance	Enables load balancing on the VRRP group.
ipv6	Specifies IPv6 on the VRRP group.
group-number	Specifies an IPv6 Virtual Router group number. The range is 1 to 255.
load-balance	Enables load balancing on the VRRP group.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The host is configured with a VRRP address as the portal address. When the VRRP master port receives the first iSCSI session from an initiator, it assigns a slave port to serve that particular host. The information is synchronized to all switches via Cisco Fabric Services (CFS) if recovery is needed when a master port fails. The initiator gets a temporary redirect iSCSI login response. The host then logs in to the slave port at its physical IP address. If the slave port goes down, the host will revert to the master port. The master port knows through CFS that the slave port has gone down and redirects the host to another slave port.

There are separate VRRP groups for IPv4 and IPv6. Each address family is allowed 256 virtual routers.

Note An initiator can also be redirected to the physical IP address of the master interface.

Tip The load balancing distribution is based on the number of initiators on a port and not on the number of sessions.

Caution A Gigabit Ethernet interface configured for iSLB can only be in one VRRP group because redirected sessions do not carry information about the VRRP IP address or group. This restriction allows the slave port to uniquely identify the VRRP group to which it belongs.

Caution Changing the VSAN membership, the forwarding mode, and the authentication of an iSCSI interface that is part of an iSLB VRRP group impacts load balancing on the interface.

The following example enables VRRP load balancing for IPv4 Virtual Router group 20:

```
switch# config t
switch(config)# islb vrrp 20 load-balance
```

The following example disables VRRP load balancing for IPv4 Virtual Router group 20:

```
switch(config)# no islb vrrp 20 load-balance
```

The following example enables VRRP load balancing for IPv6 Virtual Router group 30:

```
switch(config)# islb vrrp ipv6 30 load-balance
```

The following example disables VRRP load balancing for IPv6 Virtual Router group 30:

```
switch(config)# no islb ipv6 30 load-balance
```

Related Commands

Command	Description
show islb session	Displays detailed iSLB session information.

islb zoneset activate

To activate iSCSI server load balancing (iSLB) auto zones, use the **islb zoneset activate** command.

islb zoneset activate

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Auto-zoning of the initiator with the initiator targets is enabled by default.

A zone set must be active for a VSAN for auto-zones to be created in that VSAN. The **zoneset activate** command creates auto-zones only if at least one other change has been made to the zone set.

Examples

The following example activates an iSLB auto zone:

```
switch# config t
switch(config)# islb zoneset activate
```

Related Commands

Command	Description
show zoneset active	Displays active zone sets.

isns

To tag a Gigabit Ethernet or PortChannel interface to an Internet Storage Name Service (iSNS) profile, use the **isns** command in interface configuration submode. To untag the interface, use the **no** form of the command.

isns *profile-name*
no isns *profile-name*

Syntax Description

profile-name	Specifies the iSNS profile name.

Command Default

Disabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, iSNS must be enabled using the **isns-server enable** command.

Use the isns reregister command in EXEC mode to reregister associated iSNS objects (tagged to an iSNS profile) with the iSNS server.

Examples

The following example shows how to tag a Gigabit Ethernet interface to an iSNS profile:

```
switch# config terminal
switch(config)# interface gigabitethernet 1/2
switch(config-if)# isns Profile1
```

The following example shows how to tag a PortChannel interface to an iSNS profile:

```
switch# config terminal
switch(config)# interface port-channel 2
switch(config-if)# isns Profile2
```

Related Commands

Command	Description
isns reregister	Reregisters the iSNS object.
isns-server enable	Enables the iSNS server.
show interface gigabitethernet	Displays configuration and status information for a specified Gigabit Ethernet interface.
show interface port-channel	Displays configuration and status information for a specified PortChannel interface.
show isns	Displays iSNS information.

isns distribute

To enable Cisco Fabric Services (CFS) distribution for Internet Storage Name Service (iSNS), use the **isns distribute** command. To disable this feature, use the **no** form of the command.

isns distribute
no isns distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, iSNS must be enabled using the **isns-server enable** command.

You can configure the pWWN and nWWN of iSCSI initiators and permit a group of iSCSI initiators to share a given nWWN and pWWN pair by using a proxy initiator. The number of iSCSI initiators that register with the iSNS server is more than the number of iSCSI targets that register with the iSNS server. To synchronize the iSCSI initiator entries across switches, you can distribute the iSCSI initiator configuration to iSNS servers across switches.

Examples

The following example shows how to initiate iSNS information distribution:

```
switch# config terminal
switch(config)# isns distribute
```

The following example shows how to cancel iSNS information distribution:

```
switch# config terminal
switch(config)# no isns distribute
```

Related Commands

Command	Description
isns-server enable	Enables the iSNS server.
show isns	Displays iSNS information.

isns esi retries

To configure the number of entity status inquiry (ESI) retry attempts, use the **isns esi retries** command in configuration mode. To revert to the default value, use the **no** form of the command.

isns esi retries *number*
no isns esi retries *number*

Syntax Description

number	Specifies the number of retries. The range is 0 to 10.

Command Default

3 retries.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, Internet Storage Name Service (iSNS) must be enabled using the **isns-server enable** command.

The iSNS client queries the ESI port at user-configured intervals. Receipt of a response indicates that the client is still alive. Based on the configured value, the interval specifies the number of failed tries before which the client is deregistered from the server.

Examples

The following example shows how change the ESI retries limit to eight:

```
switch# config terminal
switch(config)# isns esi retries 8
```

Related Commands

Command	Description
isns-server enable	Enables the iSNS server.
show isns	Displays iSNS information.

isns profile name

To create an Internet Storage Name Service (iSNS) profile and enter iSNS profile configuration submode, use the **isns profile name** command in configuration mode. To delete the iSNS profile, use the **no** form of the command.

isns profile name *profile-name*
no isns profile name *profile-name*

Syntax Description

profile-name	Specifies the profile name. Maximum length is 64 characters.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

To use this command, iSNS must be enabled using the **isns-server enable** command.

Examples

The following example shows how to specify an iSNS profile name and enter iSNS profile configuration submode:

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

Related Commands

Command	Description
server	Configures a server IP address in an iSNS profile.
show isns	Displays iSNS information.

isns reregister

To register all Internet Storage Name Service (iSNS) objects for an interface that is already tagged to an iSNS profile, use the **isns register** command.

isns reregister {**gigabitethernet** *slot/number*|**port-channel** *channel-group*}

Syntax Description

gigabitethernet *slot/port*	Specifies tagged Gigabit Ethernet interface slot and port.
port-channel *channel-group*	Specifies tagged PortChannel group. The range is 1 to 128.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Use this command to reregister portals and targets with the iSNS server for a tagged interface.

Examples

The following command reregisters portal and targets for a tagged interface:

```
switch# isns reregister gigabitethernet 1/4
```

Related Commands

Command	Description
show isns profile	Displays details for configured iSNS profiles.

isns-server enable

To enable the Internet Storage Name Service (iSNS) server, use the **isns-server enable** command in configuration mode. To disable iSNS, use the **no** form of the command.

isns-server enable
no isns-server enable

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

Performing the **isns-server enable** command enables the commands used to configure iSNS.

Examples

The following example shows how to enable iSNS:

```
switch# config terminal
switch(config)# isns-server enable
```

The following example shows how to disable iSNS:

```
switch# config terminal
switch(config)# no isns-server enable
```

Related Commands

Command	Description
isns distribute	Enables iSNS distributed support.
isns esi retries	Configures ESI retry attempts.
isns profile name	Creates and configures iSNS profiles.
server	Configures iSNS server attributes.
show isns	Displays iSNS information.

ivr aam pre-deregister-check

To configure fabric precheck before deregistering IVR with AAM, use the **ivr aam pre-deregister-check** command in configuration mode.

ivr aam pre-deregister-check

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure precheck before deregistering IVR with AAM:

```
switch# config terminal
switch(config)# feature ivr
switch(config-if)# ivr distribute
switch(config-if)# ivr nat
switch(config-if)# ivr commit
switch(config-if)# ivr aam pre-deregister-check
switch(config-if)#
```

Related Commands

Command	Description
show ivr aam	Displays ivr aam status.

ivr aam register

To register IVR with AAM, use the **ivr aam register** command in configuration submode. To deregister IVR with AAM, use the **no** form of the command.

ivr aam register
no ivr aam register

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to register IVR with AAM:

```
switch# config terminal
switch(config)# feature ivr
switch(config-if)# ivr distribute
switch(config-if)# ivr nat
switch(config-if)# ivr commit
switch(config-if)# ivr aam register
switch(config-if)# 2009 Oct 20 22:12:32 isola-77 last message repeated 7 times
```

The following example shows how to deregister IVR with AAM:

```
switch# config terminal
switch(config)# feature ivr
switch(config-if)# ivr distribute
switch(config-if)# ivr nat
switch(config-if)# ivr commit
switch(config-if)# ivr aam pre-deregister-check
switch(config)# no ivr aam register

You could use "show ivr aam pre-deregister-check" to check pre-deregister status
.If the status indicates a failure, but you still go ahead with the commitment, t
he deregister might fail.
switch(config)#
```

Related Commands

Command	Description
show ivr aam	Displays IVR AAM status.

ivr abort

To discard an Inter-VSAN Routing (IVR) CFS distribution session in progress, use the **ivr abort** command in configuration mode.

ivr abort

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to discard an IVR CFS distribution session in progress:

```
switch# config terminal
switch(config)# ivr abort
```

Related Commands

Command	Description
ivr distribute	Enables CFS distribution for IVR.
show ivr	Displays IVR CFS distribution status and other details.

ivr commit

To apply the pending configuration pertaining to the Inter-VSAN Routing (IVR) Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **ivr commit** command in configuration mode.

ivr commit

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to apply an IVR configuration to the switches in the fabric:

```
switch# config terminal
switch(config)# ivr commit
```

Related Commands

Command	Description
ivr distribute	Enables CFS distribution for IVR.
show ivr	Displays IVR CFS distribution status and other details.

ivr copy active-service-group user-configured-service-group

To copy the active service group to the user-configured service group, use the **ivr copy active-service-group user-configured-service-group** command in EXEC mode.

ivr copy active-service-group user-configured-service-group

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example copies the active service group to the user-defined service group:

```
switch# ivr copy active-service-group user-configured-service-group
Successfully copied active service group to user-configured service group database
```

Related Commands

Command	Description
clear ivr service-group database	Clears the IVR service group database.
show ivr service-group	Displays IVR service groups.

ivr copy active-topology user-configured-topology

To copy the active inter-VSAN routing (IVR) VSAN topology to the user configured topology, use the **ivr copy active-topology user-configured-topology** command in EXEC mode.

ivr copy active-topology user-configured-topology

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The **ivr copy active-topology user-configured-topology** command is useful if you need to edit the active IVR topology, which is not allowed. Instead you copy the active IVR topology to the user configured topology, and then edit the user configured topology.

Examples

The following example copies the active IVR topology to the user configured topology:

```
switch# ivr copy active-topology user-configured-topology

Successfully copied active VSAN-topology to user-configured topology database
```

Related Commands

Command	Description
ivr copy active-zoneset full-zoneset	Copies the active zone set to the full zone set.
ivr copy auto-topology user-configured topology	Copies the automatically discovered inter-VSAN routing (IVR) VSAN topology to the user configured topology.
show ivr vsan topology	Displays the IVR VSAN topology configuration.

ivr copy active-zoneset full-zoneset

To copy the active zone set to the full zone set, use the **ivr copy active-zoneset full-zoneset** command in EXEC mode.

ivr copy active-zoneset full-zoneset

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Copying the active zone set to the full zone set may overwrite common zone and zone set configurations in the full zoning database.

Examples

The following example copies the active zone set to the full zone set:

```
switch# ivr copy active-zoneset full-zoneset

WARNING: This command may overwrite common zones/zonesets
         in the IVR full zoneset database
Please enter yes to proceed.(y/n) [n]?
```

Related Commands

Command	Description
ivr copy active-topology user-configured topology	Copies the active inter-VSAN routing (IVR) VSAN topology to the user configured topology.
ivr copy auto-topology user-configure topology	Copies the automatically discovered inter-VSAN routing (IVR) VSAN topology to the user configured topology.
show ivr zoneset active	Displays the active IVR zone set.

ivr copy auto-topology user-configured-topology

To copy the automatically discovered inter-VSAN routing (IVR) VSAN topology to the user configured topology, use the **ivr copy auto-topology user-configured-topology** command in EXEC mode.

ivr copy auto-topology user-configured-topology

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC configuration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

After using the **ivr copy auto-topology user-configured-topology** command to copy the automatically discovered VSAN topology into the user- configured topology you must use the **ivr commit** command to apply the pending configuration changes to the IVR topology using Cisco Fabric Services (CFS) distribution.

Examples

The following example copies the automatically discovered VSAN topology into the user configured topology:

```
switch# ivr copy auto-topology user-configured-topology
```

Related Commands

Command	Description
ivr commit	Applies the changes to the IVR topology.
ivr copy active-topology user-configured topology	Copies the active inter-VSAN routing (IVR) VSAN topology to the user configured topology.
ivr copy active-zoneset full-zoneset	Copies the active zone set to the full zone set.
show ivr vsan topology	Displays the IVR VSAN topology configuration .

ivr distribute

To enable Cisco Fabric Services (CFS) distribution for Inter-VSAN Routing (IVR), use the **ivr distribute** command. To disable this feature, use the **no** form of the command.

ivr distribute
no ivr distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable IVR fabric distribution:

```
switch# config terminal
switch(config)# ivr distribute
```

Related Commands

Command	Description
ivr commit	Commits temporary IVR configuration changes to the active configuration.
show ivr	Displays IVR CFS distribution status and other details.

ivr enable

To enable the Inter-VSAN Routing (IVR) feature, use the **ivr enable** command in configuration mode. To disable this feature, use the **no** form of the command.

ivr enable
no ivr enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
NX-OS 4.1(1b)	This command was deprecated.

Usage Guidelines

The IVR feature must be enabled in all edge switches in the fabric that participate in the IVR.

The configuration and display commands for the IVR feature are only available when IVR is enabled on a switch.

When you disable this configuration, all related configurations are automatically discarded.

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 command enters the configuration mode and enables the IVR feature on this switch:

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

Related Commands

Command	Description
show ivr	Displays IVR feature information.

ivr fcdomain database autonomous-fabric-num

To create IVR persistent FC IDs, use the **ivr fcdomain database autonomous-fabric-num** command. To delete the IVR fcdomain entry for a given AFID and VSAN, use the **no** form of the command.

ivr fcdomain database autonomous-fabric-num *afid-num* **vsan** *vsan-id*
no ivr fcdomain database autonomous-fabric-num *afid-num* **vsan** *vsan-id*

Syntax Description

afid-num	Specifies the current AFID. The range is 1 to 64.
vsan *vsan-id*	Specifies the current VSAN. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

This configuration only takes effect when NAT mode is enabled.

Examples

The following example shows how to enter IVR fcdomain database configuration submode for AFID 10 and VSAN 20:

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config) fcdomain#
```

The following example shows how to delete all persistent FC ID database entries for AFID 10 and VSAN 20:

```
switch# config t
switch(config)# no ivr fcdomain database autonomous-fabric-num 10 vsan 20
```

Related Commands

Command	Description
show ivr fcdomain database	Displays IVR fcdomain database entry information.

ivr nat

To explicitly enable Network Address Translation (NAT) functionality for Inter-VSAN Routing (IVR), use the **ivr nat** command in configuration mode. To disable this feature, use the **no** form of the command.

ivr nat
no ivr nat

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

The **ivr nat** command allows you to explicitly enable NAT functionality of IVR. Upgrading to SAN-OS Release 2.x from SAN-OS Release 1.3.x does not automatically enable the Fibre Channel NAT functionality. This command also allows you to continue to operate in non-NAT mode even in SAN-OS Release 2.x and later and NX-OS.

Note You might need to operate in non-NAT mode to support proprietary protocols that embed FCIDs in the frame payloads.

Examples

The following example shows how to explicitly enable NAT functionality for IVR:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr nat
```

Related Commands

Command	Description
show ivr	Displays IVR feature information.

ivr refresh

To refresh devices being advertised by Inter-VSAN Routing (IVR), use the **ivr refresh** command in EXEC mode.

ivr refresh

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(2)	This command was introduced.

Usage Guidelines

The **IVR refresh** command runs internally when IVR zone set or topology is activated. The limit for the maximum number of IVR zones per VSAN is 250 zones (two members per zone).

Examples

The following example shows refresh devices being advertised by IVR:

```
switch# ivr refresh
```

Related Commands

Command	Description
ivr enable	Enables the Inter-VSAN Routing (IVR) feature.
ivr withdraw domain	Withdraws an overlapping virtual domain from a specified VSAN.

ivr service-group activate

To activate an inter-VSAN routing (IVR) service group, use the **ivr service-group activate** command in configuration mode. To disable this feature, use the **no** form of the command.

ivr service-group activate [**default-sg-deny**]
no ivr service-group activate [**default-sg-deny**]

Syntax Description

default-sg-deny	(Optional) Sets the policy to deny for the default service group.

Command Default

Deactivated.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You must activate a configured IVR service group for the IVR service group to take effect. Once a configured IVR service group is activated, it replaces the currently activated service group, if there is one.

Activating an IVR service group with the **default-sg-deny** option sets the default service group policy to deny. To change the default service group policy to allow, issue the **ivr service-group activate** command again, but without the **default-sg-deny** option.

Examples

The following example activates the default IVR service group:

```
switch# config terminal
switch(config)# ivr service-group activate
```

The following example sets the default IVR service group policy to deny:

```
switch# config terminal
switch(config)# ivr service-group activate default-sg-deny
```

The following example disables the default service group:

```
switch# config terminal
switch(config)# no ivr service-group activate
```

Related Commands

Command	Description
ivr enable	Enables inter-VSAN routing (IVR).
ivr service-group name	Configures an inter-VSAN routing (IVR) service group.
show ivr service-group database	Displays an inter-VSAN routing service group database.

ivr service-group name

To configure an Inter-VSAN Routing (IVR) service group, use the **ivr service-group name**command in configuration mode. To disable this feature, use the **no** form of the command.

ivr service-group name *service-group*
no ivr service-group name *service-group*

Syntax Description

service-group	Specifies the service group name.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

In a complex network topology, you might only have a few IVR-enabled VSANs. To reduce the amount of traffic to non-IVR-enabled VSANs, you can configure a service group that restricts the traffic to the IVR-enabled VSANs. A service group is a combination of AFIDs and VSANs. Up to 16 service groups can be configured. A VSAN or AFID can belong to just one service group. When a new IVR-enabled switch is added to the network, you must update the service group to include the new VSANs.

There can be a maximum of 128 AFID/VSAN combinations in all service group. However, all 128 combinations can be in one service group.

The default service group ID is 0. The default service group is for all VSANs that are not a part of a user-defined service group.

Before configuring an IVR service group, you must enable the following:

- IVR using the **ivr commit** command
- IVR distribution using the **ivr commit** command
- Automatic IVR topology discovery using the **ivr commit auto command.**

Using the **autonomous-fabric-id (IVR topology database configuration)** command, you can restrict the IVR traffic to the AFIDs and VSANs configured in the service group.

Examples

The following example shows how to configure an IVR service group and change to IVR service group configuration mode:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr enable
switch(config)# ivr vsan-topology auto
switch(config)# ivr service-group name serviceGroup1
switch(config-ivr-sg)#
```

Related Commands

Command	Description
ivr enable	Enables the Inter-VSAN Routing (IVR) feature
ivr vsan-topology auto	Enables automatic discovery of the IVR topology.
show ivr	Displays IVR feature information.

ivr virtual-fcdomain-add

To add the Inter-VSAN Routing (IVR) virtual domains in a specific VSAN(s) to the assigned domains list in that VSAN, use the **ivr virtual-fcdomain-add** command. To delete the IVR virtual domains, use the **no** form of the command.

ivr virtual-fcdomain-add vsan-ranges *vsan-range*
no ivr virtual-fcdomain-add vsan-ranges *vsan-range*

Syntax Description

vsan-ranges *vsan-range*	Specifies the IVR VSANs or range of VSANs. The range of values for a VSAN ID is 1 to 4093.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

Use the **no ivr virtual-fcdomain-add** command to remove the currently active domains from the fcdomain manager list in a specified VSAN.

Examples

The following command adds the IVR virtual domains in VSAN:

```
switch# config terminal
switch(config)# ivr virtual-fcdomain-add vsan-ranges 1
```

The following command reverts to the factory default of not adding IVR virtual domains:

```
switch# config terminal
switch(config)# ivr virtual-fcdomain-add vsan-ranges 1
```

Related Commands

Command	Description
ivr withdraw domain	Removes overlapping domains.
show ivr virtual-fcdomain-add-status	Displays the configured VSAN topology for a fabric.

ivr virtual-fcdomain-add2

To configure the request domain_ID (RDI) mode in a specific autonomous fabric ID (AFID) and VSAN for all IVR-enabled switches, use the **ivr virtual-fcdomain-add2** command. To delete the RDI mode, use the **no** form of the command.

ivr virtual-fcdomain-add2 autonomous-fabric-id *value* **vsan-ranges** *value*
no ivr virtual-fcdomain-add2 autonomous-fabric-id *value* **vsan-ranges** *value*

Syntax Description

fabric-id *value*	Specifies the fabric ID on which the RDI mode needs to be configured.
vsan-ranges *value*	Specifies the VSAN range value on which the RDI mode needs to be configured.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

This is a CFS distributable command.

Examples

The following example configures the RDI mode on a specific AFID and VSAN:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch# ivr virtual-fcdomain-add2 autonomous-fabric-id 1 vsan-ranges 2
switch# fabric is now locked for configuration. Please 'commit' configuration when done.
switch(config)# ivr commit
```

Related Commands

Command	Description
show ivr virtual-fcdomain-add-status2	Displays the RDI mode in a specific AFID and VSAN for all IVR-enabled switches.

ivr vsan-topology

To configure manual or automatic discovery of the Inter-VSAN Routing (IVR) topology, use the **ivr vsan-topology** command in configuration mode.

ivr vsan-topology {**activate**|**auto**}

Syntax Description

activate	Configures manual discovery of the IVR topology and disables automatic discovery mode.
auto	Configures automatic discovery of the IVR topology.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.1(1a)	Added **auto** keyword.

Usage Guidelines

To use this command you must first enable IVR using the **ivr enable** command and configure the IVR database using the **ivr vsan-topology database** command.

Caution Active IVR topologies cannot be deactivated. You can only switch to automatic topology discovery mode.

Examples

The following **ivr vsan-topology activate** command activates the VSAN topology database:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr enable
switch(config)# ivr vsan-topology database
switch(config-ivr-topology-db)# autonomous-fabric-id 1 switch 20:00:00:00:30:00:3c:5e
vsan-ranges 2,2000
switch(config)# ivr vsan-topology activate
```

The following command enables VSAN topology database auto mode, which allows the switch to automatically discover the IVR topology:

```
switch(config)# ivr vsan-topology auto
```

Related Commands

Command	Description
autonomous-fabric-id(IVR topology database configuration)	Configure an autonomous phobic ID into the IVR topology database.

Command	Description
ivr enable	Enables the Inter-VSAN Routing (IVR) feature.
show ivr	Displays IVR feature information.

ivr vsan-topology auto

To configure automatic discovery of the Inter-VSAN Routing (IVR) topology, use the **ivr vsan-topology auto** command in configuration mode.

ivr vsan-topology auto

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

To use this command you must first enable IVR using the **ivr enable** command.

IVR configuration distribution must be enabled using the **ivr distribute** command before configuring automatic topology discovery. Once automatic IVR topology discovery is enabled, you cannot disable IVR configuration distribution.

Examples

The following command enables VSAN topology database auto mode, which allows the switch to automatically discover the IVR topology.

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

  activate  Activate VSAN topology database for inter-VSAN routing
  auto      Enable discovery of VSAN topology for inter-VSAN routing
  database  Configure VSAN topology database for inter-VSAN routing
switch(config)# ivr vsan-topology auto
switch(config)#
```

Related Commands

Command	Description
ivr enable	Enables the Inter-VSAN Routing (IVR) feature.
autonomous-fabric-id (IVR topology database configuration)	Configure an autonomous phobic ID into the IVR topology database
show ivr	Displays IVR feature information.

ivr vsan-topology database

To configure an Inter-VSAN Routing (IVR) topology database, use the **ivr vsan-topology database** command in configuration mode. To delete an IVR topology database, use the **no** form of the command.

ivr vsan-topology database
no ivr vsan-topology database

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

To use this command you must first enable IVR using the **ivr enable** command.

You can have up to 64 VSANs (or 128 VSANs as of Cisco MDS SAN-OS Release 2.1(1a)) in an IVR topology. Specify the IVR topology using the following information:

- The switch WWNs of the IVR-enabled switches.
- A minimum of two VSANs to which the IVR-enabled switch belongs.
- The autonomous fabric ID (AFID), which distinguishes two VSANs that are logically and physically separate, but have the same VSAN number. Cisco MDS SAN-OS Release 1.3(1) and later NX-OS supports only one default AFID (AFID 1) and thus does not support non-unique VSAN IDs in the network. As of Cisco MDS SAN-OS Release 2.1(1a), you can specify up to 64 AFIDs.

Note The use of a single AFID does not allow for VSANs that are logically and physically separate but have the same VSAN number in an IVR topology.

Caution You can only configure a maximum of 128 IVR-enabled switches and 64 distinct VSANs (or 128 distinct VSANs as of Cisco MDS SAN-OS Release 2.1(1a)) in an IVR topology.

The **no ivr vsan-topology database** command only clears the configured database, not the active database. You can only delete the user-defined entries in the configured database. Auto mode entries only exist in the active database.

Examples

The following command enters configuration mode, enables the IVR feature, enters the VSAN topology database, and configures the pWWN-VSAN association for VSANs 2 and 2000:

```
switch# config terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr enable
switch(config)# ivr vsan-topology database
switch(config-ivr-topology-db)# autonomous-fabric-id 1 switch 20:00:00:00:30:00:3c:5e
vsan-ranges 2,2000
```

Related Commands

Command	Description
autonomous0fabric-id(IVR topology database configuration)	Configures an autonomous phobic ID into the IVR topology database
ivr enable	Enables the Inter-VSAN Routing (IVR) feature.
show ivr	Displays IVR feature information.

ivr withdraw domain

To withdraw overlapping virtual domain from a specified VSAN, use the **ivr withdraw domain** command in EXEC mode.

ivr withdraw domain *domain-id* **vsan** *vsan-id*

Syntax Description

domain-id	Specifies the domain id. The range is 1 to 239.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

When you enable the **ivr virtual-fcdomain-add** command, links may fail to come up due to overlapping virtual domain identifiers. If so, temporarily withdraw the overlapping virtual domain from that VSAN using the **ivr withdraw domain** command in EXEC mode.

Examples

The following command withdraws overlapping domains:

```
switch# ivr withdraw domain 10 vsan 20
```

Related Commands

Command	Description
show ivr virtual-fcdomain-add-status	Displays the configured VSAN topology for a fabric.

ivr zone name

To configure a zone for Inter-VSAN Routing (IVR), use the **ivr zone name** command. To disable a zone for IVR, use the **no** form of the command.

ivr zone name *ivzs-name*
no ivr zone name *ivz-name*

Syntax Description

ivz-name	Specifies the IVZ name. Maximum length is 59 characters.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

This command enters IVR zone configuration submode.

Examples

The following command enters the configuration mode, enables the IVR feature, creates an IVZ, and adds a pWWN-VSAN member:

```
switch# config terminal
switch(config)# ivr enable
switch(config)# ivr zone name Ivz_vsan2-3
switch(config-ivr-zone)# member pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
```

Related Commands

Command	Description
show ivr	Displays IVR feature information.

ivr zone rename

To rename an inter-VSAN routing (IVR) zone, use the **ivr zone rename** command.

ivr zone rename *current-name new-name*

Syntax Description

current-name	Specifies the current zone name. The maximum size is 64 characters.
new-name	Specifies the new zone name. The maximum size is 64 characters.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example renames the IVR zone from *east* to *west:*

```
switch# ivr zone rename east west
```

Related Commands

Command	Description
ivr zone name	Creates and configures an IVR zone.
show ivr	Displays IVR information.

ivr zoneset

To configure a zoneset for Inter-VSAN Routing (IVR), use the **ivr zoneset** command. To revert to the factory defaults, use the **no** form of the command.

ivr zoneset {**activate name** *ivzs-name* **[force]**|**name** *ivzs-name*}
no ivr zoneset {**activate name** *ivzs-name* **[force]**|**name** *ivzs-name*}

Syntax Description

activate	Activates a previously configured IVZS.
force	(Optional) Forces a IVZS activation
name *ivzs-name*	Specifies the IVZS name. Maximum length is 59 characters.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

This command enters IVR zoneset configuration submode.

Note To replace the active IVR zone set with a new IVR zone set without disrupting traffic, activate the new IVR zone set without deactivating the current active IVR zone set.

Examples

The following command enters the configuration mode, enables the IVR feature, creates an IVZS, adds a IVZ member, and activates the IVZS:

```
switch# config terminal
switch(config)# ivr enable
switch(config)# ivr zoneset name Ivr_zoneset1
switch(config-ivr-zoneset)# member Ivz_vsan2-3
switch(config-ivr-zoneset)# exit
switch(config)# ivr zoneset activate name IVR_ZoneSet1
```

Related Commands

Command	Description
show ivr	Displays IVR feature information.

ivr zoneset rename

To rename an inter-VSAN routing (IVR) zone set, use the **ivr zoneset rename** command.

ivr zoneset rename *current-name new-name*

Syntax Description

current-name	Specifies the current zone set name. The maximum size is 64 characters.
new-name	Specifies the new zone set name. The maximum size is 64 characters.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example renames the IVR zone set from *north* to *south:*

```
switch# ivr zoneset rename north south
```

Related Commands

Command	Description
ivr zoneset name	Creates and configures an IVR zone set.
show ivr	Displays IVR information.

J Commands

job name

To assign a job to a command schedule, use the **job name** command**.** To remove the job, use the **no** form of the command.

job name *job-name*
no job name *job-name*

Syntax Description

job-name	Specifies the job name for the command schedule to run.

Command Default

None.

Command Modes

Scheduler schedule configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, the command scheduler must be enabled using the **scheduler enable** command.

You can configure multiple jobs in a command schedule.

Examples

The following example shows how to specified the job for a command schedule:

```
switch# config terminal
switch(config)# scheduler schedule name MySchedule
switch(config-schedule)# job name MyJob
```

Related Commands

Command	Description
scheduler enable	Enables the command scheduler.
scheduler schedule name	Configures a schedule for the command scheduler.
show scheduler	Displays scheduler information.

K Commands

keepalive

To configure the message keepalive interval for the IKE protocol, use the **keepalive** command in IKE configuration submode. To revert to the default, use the **no** form of the command.

keepalive *seconds*
no keepalive *seconds*

Syntax Description

seconds	Specifies the number of seconds for the keepalive interval. The range is 120 to 86400.

Command Default

3600 seconds or 1 hour.

Command Modes

IKE configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

The keepalive interface only applies to IKE version 2 tunnels.

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Examples

The following example shows how to configure the keepalive interval:

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# keepalive 7200
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

kernel core

Use the **kernel core** command to generate a core dump for each module. Use the **no** form of this command to negate the command or revert to its factory

kernelcore{**limit***number*|**module***slot*{**force**|**level**{**all**|**header**|**kernel**|**ram**|**used-ram**}|**target***ipaddress*}}
nokernelcore{**limit***number*|**module***slot*{**force**|**level**{**all**|**header**|**kernel**|**ram**|**used-ram**}|**target***ipaddress*}}

Syntax Description

limit *number*	Limits the number of modules for which the core is generated. The range is 1 to 6.
module *slot*	Configures the module requiring the core generation.
force	Forces a module to dump kernel core.
level	Specifies the core dump level for the selected module.
all	Dumps all the memory (requires 1G of space)
header	Dumps kernel header only.
kernel	Dumps all kernel memory pages.
ram	Dumps all the RAM pages.
used-ram	Dumps all the used RAM pages.
target *ipaddress*	Configures the external server IP address on the same physical LAN.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Core dumps performed on the supervisor module can lead to packet loss, even in a dual supervisor configuration.

Examples

The following example limits core generation to two modules:

```
switch(config)# kernel core limit 2
succeeded
```

The following example configures module 5 to generate cores:

```
switch(config)# kernel core module 5
succeeded
```

The following example configures module 5 to generate only header-level cores:

```
switch(config)# kernel core module 5 level header
succeeded
```

The following example configures the external server:

```
switch(config)# kernel core target 10.50.5.5
succeeded
```

Related Commands

Command	Description
show kernel	Displays configured kernel core settings.
show running-config	Displays all switch configurations saved to PSS.

key

To configure the preshared key for the IKE protocol, use the **key** command in IKE configuration submode. To revert to the default, use the **no** form of the command.

key *key-id* { **address** *ip-address* | **hostname** *name* }
no **key** *key-id* { **address** *ip-address* | **hostname** *name* }

Syntax Description

key-id	Specifies the ID for the preshared key. The maximum length is 128 characters.
address *ip-address*	Specifies the peer IP address. The format is *A* . *B* . *C* . *D* .
hostname *name*	Specifies the peer host name. The maximum length is 128 characters.

Command Default

None.

Command Modes

IKE configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.
3.0(1)	Added the **hostname** keyword.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Note The **key** command supports only the IPv4 format for IP address.

Examples

The following example shows how to configure the key:

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# key ctct address 209.165.200.226
```

The following example shows how to delete the configured key:

```
switch(config-ike-ipsec)# no key ctct address 209.165.200.226
```

The following example shows how to set the preshared key for the specified peer:

```
switch(config-ike-ipsec)# key sample hostname node1
```

The following example shows how to delete the preshared key for the specified peer:

```
switch(config-ike-ipsec)# no key sample hostname node1
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

key (sa configuration submode)

To configure the key for the current Security Association[SA], use the key command. To delete the key from the current SA, use the no form of the command.

key *key*
no key *key*

Syntax Description

key	Specifies the key for encryption as a 16-byte hexadecimal string. The maximum size of the string is 34.

Command Default

None.

Command Modes

Configuration submode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure the key 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)# key 0x1234
switch(config-sa)#
```

Related Commands

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

key-ontape

To configure keys on the tape mode and store the encrypted security keys on the backup tapes, use the key-ontape command. To disable this feature, use the no form of the command.

key-ontape
no key-ontape

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Cisco SME cluster configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

This command allows the encrypted security keys to be stored on the backup tapes.

Note This feature is supported only for unique keys.

Before using this command, automatic volume grouping should be disabled by using the auto-volgrp command.

Examples

The following example enables the key-ontape feature:

```
switch# config terminal
switch(config)# sme cluster clustername1
switch(config-sme-cl)# key-ontape
```

The following example disables the key-ontape feature:

```
switch# config terminal
switch(config)# sme cluster clustername1
switch(config-sme0-cl)# no key-ontape
```

Related Commands

Command	Description
no shared-key	Specifies unique key mode.
no auto-volgrp	Disables automatic volume grouping.
show sme cluster key	Displays information about cluster key database.
show sme cluster tape	Displays information about tapes.

L Commands

ldap search-map

To configure a search map, use the ldap search-map command. To disable this feature, use the no form of the command.

ldap search-map *map-name*
no ldap search-map *map-name*

Syntax Description

map-name	Specifies the name of the search map. The maximum length is 128 characters.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to specify the LDAP search mapping table:

```
switch(config)# ldap search-map map1
switch(config-ldap-search-map)#
```

Related Commands

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

ldap-search-map

To attach the configured LDAP search map to the group, use the ldap search-map command. To disable this feature, use the no form of the command.

ldap-search-map *map-name*
no ldap-search-map *map-name*

Syntax Description

map- name	Specifies the name of the search map. The maximum length is 128 characters.

Command Default

None.

Command Modes

Configuration submode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure the name of the LDAP search mapping table:

```
switch(config)# ldap search-map map1
switch(config-ldap)#
```

Related Commands

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

ldap-server deadtime

To configure global LDAP server deadtime period in seconds, use the **ldap-server deadtime** command To disable this feature, use the no form of the command.

ldap-server deadtime *minutes*
no ldap-server deadtime *minutes*

Syntax Description

minutes	Specifies LDAP server deadtime period in minutes. The range is from 1 to 60 minutes. Default is 5 minutes.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure global LDAP server deadtime period in seconds:

```
switch(config)# ldap-server deadtime 5
switch(config)#
```

Related Commands

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

ldap-server host

To configure global LDAP server IP address, use the ldap-server host command in configuration mode. To disable this feature, use the no form of the command.

{**ldap-server host** {**server-name**|**ip-address**} **enable-ssl**|[**port port number**] [**timeout timeout in seconds**]|**rootDN rootDN password** [{**7 password**|**password**}] [**port port number**] [**timeout timeout in seconds**]|**test rootDN DN string** [**username user-name**] [**password** [{**7 password**|**password**}]] [**idle-time n**]}
{**no ldap-server host** {**server-name**|**ip-address**} **enable-ssl**|[**port port number**] [**timeout timeout in seconds**]|**rootDN rootDN password** [{**7 password**|**password**}] [**port port number**] [**timeout timeout in seconds**]|**test rootDN DN string** [**username user-name**] [**password** [{**7 password**|**password**}]] [**idle-time n**]}

Syntax Description

server-name	Specifies LDAP server DNS name. The maximum length is 255 characters.
ip-address	Specifies LDAP server IP address.
enable-ssl	Specifies LDAP server, enable SSL.
port	Specifies LDAP server port.
port-number	Specifies port number. The range is from 1 to 65535.
root DN	Specifies LDAP rootDN for the LDAP server database.
rootDN	The maximum length is 63 characters and default is empty string.
password 7 *pasword*	Specifies encrypted bind password for root. The maximum length is 63 characters and default is empty string.
password *password*	Specifies bind password for root. The maximum length is 63 characters and default is empty string
test rootDN *DN string*	Specifies the test keyword which turns on automated testing for the feature. The rootDN keyword is mandatory and is followed by the rootDN to be used to bind to ldap server to verify its state.
username *user-name*	Specifies the username that would be used to do a test bind.
password *password*	Specifies the password to be used in the packets. When a password cannot be obtained, the default of test is used for test packets.
idle-time *n*	Specifies the time for which the server has to remain idle before test packet(s) are sent out. If any of the responses are not received, the server is assumed dead. The default idle-time is 0, but can be configured as low as 1 minute.
timeout *timeout in seconds*	Specifies the timeout period to wait for a response from the server before client can declare a timeout failure. The range is from 1 to 60 seconds.

Command Default

Port -Globally configured value (“ldap-server port <>”), in absence of which a value of 389. Timeout- Globally configured value (“ldap-server timeout <>”), in absence of which a value of 5 seconds.

idle-time- Default is 0.

testrootDN-Default value dc=test, dc=com.

username- default value is test.

Password- For test commands default value is test.

Command Modes

Configuration submode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to Specify the test keyword turns on automated testing for the feature:

```
switch(config)# ldap-server host 10.64.66.140 test rootDN cn=Manager,dc=acme,dc=com user
test password secret idle-time 1
```

The following example shows how to enable TLS while connecting to the server:

```
switch(config)# ldap-server host 10.64.66.140 enable-ssl
switch(config)#
```

The following example shows how to configure LDAP server port:

```
switch(config)# ldap-server host 10.64.66.140 root DN cn=Manager, dc=acme, dc=com password
 secret port 389
switch(config)#
```

Related Commands

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

ldap-server port

To configure global LDAP server port, use the ldap-server port command in configuration mode. To disable this feature, use the no form of the command.

ldap-server port *port-number*

Syntax Description

port-number	Specifies port number. The range is from 1 to 65535.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure global LDAP server port:

```
switch(config)# no ldap-server port 65532
switch(config)#
```

Related Commands

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

ldap-server timeout

To configure global timeout period in seconds, use the ldap-server timeout command in configuration mode. To disable this feature, use the no form of the command.

ldap-server timeout *timeout in second*
no ldap-server timeout*timeout in second*

Syntax Description

timeout in seconds	Specifies timeout value in seconds. The default timeout value is 5 seconds and valid range is from 1 to 60 seconds. This value will be used only for those servers for which timeout is not configured at a per-server level.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure global LDAP server timeout in seconds:

```
switch(config)# no ldap-server timeout 1
switch(config)#
```

Related Commands

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

lifetime seconds

To configure the security association (SA) lifetime duration for an IKE protocol policy, use the **lifetime seconds** command in IKE policy configuration submode. To revert to the default, use the **no** form of the command.

lifetime seconds *seconds*
no lifetime seconds *seconds*

Syntax Description

seconds	Specifies the lifetime duration in seconds. The range is 600 to 86400.

Command Default

86,400 seconds.

Command Modes

IKE policy configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

The **lifetime seconds** command overrides the default.

Examples

The following example shows how to configure the SA lifetime duration for the IKE protocol:

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# policy 1
switch(config-ike-ipsec-policy)# lifetime seconds 6000
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
policy	Configures IKE protocol policy.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

line com1

To configure auxiliary COM 1 port, use the **line com1** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

line com1->databits *number* **|flowcontrol hardware|modem {in|init-string {default|user-input} |set-string user-input** *string*} **|parity {even|none|odd} |speed** *speed* **|stopbits {1|2}**
no line com1->databits *number* **|flowcontrol hardware|modem {in|init-string|set-string user-input} |parity {even|none|odd} |speed** *speed* **|stopbits {1|2}**

Syntax Description

databits *number*	Specifies the number of databits per character. The range is 5 to 8.
flowcontrol hardware	Enables modem flow on the COM1 port control.
modem	Enables the modem mode.
in	Enables the COM 1 port to only connect to a modem.
init-string default	Writes the default initialization string to the modem.
set-string user-input *string*	Sets the user-specified initilization string to its corresponding profile. Maximum length is 80 characters.
init-string user-default	Writes the provided initialization string to the modem.
parity	Sets terminal parity.
even	Sets even parity.
none	Sets no parity.
odd	Sets odd parity.
speed *speed*	Sets the transmit and receive speeds. The range is 110 to 115, 200 baud.
stopbits	Sets async line stopbits.
1	Sets one stop bit.
2	Sets two stop bits.

Command Default

9600 Baud

8 databits

1 stopbit

Parity none

Default init string

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(2)	This command was introduced.
3.0(1)	Added an example to show the user-input initialization string for the Supervisor-2 module.

Usage Guidelines

The **line com1** command available in config t command mode. The **line com1** configuration commands are available in **config-com1** submode.

You can perform the configuration specified in this section only if you are connected to the console port or the COM1 port.

We recommend you use the default initialization string. If the required options are not provided in the user-input string, the initialization string is not processed.

You must first set the user-input string before initializing the string.

Examples

The following example configures a line console and sets the options for that terminal line:

```
switch## config terminal
switch(config)#
switch(config)# line com1
switch(config-com1)# databits 6
switch(config-com1)# parity even
switch(config-com1)# stopbits 1
```

The following example disables the current modem from executing its functions:

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# no modem in
```

The following example enables (default) the COM1 port to only connect to a modem:

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# modem in
```

The following example writes the initialization string to the modem. This is the default.

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# modem init-string default
```

The following example assigns the user-specified initialization string for a Supervisor-1 module to its corresponding profile:

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# modem set-string user-input ATE0Q1&D2&C1S0=3\015
```

The following example assigns the user-specified initialization string for a Supervisor-2 module to its corresponding profile:

```
switch# config terminal
```

```
switch(config)# line com1
switch(config-com1)# modem set-string user-input ATE0Q0V1&D0&C0S0=1
```

The following example deletes the configured initialization string:

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# no modem set-string user-input ATE0Q1&D2&C1S0=3\015
```

The following example writes the user-specified initialization string to the modem:

```
switch# config terminal
switch(config)# line com1
switch(config-com1)# modem init-string user-input
```

Related Commands

Command	Description
line console	Configures primary terminal line.
line vty	Configures virtual terminal line.
show line com1	Displays COM1 information.

line console

To configure a terminal line, use the **line console** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

lineconsole->databits*number*|**exec-timeout***minutes*|**modem**
{**in**|**init-string**|**set-stringuser-inputstring**}|**parity**{**even**|**none**|**odd**}|**speed***speed*|**stopbits**{**1**|**2**}
nolineconsoledatabits
number|**exec-timeout***minutes*|**modem**{**in**|**init-string**{**default**|**user-input**}|**set-stringuser-input***string*}|**parity**{**even**|**none**|**odd**}|**speed***speed*|**stopbits**{**1**|**2**}

Syntax Description

databits *number*	Specifies the number of databits per character. The range is 5 to 8.
exec-timeout *minutes*	Configures exec timeout in minutes. The range is 0 to 525,600. To disable, set to 0 minutes.
modem	Enables the modem mode.
in	Enables the COM 1 port to only connect to a modem.
init-string default	Writes the default initialization string to the modem.
init-string user-input	Writes the provided initialization string to the modem.
set-string user-input *string*	Sets the user-specified initilization string to its corresponding profile. Maximum length is 80 characters.
parity	Sets terminal parity.
even	Sets even parity.
none	Sets no parity.
odd	Sets odd parity.
speed *speed*	Sets the transmit and receive speeds. Valid values for Supervisor-1 modules are between 110 and 115,200 bps (110, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, 28800, 38400, 57600, 115200). Valid values for Supervisor-2 modules are 9600, 19200, 38400, and 115200.
stopbits	Sets async line stopbits.
1	Sets one stop bit.
2	Sets two stop bits.

Command Default

9600 Baud.

8 databits.

1 stopbit.

Parity none.

Default init string.

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(2)	This command was introduced.
3.0(1)	Modified the **speed** option by specifying speeds for the Supervisor-1 module and Supervisor-2 module.

Usage Guidelines

The **line console** command available in config t command mode. The **line console** configuration commands are available in config-console submode.

When setting the **speed** option, be sure to specify one of the exact values.

Examples

The following example configures a line console and sets the options for that terminal line:

```
switch## config terminal
switch(config)##
switch(config)# line console
switch(config-console)# databits 60
switch(config-console)# exec-timeout 60
switch(config-console)#

flowcontrol software
switch(config-console)# parity even
switch(config-console)# stopbits 1
```

The following example disables the current modem from executing its functions:

```
switch# config terminal
switch(config)# line console
switch(config-console)# no modem in
```

The following example enables (default) the COM1 port to only connect to a modem:

```
switch# config terminal
switch(config)# line console
switch(config-console)# modem in
```

The following example writes the initialization string to the modem. This is the default.

```
switch# config terminal
switch(config)# line console
switch(config-console)# modem init-string default
```

The following example assigns the user-specified initialization string to its corresponding profile:

```
switch# config terminal
switch(config)# line console
switch(config-console)# modem set-string user-input ATE0Q1&D2&C1S0=3\015
```

The following example deletes the configured initialization string:

```
switch# config terminal
```

```
switch(config)# line console
switch(config-console)# no modem set-string user-input ATE0Q1&D2&C1S0=3\015
```

The following example writes the user-specified initialization string to the modem:

```
switch# config terminal
switch(config)# line console
switch(config-console)# modem init-string user-input
```

Related Commands

Command	Description
line com1	Configures the auxiliary COM 1 port
line vty	Configures virtual terminal line.
show line console	Displays console information.

line vty

To configure a virtual terminal line, use the **line vty** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

linevty->exec-timeout*minutes*|**session-limit***number*
nolinevtyexec-timeout|**session-limit***number*

Syntax Description

exec-timeout *minutes*	Configures timeout in minutes. The range is 0 to 525600. To disable, set to 0 minutes.
session-limit *number*	Configures the number of VSH sessions. The range is 1 to 64.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The **line vty** command is available in config t command mode. The **line vty** configuration commands are available in config-line submode.

Examples

The following example configures a virtual terminal line and sets the timeout for that line:

```
switch## config terminal
switch(config)# line vty
switch(config-line)# exec-timeout 60
```

Related Commands

Command	Description
line com1	Configures the auxiliary COM 1 port.
line console	Configures primary terminal line.

link (SDV virtual device configuration submode)

To link a virtual device to a real device, use the **link** command in SDV virtual device configuration submode. To remove a link, use the **no** form of the command.

link {**device-alias** *device-name*|**pwwn** *pwwn-name*}
no link {**device-alias** *device-name*|**pwwn** *pwwn-name*}

Syntax Description

device-alias *device-name*	Links a virtual device to a device alias.
pwwn *pwwn-name*	Links a virtual device to a pWWN. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.

Command Default

None.

Command Modes

SDV virtual device configuration submode.

Command History

Release	Modification
3.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to link a virtual device to a device alias:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# sdv virtual-device name sqa1 vsan 1
switch(config-sdv-virt-dev)# link device-alias sqa3
```

The following example shows how to link a virtual device to a pWWN:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# sdv virtual-device name sqa1 vsan 1
switch(config-sdv-virt-dev)# link pwwn 21:00:00:04:cf:cf:45:40
```

Related Commands

Command	Description
sdv enable	Enables or disables SAN device virtualization.
show sdv statistics	Displays SAN device virtualization statistics.

link-state-trap

To enable an SNMP link state trap on an interface, use the **link-state-trap** command in interface configuration submode. To disable an SNMP link state trap, use the **no** form of the command.

link-state-trap
no link-state-trap

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
3.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable an SNMP link state trap on interface bay2:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface bay 2
switch(config-if)# link-state-trap
```

The following example shows how to disable an SNMP link state trap on interface bay2:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface bay 2
switch(config-if)# no link-state-trap
```

Related Commands

Command	Description
show interface	Displays interface information.

link-state-trap (SME)

To enable an Simple Network Management Protocol (SNMP) link state trap on an interface, use the link-state-trap command. To disable this feature, use the no form of the command.

link-state-trap
no link-state-trap

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable the link-state-trap on the Fibre Channel interface:

```
switch# config t
switch(config)# interface fc 1/1
switch(config-if)# link-state-trap
switch(config-if)#
```

The following example shows how to disable the link-state-trap on the Fibre Channel interface:

```
switch# config t
switch(config)# interface fc 1/1
switch(config-if)# no link-state-trap
switch(config-if)#
```

Related Commands

Command	Description
show interface	Displays interface information.

load-balancing

To enable cluster reload balancing for all targets or specific targets, use the load-balancing command. To disable this command, use the no form of the command.

load-balancing {**enable**|*target wwn* }
no load-balancing {**enable**|*target wwn* }

Syntax Description

enable	Enables cluster load balancing.
target *wwn*	Specifies the world-wide name (WWN) of the target port.

Command Default

None.

Command Modes

Cisco SME cluster configuration submode.

Command History

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

Usage Guidelines

The reload balancing operation is performed by the Cisco SME administrator for all or specific target ports. This operation first unbinds all the targets from the Cisco SME interfaces. The targets are then associated, one at a time, based on the load-balancing algorithm.

The reload balancing operation can be triggered if the targets remain unconnected due to errors in the prior load balancing opertions in the backend.

Examples

The following example enables reload balancing in Cisco SME:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# load-balancing enable
switch(config-sme-cl-node)#
```

The following example adds the host to the Cisco SME interface based on the load-balancing policy:

```
switch# config t
switch(config))# sme cluster c1
switch(config-sme-cl)# load-balancing 17:11:34:44:44:12:14:10
switch(config-sme-cl-node)#
```

Related Commands

Command	Description
show sme cluster	Displays Cisco SME information.

load-balancing (Cisco IOA cluster Configuration submode)

To enable cluster reload balancing of all flows in an IOA cluster, use the load-balancing command.

load-balancing {**enable**|*target wwn* }
no load-balancing {**enable**|*target wwn* }

Syntax Description

enables	Enables cluster load balancing.
target *pwwn*	Specifies the world-wide name (WWN) of the target port.

Command Default

None.

Command Modes

Cisco IOA cluster 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 enable cluster reload balancing of all targets:

```
rtp-sw1(config)# ioa cluster tape_vault
rtp-sw1(config-ioa-cl)# load-balancing enable
switch#(config-ioa-cl)# load-balancing10:00:00:00:00:00:00:00
This command will first disable all the IT nexuses (only for a target if specifi
ed) and then enable them back. This process is disruptive. Also, in case you abo
rt the request in the middle, you can enable load balancing back by executing th
e command 'load-balancing enable'.
Do you wish to continue? (yes/no) [no] y
Cluster config fails: This switch is not the master switch, configuration change
 not allowed. (0x420f003c)
switch#(config-ioa-cl)#
```

Related Commands

Command	Description
interface ioa	Configures the IOA interface.

locator-led

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

locator-led {**chassis**|**fan** *f-number*|**module** *slot*|**powersupply** *ps-number*|**xbar** *x-number*}
no locator-led {**chassis**|**fan** *f-number*|**module** *slot*|**powersupply** *ps-number*|**xbar** *x-number*}

Syntax Description

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

Command Default

None

Command Modes

Any command mode

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

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

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

This command is available only in modular Cisco MDS switches.

Examples

This example shows how to blink the LED for module 4:

switch# **locator-led module 4**

Related Commands

Command	Description
show locator-led status	Displays the status of locator LEDs on the system.

logging abort

To discard the logging Cisco Fabric Services (CFS) distribution session in progress, use the **logging abort** command **in configuration mode.**

logging abort

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to discard logging CFS distribution session in progress:

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

Related Commands

Command	Description
show logging	Displays logging information.

logging commit

To apply the pending configuration pertaining to the logging Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **logging commit** command **in configuration mode.**

logging commit

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to commit changes to the active logging configuration:

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

Related Commands

Command	Description
show logging	Displays logging information.

logging console

To set console logging, use the **logging console** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

logging console [*severity-level*]
no logging console [*severity-level*]

Syntax Description

severity-level	(Optional) Specifies the maximum severity of messages logged. The range is 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.

Command Default

Disabled.

The default severity level is 2.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The switch logs messages at or above the configured severity level.

Examples

The following example reverts console logging to the factory set default severity level of 2 (critical). Logging messages with a severity level of 2 or above will be displayed on the console.

```
switch# config terminal
switch(config)# logging console 2
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging distribute

To enable Cisco Fabric Services (CFS) distribution for logging, use the **logging distribute** command. To disable this feature, use the **no** form of the command.

logging distribute
no logging distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to change the distribute logging configuration changes:

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

Related Commands

Command	Description
logging commit	Commits the logging configuration changes to the active configuration.
show logging	Displays logging information.

logging level

To modify message logging facilities, use the **logging level** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

logging level *facility-name severity-level*
no logging level *facility-name severity-level*

Syntax Description

facility-name	Specifies the required facility name (for example **acl**, or **ivr**, or **port**, etc.)
severity-level	Specifies the maximum severity of messages logged. The range is 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The switch logs messages at or above the configured severity level.

Examples

Configures Telnet or SSH logging for the kernel facility at level 4 (warning). As a result, logging messages with a severity level of 4 or above will be displayed:

```
switch# config terminal
switch(config)# logging level kernel 4
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging level port

To configure logging level for port syslog messages, use the **logging level port** command. To remove this configuration, use the **no** form of this command.

logging level port {*severity-level* | **link-failure** | {**critical** | **notif**}}

no logging level port {*severity-level* | **link-failure** | {**critical** | **notif**}}

Syntax Description

severity-level	Specifies the severity of messages logged. The range is from 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.
link-failure	Specifies logging level for port link failure syslog messages.
critical	Specifies that when an active link fails, the message that is issued is a critical level (2) message: %PORT-2-IF_DOWN_LINK_FAILURE_CRIT.
notif	Specifies that when an active link fails, the message that is issued is a notification level (5) message: %PORT-5-IF_DOWN_LINK_FAILURE.

Command Default

The default severity is the notification level (5).

Command Modes

Configuration mode (config)

Command History

Release	Modification
1.3(1)	This command was introduced.

Examples

The following example displays how to configure Telnet or SSH logging for port at level 4 (warning). As a result, logging messages with a severity level of 4 or above will be displayed:

```
switch# configure
switch(config)# logging level port 4
```

The following example displays how to configure Telnet or SSH logging for critical port link failure messages. As a result, logging messages that are critical will be displayed:

```
switch# configure
switch(config)# logging level port link-failure critical
```

The following example displays the syslog message when a critical port link failure is configured:

```
PORT-2-IF_DOWN_LINK_FAILURE_CRIT: Interface [chars] is down (Link failure)
```

The following example displays the syslog message when a notification port link failure is configured:

```
PORT-5-IF_DOWN_LINK_FAILURE: Interface [chars] is down (Link failure [chars]) [chars] [chars]
```

Command	Description
show logging	Displays logging configuration information.

logging logfile

To set message logging for logfile, use the **logging logfile** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

logging logfile *filename severity-level* [**size** *filesize*]
no logging logfile *filename severity-level* [**size** *filesize*]

Syntax Description

filename	Specifies the log filename. Maximum length is 80 characters.
severity-level	Specifies the maximum severity of messages logged. The range is 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.
size *filesize*	(Optional) Specifies the log file size. The range is 4096 to 4194304 bytes.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The switch logs messages at or above the configured severity level.

Examples

The following example configures logging information for errors or events above a severity level of 3 (errors) to be logged in a file named ManagerLogFile. By configuring this limit, the file size is restricted to 3,000,000 bytes:

```
switch# config terminal
switch(config)# logging logfile
ManagerLogFile 3 size 3000000
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging module

To set message logging for linecards, use the **logging module** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

logging module [*severity-level*]
no logging module [*severity-level*]

Syntax Description

severity-level	(Optional) Specifies the maximum severity of messages logged. The range is 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example sets message logging for modules at level 7:

```
switch## config terminal
switch(config)# logging module 7
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging monitor

To set monitor message logging, use the **logging monitor** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

logging monitor *severity level*

Syntax Description

logging monitor	Sets message logging.
severity level	Specifies the maximum severity of messages logged. The range is 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example sets terminal line (monitor) message logging at level 2:

```
switch## config terminal
switch(config)# logging monitor 2
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging server

To set message logging for the remote server, use the **logging server** command.

logging server [{*hostname*|*ip address severity_level*|**facility auth**|**authpriv**|**cron**|**daemon**|**ftp**|**kernel**|**local0**|**local1**|**local2**|**local3**|**local4**|**local5**|**local6**|**local7**|**lpr**|**mail**|**news**|**syslog**|**user**|**uucp**}]

Syntax Description

logging server	Sets message logging for remote server.
hostname	Specifies the host name for remote server.
ip address	Specifies IP address for the remote server.
severity_level	(Optional) Specifies the maximum severity of messages logged. The range is 0 to 7, where 0 is emergency, 1 is alert, 2 is critical, 3 is error, 4 is warning, 5 is notify, 6 is informational, and 7 is debugging.
facility	(Optional) Specifies facility to use when forwarding to server.
auth	Specifies auth facility.
authpriv	Specifies authpriv facility.
cron	Specifies Cron/at facility.
daemon	Specifies daemon facility.
ftp	Specifies file transfer system facility.
kernel	Specifies kernel facility.
local0	Specifies local0 facility.
local1	Specifies local1 facility.
local2	Specifies local2 facility.
local3	Specifies local3 facility.
local4	Specifies local4 facility.
local5	Specifies local5 facility.
local6	Specifies local6 facility.
local7	Specifies local7 facility.
lpr	Specifies lpr facility.
mail	Specifies mail facility.
news	Specifies USENET news facility.

syslog	Specifies use syslog facility.
user	Specifies user facility.
uucp	Specifies Unix-to-Unix copy system facility.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

Enable message logging to the specified remote server for level 7 messages:

```
switch## config terminal
switch(config)# logging sever sanjose 7
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

logging timestamp

To set the time increment for the message logging time stamp, use the **logging timestamp** command. To negate the previously issued command or to revert to factory defaults, use the **no** form of the command.

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

Syntax Description

microseconds	Sets the logging time stamp to microseconds.
milliseconds	Sets the logging time stamp to milliseconds.
seconds	Sets the logging time stamp to seconds.

Command Default

Seconds.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example sets the logging time stamp to milliseconds:

```
switch## config terminal
switch(config)# logging timestamp milliseconds
```

Related Commands

Command	Description
show logging	Displays logging configuration information.

M Commands

match

To configure QoS class map match criteria, use the **match** command in class map configuration submode. Remove QoS class map match criteria, use the **no** form of the command.

match {**any**|**destination-address** *fc-id* [**mask** *address-mask*]|**destination-device-alias** *name*|**destination-wwn** *wwn-id*|**input-interface fc** *slot/port*|**source-address** *fc-id* [**mask** *address-mask*]|**source-device-alias** *name*|**source-wwn** *wwn-id*}
nomatch {**any**|**destination-address** *fc-id* [**mask** *address-mask*]|**destination-device-alias** *name*|**destination-wwn** *wwn-id*|**input-interface fc** *slot/port*|**source-address** *fc-id* [**mask** *address-mask*]|**source-device-alias** *name*|**source-wwn** *wwn-id*}

Syntax Description

any	Enables matching of any frame.
destination-address *fc-id*	Specifies the destination FCID to match frames.
mask *address-mask*	(Optional) Specifies an address mask to match frames. The range is 0x0 to 0xffffffff.
destination-device-alias *name*	Specifies the destination device alias to match frames. Maximum length is 64 characters.
destination-wwn *wwn-id*	Specifies the destination WWN to match frames.
input-interface fc *slot/port*	Specifies the source Fibre Channel interface to match frames.
source-address *fc-id*	Specifies the source FCID to match frames.
source-device-alias *name*	Specifies the source device alias to match frames. Maximum length is 64 characters.
source-wwn *wwn-id*	Specifies the source WWN to match frames.

Command Default

None.

Command Modes

Class map configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(x)	Added the **destination-device-alias** and **source-device-alias** options.

Usage Guidelines

You can access this command only if you enable the QoS data traffic feature using the **qos enable** command.

Examples

The following example creates a class map called MyClass1 and places you in the class map configuration submode to match any (default) criteria specified for this class:

```
switch# config terminal
switch(config)# qos class-map MyClass1 match-any
switch(config-cmap)# match any
```

The following example specifies a destination address match for frames with the specified destination FCID:

```
switch(config-cmap)# match destination-address 0x12ee00
```

The following example specifies a source address and mask match for frames with the specified source FCID. Mask refers to a single or entire area of FCIDs:

```
switch(config-cmap)# match source-address 0x6d1090 mask 0
```

The following example specifies a destination WWN to match frames:

```
switch(config-cmap)# match destination-wwn 20:01:00:05:30:00:28:df
Operation in progress. Please check class-map parameters
```

The following example specifies a source WWN to match frames:

```
switch(config-cmap)# match source-wwn 23:15:00:05:30:00:2a:1f
Operation in progress. Please check class-map parameters
```

The following example specifies a source interface to match frames:

```
switch(config-cmap)# match input-interface fc 2/1
Operation in progress. Please check class-map parameters
```

The following example removes a match based on the specified source interface:

```
switch(config-cmap)# no match input-interface fc 3/5
```

Related Commands

Command	Description
qos enable	Enables QoS.
show qos	Displays QoS information.

match (fcroute-map configuration submode)

To configure Fibre Channel route map match criteria, use the **match** command in Fibre Channel route map configuration submode. To remove the match criteria, use the **no** form of the command.

match source-fcid *source-fcid* [*network-mask*] **dest-fcid** *destination-fcid* [*network-mask*]
no match source-fcid *source-fcid* [*network-mask*] **dest-fcid** *destination-fcid* [*network-mask*]

Syntax Description

source-fcid *source-fcid*	Specifies the source FC ID match criteria. The format is **0x***hhhhhh*.
network_mask	Specifies the network mask of the FC ID. The range is **0x***0* to **0x***ffffff*.
dest-fcid *destination-fcid*	Specifies the destination FC ID. The format is **0x***hhhhhh*

Command Default

The FC ID match criteria mask default value is **0x***ffffff*.

Command Modes

Fibre Channel route map configuration submode.

Command History

Release	Modification
3.0(3)	This command was introduced.

Usage Guidelines

None.

Examples

The following example specifies the FC ID match criteria with the default mask value of **0x***ffffff*.

```
switch# config terminal
switch(config)# fcroute-map vsan 2 12
switch(config-fcroute-map)# match source-fcid 0x123456 dest-fcid 0x567890
```

The following example specifies the FC ID match criteria with a mask value of **0x***ffffff*.

```
switch# config terminal
switch(config)# fcroute-map vsan 2 12
switch(config-fcroute-map)# match source-fcid 0x123456 0xffffff dest-fcid 0x567890 0xffffff
```

The following example removes the FC ID match criteria.

```
switch(config-fcroute-map)# no match source-fcid 0x123456 0xffffff dest-fcid 0x567890
0xffffff
```

Note The only valid mask value is **0x***ffffff*.

Related Commands

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

match address

To configure match addresses in an IPsec crypto map with an access control list (ACL), use the **match address** command in IPsec crypto map configuration submode. To not match addresses, use the **no** form of the command.

match address *acl-name*
no match address [*acl-name*]

Syntax Description

acl-name	Specifies the ACL name. Maximum length is 64 characters.

Command Default

None.

Command Modes

IPsec crypto map configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Examples

The following example shows how to match addresses in an IPsec crypto map with an ACL:

```
switch# config terminal
switch(config)# crypto map domain ipsec x 1
switch(config-crypto-map-ip)# match address UserACL
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
show crypto map domain ipsec	Displays IPsec crypto map information.

mcast root

To configure the multicast feature, use the **mcast root** command in configuration mode. To revert to the default, use the **no** form of the command.

mcast root {**lowest**|**principal**} **vsan** *vsan-id*
no mcast root {**lowest**|**principal**} **vsan** *vsan-id*

Syntax Description

lowest	Specifies the lowest domain switch as root.
principal	Specifies the principal switch as root.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

principal

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the multicast root VSAN:

```
switch# config terminal
switch(config)#mcast root principal vsan 4001
```

Related Commands

Command	Description
show mcast	Displays multicast information.

member (fcalias configuration submode)

To add a member name to an Fibre Channel alias on a VSAN, use the **member** command in fcalias configuration submode. To remove a member name from an FC alias, use the **no** form of the command.

member {**device-alias** *aliasname* [**lun** *lun-id*]|**domain-id** *domain-id* [**lun** *lun-id*]|**fcid** *fc-id* [**lun** *lun-id*]|**fwwn** *fwwn-id*|**interface fc** *slot/port* [{**domain-id** *domain-id*|**swwn** *swwn-id*}]|**ip-address** *ipv4ipv6*|**pwwn** *pwwn-id* [**lun** *lun-id*]|**symbolic-nodename** *nodename*}
nomember {**device-alias** *aliasname* [**lun** *lun-id*]|**domain-id** *domain-id* [**lun** *lun-id*]|**fcid** *fc-id* [**lun** *lun-id*]|**fwwn** *fwwn-id*|**interface fc** *slot/port* [{**domain-id** *domain-id*|**swwn** *swwn-id*}]|**ip-address** *ipv4ipv6*|**pwwn** *pwwn-id* [**lun** *lun-id*]|**symbolic-nodename** *nodename*}

Syntax Description

device-alias *aliasname*	Specifies the member device alias. Maximum length is 64 characters.
lun *lun-id*	(Optional) Specifies the member LUN ID. The format is *0***x***hhhh* [**:***hhhh* [**:***hhhh* [**:***hhhh*]]], where *h* is a hexadecimal digit.
domain-id *domain-id*	Specifies the member domain ID. The range is 1 to 239.
fcid *fc-id*	Specifies the member FC ID. The format is *0***x***hhhhhh,* where *h* is a hexadecimal digit.
fwwn *fwwn-id*	Specifies the member fWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh,* where *h* is a hexadecimal digit.
interface fc *slot*/*port*	Specifies the member interface ID.
swwn *swwn-id*	(Optional) Specifies the member sWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh,* where *h* is a hexadecimal digit.
ip-address *ipv4*|*ipv6*	Specifies a member IP address in either IPv4 format, *A.B.C.D* , or IPv6format, *X:X:X::X/n* .
pwwn *pwwn-id*	Specifies the member pWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh,* where *h* is a hexadecimal digit.
symbolic-nodename *nodename*	Specifies the member symbolic node name. The maximum length is 255 characters.

Command Default

None.

Command Modes

Fcalias configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to add a member to an FC alias called samplealias:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# fcalias name samplealias
switch(config-fcalias)#
```

The following example defines an IPv6 address for the member:

```
switch(switch(config-fcalias)# member ip-address 2020:dbc0:80::4076
```

The following example shows how to delete the specified member:

```
switch(config-fcalias)# no member ip-address 2020:dbc0:80::4076
```

Related Commands

Command	Description
fcalias name	Configures an FC alias.
show fcalias	Displays the member name information in an FC alias.

member (ivr zone configuration)

To add a member name to an Inter-VSAN Routing (IVR) zone, use the **member** command in IVR zone configuration submode. To remove a member name from an fcalias, use the **no** form of the command.

member {**device-alias** *aliasname* {**lun** *lun-id* **vsan** *vsan-id* **autonomous-fabric-id** *afid*|**vsan** *vsan-id* **autonomous-fabric-id** *afid*}|**pwwn** *pwwn-id* {**lun** *lun-id* **vsan** *vsan-id* **autonomous-fabric-id** *afid*|**vsan** *vsan-id* **autonomous-fabric-id** *afid*}}
no member {**device-alias** *aliasname* {**lun** *lun-id* **vsan** *vsan-id* **autonomous-fabric-id** *afid*|**vsan** *vsan-id* **autonomous-fabric-id** *afid*}|**pwwn** *pwwn-id* {**lun** *lun-id* **vsan** *vsan-id* **autonomous-fabric-id** *afid*|**vsan** *vsan-id* **autonomous-fabric-id** *afid*}}

Syntax Description

device-alias*aliasname*	Specifies the member device alias. Maximum length is 64 characters.
lun *lun-id*	Specifies the member LUN ID. The format is *0***x***hhhh* [**:***hhhh* [**:***hhhh* [**:***hhhh*]]], where *h* is a hexadecimal digit.
vsan*vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
autonomous-fabric-id *afid*	Specifies the AFID to the local VSAN.
pwwn *pwwn-id*	Specifies the member pWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh,* where *h* is a hexadecimal digit.

Command Default

None.

Command Modes

IVR zone configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.1(1a)	Added **lun** parameter.

Usage Guidelines

You can configure an IVR zone member based on the specified pWWN and LUN value or, based on the specified pWWN, LUN value, and AFID.

Note The CLI interprets the LUN identifier value as a hexadecimal value whether or not the 0x prefix is included.

Examples

The following example shows how to configures an IVR zone member based on the device alias VSAN, and the AFID:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr zone name IvrLunZone
switch(config-ivr-zone)# member device-alias Switch4 vsan 1 autonomous-fabric-id 14
```

The following example shows how to configures an IVR zone member based on the pWWN, VSAN, and the AFID:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr zone name IvrLunZone
switch(config-ivr-zone)# member pwwn 29:00:00:05:30:00:06:ea vsan 1 autonomous-fabric-id
14
```

Related Commands

Command	Description
show ivr zone	Displays the IVR zone information.

member (zone configuration and zoneset-zone configuration submode)

To add a member name to a Fibre Channel zone set zone member, use the **member** command in zone set zone configuration submode. To remove a member name from a zone set zones, use the **no** form of the command.

member {**device-alias** *aliasname* [**lun** *lun-id*]|**domain-id** *domain-id* [**lun** *lun-id*]|**fcid** *fc-id* [**lun** *lun-id*]|**fwwn** *fwwn-id*|**interface fc** *slotport* [{**domain-id** *domain-id*|**swwn** *swwn-id*}]|**ip-address** *ipv4/ipv6*|**pwwn** *pwwn-id* [**lun** *lun-id*]|**symbolic-nodename** *nodename*}
nomember {**device-alias** *aliasname* [**lun** *lun-id*]|**domain-id** *domain-id* [**lun** *lun-id*]|**fcid** *fc-id* [**lun** *lun-id*]|**fwwn** *fwwn-id*|**interface fc** *slotport* [{**domain-id** *domain-id*|**swwn** *swwn-id*}]|**ip-address** *ipv4/ipv6*|**pwwn** *pwwn-id* [**lun** *lun-id*]|**symbolic-nodename** *nodename*}

Syntax Description

device-alias *aliasname*	Specifies the member device alias. Maximum length is 64 characters.
both	Specifies the device type as both.
initiator	Specifies the device type as initiator.
target	Specifies the device type as target.
lun *lun-id*	(Optional) Specifies the member LUN ID. The format is *0***x***hhhh* [**:***hhhh* [**:***hhhh* [**:***hhhh*]]], where *h* is a hexadecimal digit.
domain-id *domain-id*	Specifies the member domain ID. The range is 1 to 239.
alias-name	The name of the fcalias. Maximum length is 64 characters.
port-number *port*	Specifies the member port number. The range is 0 to 255.
fcid *fc-id*	Specifies the member FC ID. The format is *0***x***hhhhhh,* where *h* is a hexadecimal digit.
fwwn *fwwn-id*	Specifies the member fWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh,* where *h* is a hexadecimal digit.
interface fc *slot*/*port*	Specifies the member interface ID.
swwn *swwn-id*	Specifies the member sWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh,* where *h* is a hexadecimal digit.
ip-address *ipv4*|*ipv6*	Specifies a member IP address in either IPv4 format, *A.B.C.D* , or IPv6format, *X:X:X::X/n* .
pwwn *pwwn-id*	Specifies the member pWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh,* where *h* is a hexadecimal digit.
symbolic-nodename *nodename*	Specifies the member symbolic node name. The maximum length is 255 characters.

Command Default

This command can be used in both zone configuration submode and zoneset-zone configuration submode.

Command Modes

Zone set zone configuration submode and zoneset-zone configuration submode.

Command History

Release	Modification
5.2(6)	Added the keywords both, initiator, target to the syntax description.
1.0(2)	This command was introduced.
2.1(1a)	Added zoneset-zone configuration submode.
3.0(1)	Added the **IPv6** IP address format.

Usage Guidelines

Create a zone set zone member only if you need to add member to a zone from the zone set prompt.

Examples

The following example shows how to enter the device type as target:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# zone name zs1 vsan 1
switch(config-zone)# member device-alias a target
switch(config-zone)#
```

The following example shows how to add a member to a zone called zs1 on VSAN 1:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# zone name zs1 vsan 1
switch(config-zone)# member fcid 0x111112
```

The following example shows how to add a zone to a zoneset called Zoneset1 on VSAN 1:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# zoneset name ZoneSet1 vsan 1
switch(config-zoneset-zone)# member fcid 0x111112
```

The following example shows how to assign an iSCSI IPv6 address-based membership into a zone:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# zoneset name ZoneSet1 vsan 1
switch(config-zoneset-zone)#member ipv6-address 2001:0DB8:800:200C::417A
```

The following example shows how to delete the specified device from a zone:

```
switch(config-zoneset-zone)# no member ipv6-address 2001:0DB8:800:200C::417A
```

Related Commands

Command	Description
show zoneset	Displays zone set information.

Command	Description
zoneset (configuration submode)	Used to specify a name for a zone set.
zone name (zone set configuration submode)	Configures a zone in a zoneset.

member (zoneset configuration submode)

To configure zone set zone members, use the **member** command in zone set configuration submode. To remove a zone set member, use the **no** form of the command.

member *member-name*
no member *member-name*

Syntax Description

member-name	Specifies the member name. Maximum length is 64 characters.

Command Default

None.

Command Modes

Zone set configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to add a member zone to a zone set:

```
switch# config terminal
switch(config)# zoneset name Zoneset1 vsan 10
switch(config-zoneset)# member ZoneA
```

Related Commands

Command	Description
show zone	Displays zone information.
zoneset name	Creates a zone set.

member (zoneset-zone configuration submode)

To add a member name to a Fibre Channel zone set zone member, use the **member** command in zone set zone configuration submode. To remove a member name from a zone set zones, use the **no** form of the command.

member {**device-alias** *aliasname* [**lun** *lun-id*]|**domain-id** *domain-id* **port-number** *port*|**fcalias** *alias-name* [**lun** *lun-id*]|**fcid** *fc-id* [**lun** *lun-id*]|**fwwn** *fwwn-id*|**interface fc** *slot/port* [{**domain-id** *domain-id*|**swwn** *swwn-id*}]|**ip-address** *ip-address*|**pwwn** *pwwn-id* [**lun** *lun-id*]|**symbolic-nodename** *nodename*}
no member {**device-alias** *aliasname* [**lun** *lun-id*]|**domain-id** *domain-id* **port-number** *port*|**fcalias** *alias-name* [**lun** *lun-id*]|**fcid** *fc-id* [**lun** *lun-id*]|**fwwn** *fwwn-id*|**interface fc** *slot/port* [{**domain-id** *domain-id*|**swwn** *swwn-id*}]|**ip-address** *ip-address*|**pwwn** *pwwn-id* [**lun** *lun-id*]|**symbolic-nodename** *nodename*}

Syntax Description

device-alias *aliasname*	Specifies the member device alias. Maximum length is 64 characters.
lun *lun-id*	Specifies the member LUN ID. The format is *0***x***hhhh* [**:***hhhh* [**:***hhhh* [**:***hhhh*]]], where *h* is a hexadecimal digit.
domain-id *domain-id*	Specifies the member domain ID. The range is 1 to 239.
alias-name	The name of the fcalias. Maximum length is 64 characters.
port-number *port*	Specifies the member port number. The range is 0 to 255.
fcid *fc-id*	Specifies the member FC ID. The format is *0***x***hhhhhh,* where *h* is a hexadecimal digit.
fwwn *fwwn-id*	Specifies the member fWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh,* where *h* is a hexadecimal digit.
interface fc *slot*/*port*	Specifies the member interface ID.
swwn *swwn-id*	Specifies the member sWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh,* where *h* is a hexadecimal digit.
ip-address *ip-address*	Specifies a member IP address.
pwwn *pwwn-id*	Specifies the member pWWN ID. The format is *hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh***:***hh,* where *h* is a hexadecimal digit.
symbolic-nodename *nodename*	Specifies the member symbolic node name. The maximum length is 255 characters.

Command Default

None.

Command Modes

Zone set zone configuration submode.

Command History

Release	Modification
2.1(1)	This command was introduced.

Usage Guidelines

Create a zone set zone member only if you need to add member to a zone from the zone set prompt.

Examples

The following example shows how to configure an fcalias called AliasSample on VSAN 3.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# zoneset name ZoneSet1 vsan 1
switch(config-zoneset)# zone name InLineZone1
switch(config-zoneset-zone)# member fcid 0x111112
```

Related Commands

Command	Description
show zoneset	Displays zone set information.

metric (iSLB initiator configuration)

To assign a load-balancing metric for an iSLB initiator, use the **metric** command in iSLB initiator configuration submode. To revert to the default load-balancing metric, use the **no** form of the command.

metric *metric*
no metric *metric*

Syntax Description

metric *metric*	Specifies a load-balancing metric. The range is 10 to 10000.

Command Default

1000

Command Modes

iSLB initiator configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can assign a load metric to each initiator for weighted load balancing. The load calculated is based on the number of initiators on a given iSCSI interface. This feature accommodates initiators with different bandwidth requirements. For example, you could assign a higher load metric to a database server than to a web server. Weighted load balancing also accommodates initiators with different link speeds.

Examples

The following example specifies a load-balancing metric for the iSLB initiator:

```
switch# config t
switch(config)# islb initiator ip-address 100.10.10.10
switch (config-islb-init)# metric 100
```

The following example reverts to the default load-balancing metric:

```
switch (config-islb-init)# no
 metric 100
```

Related Commands

Command	Description
islb initiator	Assigns an iSLB name and IP address to the iSLB initiator and enters iSLB initiator configuration submode.
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.

mkdir

To create a directory in the flash file system, use the **mkdir** command in EXEC mode.

mkdir *directory*

Syntax Description

directory	Name of the directory to create.

Command Default

None.

Command Modes

EXEC

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command is only valid on Class C flash file systems.

You can specify whether to create the directory on bootflash:, slot0, or volatile:. If you do not specify the device, the switch creates the directory on the current directory.

Examples

The following example creates a directory called test in the slot0: directory:

```
switch# mkdir slot0:test
```

The following example creates a directory called test at the current directory level. If the current directory is slot0:mydir, this command creates a directory called slot0:mydir/test.

```
switch# mkdir test
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
rmdir	Removes an existing directory in the flash file system.

mode

To configure the ESP mode, use the mode command. To delete the ESP mode, use the no form of the command.

mode {**gcm**|**gmac**}
no mode {**gcm**|**gmac**}

Syntax Description

gcm	Specifies the GCM mode for the interface.
gmac	Specifies the GMAC mode for the interface.

Command Default

None.

Command Modes

Configuration submode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure the GCM mode for the interface:

```
switch(config-if-esp)# mode gcm
switch(config-if-esp)#
```

The following example shows how to configure the GMAC mode for the interface:

```
switch(config-if-esp)# mode gmac
switch(config-if-esp)#
```

Related Commands

Command	Description
fcsp enable	Enables FCSP.

modem connect line

To enable a modem connection when the switch is already in operation, use the **modem connect line** command in EXEC mode.

modem connect line {**com1**|**console**}

Syntax Description

com1	Connects the modem through a COM1 line connection.
console	Connects the modem through a console line connection.

Command Default

Disabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(2)	This command was introduced.

Usage Guidelines

If the switch is already in operation when the modem is connected, issue this command to notify the software that a modem is going to be added.

You must issue the **modem connect line** command before setting the user-input string for initialization.

Examples

The following example announces a modem connection from the line console:

```
switch# modem connect line console
```

The following example announces a modem connection from the COM1 port:

```
switch# modem connect line com1
```

monitor counter (port-group-monitor configuration mode)

To configure monitoring of a specific counter within a Port Group Monitor policy, use the monitor counter command. To remove polling functionality for a specific counter within Port Group Monitor policy, use the no form of the command.

monitor counter {**rx-performance**|**tx-performance**} **poll-interval** *interval* **delta rising-threshold** *rising threshold* **falling-threshold** *low threshold*
no monitor counter {**rx-performance**|**tx-performance**} **poll-interval** *interval* **delta rising-threshold** *rising threshold* **falling-threshold** *low threshold*

Syntax Description

rx-performance	Counfigures RX performance counter.
tx-performance	Configures TX performance counter.
poll-interval	Configures poll interval for counter.
interval	Displays poll interval in seconds. The range is from 0 to 2147483647.
delta	Displays the threshold type.
rising-threshold	Configures the upper threshold value.
rising-threshold	Sets numerical upper threshold limit. The range is from 0 to 100.
falling-threshold	Configures the lower threshold value.
low-threshold	Sets numerical low threshold limit. The range is from 0 to 100.

Command Default

None.

Command Modes

Configuration Port Group Monitor mode.

Command History

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

Usage Guidelines

When the no monitor counter command is used in the config-port-group-monitor mode, it turns-off the monitoring of that specific counter in the given policy.

Examples

The following example shows how to configure monitoring of a specific counter within a Port Group Monitor policy:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#port-group-monitor name pgmon
switch(config-port-group-monitor)# monitor counter rx-performance
switch(config-port-group-monitor)# monitor counter tx-performance
switch(config-port-group-monitor)#
```

The following example shows how to turn off the monitoring of a specific counter in the given policy:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# no port-group-monitor name pgmon
switch(config-port-group-monitor)# no port-group-monitor rx-performance
switch(config-port-group-monitor)# no port-group-monitor tx-performance
switch(config-port-group-monitor)# show port-group-monitor
--------------------------------------------------------------------------------
-----------
Port Group Monitor : enabled
--------------------------------------------------------------------------------
-----------
Policy Name : pgmonAdmin status : Not Active
Oper status  : Not Active
Port type    : All Port Groups
-------------------------------------------------------------------------------------------Counter
 Threshold Interval %ge Rising Threshold %ge Falling Threshold portguard------- ---------
-------- -------------------- ---------------------- ------RX Performance Delta 60 80 20
YesTX Performance Delta 60 80 20
No-----------------------------------------------------------------------
```

Related Commands

Command	Description
show port-group-monitor	Displays Port Group Monitor information.

monitor counter (port-monitor configuration mode)

To configure monitoring of a specific counter within a Port Monitor policy, use the monitor counter command. To remove polling functionality for a specific counter within Port Monitor policy, use the no form of the command.

monitor counter
{credit-loss-reco|invalid-crc|invalid-words|link-loss|lr-rx|lr-tx|rx-datarate|signal-loss|sync-loss|timeout-discards|tx-credit-not-available|tx-datarate|tx-discards}
no monitor counter
{credit-loss-reco|invalid-crc|invalid-words|link-loss|lr-rx|lr-tx|rx-datarate|signal-loss|sync-loss|timeout-discards|tx-credit-not-available|tx-datarate|tx-discards}

Syntax Description

credit-loss-reco	Counfigures credit loss recovery counter.
invalid-crc	Configures invalid crc counter.
invalid-words	Configures invalid words counter.
link-loss	Configures link failure counter.
lr-rx	Configures the number of link reset responses received by the Fc port.
lr-tx	Configures link reset responses transmitted by the FC port.
rx-datarate	Configure rx performance counter.
signal-loss	Configures the signal loss counter.
sync-loss	Configures the sync loss counter.
timeout-discards	Configure timeout discards counter.
tx-credit-not-available	Configure credit not available counter.
tx-datarate	Configure tx performance counter.
tx-discards	Configure tx discards counter.

Command Default

All counters are monitored by default in this release.

Command Modes

Configuration Port Monitor mode.

Command History

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

Usage Guidelines

When the **no monitor counter** command is used in the config-port-group-monitor mode, it turns-off the monitoring of that specific counter in the given policy.

This command is available in **port-monitor-configuration** mode.

Examples

The following example shows how to configure the credit loss recovery counter within a Port Monitor policy:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-monitor name pgmon
switch(config-port-monitor)# monitor counter credit-loss-reco
switch(config-port-monitor)#
```

Related Commands

Command	Description
port-monitor	
counter	Displays the individual counter.
show port-monitor	Displays Port Monitor information.

monitor counter tx-slowport-count

To configure monitoring of the tx-slowport-count counter, use the monitor counter tx-slowport-count command. To remove monitoring of tx-slowport-count, use the no form of the command.

monitor counter tx-slowport-count
no monitor counter tx-slowport-count

Syntax Description

There are no keywords or arguments for this command.

Command Default

None.

Command Modes

Configuration Port Group Monitor mode.

Command History

Release	Modification
6.2(13)	This command was introduced.

Examples

The following example shows how to configure monitoring of the tx-slowport-count counter within a Port Monitor policy:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-monitor name pmon
switch(config-port-monitor)# monitor counter tx-slowport-count
switch(config-port-monitor)#
```

The following example shows how to turn off monitoring of the tx-slowport-count counter within a Port Monitor policy:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-monitor name pmon
switch(config-port-monitor)# no monitor counter tx-slowport-count
switch(config-port-monitor)#
```

Related Commands

Command	Description
show port-monitor	Displays Port Monitor information.

monitor counter tx-slowport-oper-delay

To configure monitoring of the tx-slowport-oper-delay counter, use the monitor counter tx-slowport-oper-delay command. To remove monitoring of tx-slowport-count, use the no form of the command.

monitor counter tx-slowport-oper-delay
no monitor counter tx-slowport-oper-delay

Syntax Description

There are no keywords or arguments for this command.

Command Default

None.

Command Modes

Configuration Port Group Monitor mode.

Command History

Release	Modification
6.2(13)	This command was introduced.

Examples

The following example shows how to configure monitoring of the tx-slowport-oper-delay counter within a Port Monitor policy:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-monitor name pmon
switch(config-port-monitor)# monitor counter tx-slowport-oper-delay
switch(config-port-monitor)#
```

The following example shows how to turn off monitoring of the tx-slowport-oper-delay counter within a Port Monitor policy:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-monitor name pmon
switch(config-port-monitor)# no monitor counter tx-slowport-oper-delay
switch(config-port-monitor)#
```

Related Commands

Command	Description
show port-monitor	Displays Port Monitor information.

monitor counter txwait

To configure monitoring of the txwait counter, use the no monitor counter txwait command. To remove monitoring of txwait, use the no form of the command.

monitor counter txwait
no monitor counter txwait

Syntax Description

There are no keywords or arguments for this command.

Command Default

None.

Command Modes

Configuration Port Group Monitor mode.

Command History

Release	Modification
6.2(13)	This command was introduced.

Examples

The following example shows how to configure monitoring of the txwait counter within a Port Monitor policy:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-monitor name pmon
switch(config-port-monitor)# monitor counter txwait
switch(config-port-monitor)#
```

The following example shows how to turn off monitoring of the txwait counter within a Port Monitor policy:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-monitor name pmon
switch(config-port-monitor)# no monitor counter txwait
switch(config-port-monitor)#
```

Related Commands

Command	Description
show port-monitor	Displays Port Monitor information.

monitor session

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

monitor session *session-id*
no span session *session-id*

Syntax Description

session-id	Specifies the SPAN session ID. The range is 1 to 48.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure a local SPAN session in RX mode:

```
switch# config terminal
switch(config)# monitor session 1 rx
switch(config-monitor)#
```

The following example shows how to delete a local SPAN session in RX mode:

```
switch(config)# no
 monitor session 1 rx
```

The following example shows how to configure a local SPAN with port-channel as source in tx mode:

```
switch(config)# monitor session 1 tx
switch(config-monitor)#
```

Related Commands

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

move

To remove a file from the source file and place it in the destination file, use the **move** command in EXEC mode.

move {**bootflash:**|**slot0:**|**volatile:**} [*directory* /] *filename* {**bootflash:**|**slot0:**|**volatile:**} [*directory* /] *filename*

Syntax Description

bootflash:	Source or destination location for internal bootflash memory.
slot0:	Source or destination location for the CompactFlash memory or PCMCIA card.
volatile:	Source or destination location for volatile memory.
directory	(Optional) Specifies the name of the directory.
filename	(Optional) Specifies the name of the file to move or create.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If you do not specify the directory name in the command line, the switch prompts you for it.

Examples

The following example moves the file called samplefile from the slot0 directory to the mystorage directory:

```
switch# move slot0:samplefile slot0:mystorage/samplefile
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
mkdir	Creates a directory in the flash file system.
rmdir	Removes an existing directory in the flash file system.

mutual-chap username (iSCSI initiator configuration and iSLB initiator configuration)

To assign a username for the initiator's challenge, use the **mutual-chap username** command in iSCSI initiator configuration submode. To remove the username, use the **no** form of the command.

mutual-chap username*username* **password** {**0** *cleartext-password*|**7** *encrypted-passwordpassword*}
no mutual-chap username *username* **password** {**0** *cleartext-password*|**7** *encrypted-passwordpassword*}

Syntax Description

username *username*	Specifies a username. The maximum size is 32.
password	Specifies a password for the initiator's challenge.
0 *cleartext-password*	Specifies that the password is a cleartext CHAP password.
7 *encrypted-password*	Specifies that the password is an encrypted CHAP password.
password	Specifies a password for the username. The maximum size is 32.

Command Default

None.

Command Modes

iSCSI initiator configuration submode.
iSLB initiator configuration submode.

Command History

Release	Modification
2.0(1b)	This command was introduced.
3.0(1)	Added iSLB initiator configuration submode.

Usage Guidelines

The iSLB initiator can authenticate the Cisco MDS switch's initiator target during the iSCSI login phase. This authentication requires the user to configure a username and password for the switch to present to the iSLB initiator. The provided password is used to calculate a CHAP response to a CHAP challenge sent to the IPS port by the initiator.

Examples

The following example shows how to configure a username, password type, and password for an iSCSI initiator challenge (mutual CHAP):

```
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)# mutual-chap username userName password 0 cisco
switch(config-iscsi-init)# mutual-chap username userNameTest password 0 test
switch(config-iscsi-init)#
```

The following example assigns a username and password to the initiator's challenge for an iSLB initiator:

```
switch# config t
switch(config)# islb initiator ip-address 100.10.10.10
switch (config-islb-init)# mutual-chap username tester password K9c4*1
```

The following example removes the username and password from the initiator's challenge for an iSLB initiator:

```
switch (config-islb-init)# no mutual-chap username tester password K9c4*1
```

Related Commands

Command	Description
islb initiator	Assigns an iSLB name and IP address to the iSLB initiator and enter s iSLB initiator configuration submode.
iscsi initiator name	Assigns an iSCSI name and changes to iSCSI initiator configuration submode.
show iscsi initiator	Displays iSCSI initiator information.
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 configured iSLB initiator.
show islb initiator detail	Displays detailed iSLB initiator information.
show islb initiator summary	Displays iSLB initiator summary information.

N Commands

native-autonomous-fabric-num

To create an IVR persistent FC ID database entry, use the native-autonomous-fabric-num command in fcdomain database configuration submode. To delete all IVR persistent FC ID database entries for a given AFID and VSAN, use the **no** form of the command.

native-autonomous-fabric-num *afid-num* **native-vsan** *vsan-id* **domain** *domain-id*
no native-autonomous-fabric-num *afid-num* **native-vsan** *vsan-id* **domain** *domain-id*

Syntax Description

afid-num	Specifies the native AFID. The range is 1 to 64.
native-vsan *vsan-id*	Specifies the native VSAN ID. The range is 1 to 4093.
domain *domain-id*	Specifies the domain ID. The range is 1 to 239.

Command Default

None.

Command Modes

fcdomain database configuration submode.

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

There is only one domain ID associated with an AFID and VSAN. If you change the domain ID, all the associated FC ID mapping records are also changed.

Examples

The following example shows how to create an entry for a native AFID, VSAN, and domain:

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# native-autonomous-fabric-num 20 native-vsan 30 domain 15
switch(config-fcdomain-fcid)#
```

The following example shows how to remove all entries for a native AFID and VSAN:

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# no native-autonomous-fabric-num 20 native-vsan 30
```

Related Commands

Command	Description
ivr fcdomain database autonomous-fabric-num	Creates IVR persistent FC IDs.
show ivr fcdomain database	Displays IVR fcdomain database entry information.

node

To configure Cisco SME switch, use the node command. To disable this command, use the no form of the command.

node {**local**|{*A.B.C.D*|*X*:*X*::*X* /*n*|*DNS name*}}
nonode {**local**|{*A.B.C.D*|*X*:*X*::*X* /*n*|*DNS name*}}

Syntax Description

local	Configures the local switch.
A.B.C.D	Specifies the IP address of the remote switch in IPv4 format.
X:X::X/n	Specifies the IP address of the remote switch in IPv6 format.
DNS name	Specifies the name of the remote database.

Command Default

None.

Command Modes

Cisco SME cluster configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example adds the Cisco SME interface from a local switch:

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

The following example adds the Cisco SME interface from a remote switch:

```
switch# config t
switch(config))# sme cluster c1
switch(config-sme-cl)# node 171.71.23.33
switch(config-sme-cl-node)#
```

Related Commands

Command	Description
show sme cluster *cluster name* **node**	Displays Cisco SME node information about a local or remote switch.

node (Cisco IOA cluster node configuration submode)

To configure IOA switch, use the node command. To delete a node to the cluster, use the no form of the command.

node {**local**|*remote-node-name* **or** *ip-address*}
no node {**local**|*remote-node-name* **or** *ip-address*}

Syntax Description

local	Specifies local node as a part of the cluster.
remote-node-name	Specifies either through the DNS name or IPV4/IPV6 address.

Command Default

None.

Command Modes

Cisco IOA cluster node 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 local switch:

```
switch(config)# ioa cluster tape_vault
switch#(config-ioa-cl)# node local
switch(config-ioa-cl-node)# node 172.23.144.95
2009 May 19 21:06:57 sjc-sw2 %CLUSTER-2-CLUSTER_QUORUM_GAIN: Cluster 0x2143000dec3ee782 now
 has quorum with 1 nodes
2009 May 19 21:07:03 sjc-sw2 %CLUSTER-2-CLUSTER_QUORUM_GAIN: Cluster 0x2143000dec3ee782 now
 has quorum with 2 nodes
sjc-sw2(config-ioa-cl-node)# end
```

Related Commands

Command	Description
interface ioa	Configures the IOA interface.

npiv enable

To enable N port identifier virtualization (NPIV) for all VSANs on a switch, use the **npiv enable** command in configuration mode. To disable NPIV, use the **no** form of the command.

npiv enable
no npiv enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

NPIV provides a means to assign multiple port IDs to a single N Port. This feature allows multiple applications on the N port to use different identifiers and allows access control, zoning, and port security to be implemented at the application level.

You must globally enable NPIV for all VSANs on the MDS switch to allow the NPIV-enabled applications to use multiple N port identifiers.

Note All of the N Port Identifiers are allocated in the same VSAN.

Examples

The following example enables NPIV for all VSANs on the switch:

```
switch# config terminal
switch(config)# npiv enable
```

The following example disables NPIV for all VSANs on the switch:

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

Related Commands

Command	Description
show interface	Displays interface configurations.

nport

To configure the site and VSAN ID of the N ports, use the **nport** command. To delete the N port from the IOA cluster, use the **no** form of the command.

nport pwwn *pwwn* **site** *site name* **vsan** *vsan-id*
no nport pwwn *pwwn* **site** *site name* **vsan** *vsan-id*

Syntax Description

pwwn	Specifies the N port.
pwwn	Specifies the N port PWWN. The format is hh:hh:hh:hh:hh:hh:hh:hh.
site	Specifies an IOA site.
site name	Specifies an IOA site name. The maximum length is 31 characters.
vsan	Specifies the VSAN where this flow is accelerated.
vsan id	Specifies the VSAN ID where this flow is accelerated. The range is from 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

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 site and VSAN ID of the N port:

```
switch(config-ioa-cl)# nport pwwn 10:0:0:0:0:0:0:1 site SJC vsan 100
switch(config-ioa-cl)# no nport pwwn 11:0:0:0:0:0:0:1 site SJC vsan 100
switch(config-ioa-cl)# end
```

Related Commands

Command	Description
show ioa cluster summary	Displays the summary of all the IOA clusters.

nport pwwn

To configure the N Port pWWN for the SAN extension tuner, use the **nport pwwn** command in SAN extension configuration mode. To revert to the default value, use the **no** form of the command.

nport pwwn *pwwn-id* **vsan** *vsan-id* **interface gigabitethernet** *slot*/*port*
no nport pwwn *pwwn-id* **vsan** *vsan-id* **interface gigabitethernet** *slot*/*port*

Syntax Description

pwwn-id	Specifies the port WWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
interface gigabitethernet *slot*/*port*	Specifies the Gigabit Ethernet interface slot and port.

Command Default

None.

Command Modes

SAN extension configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to add an entry to the SAN extension tuner database:

```
switch# san-ext-tuner
switch(san-ext)# nport pwwn 11:22:33:44:55:66:77:88 vsan 1 interface gigabitethernet 1/1
```

Related Commands

Command	Description
san-ext-tuner	Enters SAN extension configuration mode.
show san-ext-tuner	Shows SAN extension tuner information.

npv auto-load-balance disruptive

To enable autoload balance disruptive, use the npv auto-load-balance disruptive command in configuration mode. To disable this feature, use the no form of the command.

npv auto load-balancing disruptive
no npv auto load-balancing disruptive

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable autoload balance disruptive:

```
switch(config)# npv auto-load-balance disruptive
Enabling this feature may flap the server intefaces whenever load is not in a ba
lanced state. This process may result in traffic disruption. Do you want to proc
eed? (y/n):
Please enter y or n Y
switch(config)#
```

Related Commands

Command	Description
npv traffic-map server interface	Configures server interface traffic engineering.

npv enable

To enable N port virtualization (NPV), use the npv enable command in configuration mode. To disable this feature, use the no form of the command.

npv enable
no npv enable

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

When NPV is enabled, all configurations are erased and the switch is rebooted. The switch restarts in the NPV mode. All configuration and verification commands for NPV are available only when NPV is enabled on the switch. When you disable this feature, all related configurations are automatically erased and the switch is rebooted.

Examples

The following example shows how to enable NPV:

```
switch# config
switch(config)# npv enable
```

Related Commands

Command	Description
show npv status	Displays the NPV current status.

npv traffic-map server-interface

To configure the server interface based traffic engineering, use the npv traffic-map server-interface command in configuration mode. To revert to the default value, use the no form of the command.

npv traffic-map server-interface if -range external-interface if-range
no npv traffic-map server-interface if-range external-interface if-range

Syntax Description

if-range	Range may vary from 1 to 1.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure NPV traffic map server interface:

```
switch(config)# npv traffic-map server-interface fc1/1 external-interface fc1/2
switch(config)# npv traffic-map server-interface fc1/4-5 external-interface fc1/6-7
switch(config)# no npv traffic-map server-interface fc1/4-5 external-interface fc1/6-7
switch(config)# no npv traffic-map server-interface fc1/1 external-interface fc1/2
switch(config)#
```

Related Commands

Command	Description
show npv-traffic-map	Displays information about the NPV traffic map.

ntp abort

To abort and unlock the existing Network Time Protocol (NTP) Cisco Fabric Services (CFS) distribution session on a switch, use the **ntp abort** command in configuration mode.

ntp abort

Syntax Description

This command has no other arguments or keywords.

Command Default

This command aborts the current NTP CFS session.

Command Modes

Configuration mode (config)

Command History

Release	Modification
2.0(x)	This command was introduced.

Examples

The following example displays how to abort the NTP CFS distribution session in progress:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp abort
```

Related Commands

Command	Description
ntp commit	Commits the NTP configuration changes to the active configuration.
ntp distribute	Enables CFS distribution for NTP.
show ntp status	Displays the status of the NTP CFS distribution.

ntp allow

To enable processing of Network Time Protocol (NTP) control mode and private mode packets, use the **ntp allow** command. To disable this feature, use the **no** form of this command.

ntp allow {**private** |**control** [**rate-limit** *seconds*]}
no ntp allow {**private** |**control**}

Syntax Description

private	Specifies to process the private mode packets.
control	Specifies to process the control mode packets.
rate-limit *seconds*	Specifies the quiet period in which further control mode packets are ignored after processing one. The default time duration is 3 seconds, which means that a control mode packet is processed or responded every 3 seconds. Range is from 1 to 65535.

Command Default

Processing of control and private mode packets is disabled by default for security reasons.

Command Modes

Configuration mode (config)

Command History

Release	Modification
6.2(13)	This command was introduced.

Examples

The following example displays how to enable the processing of private mode packets:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp allow private
```

The following example displays how to enable the processing or responding of control mode packets every 3 seconds:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp allow control
```

The following example displays how to enable the processing or responding of control mode packets every 10 seconds:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp allow control rate-limit 10
```

Related Commands

Command	Description
show ntp	Displays NTP information.

ntp authenticate

To prevent the system from synchronizing with unauthenticated, unconfigured NTP peers, use the **ntp authenticate** command. To allow synchronization with unauthenticated, unconfirmed NTP peers, use the **no** form of this command.

ntp authenticate
no ntp authenticate

Syntax Description

This command has no arguments or keywords.

Command Default

Unkeyed NTP symmetric-active, broadcast, and multicast packets are trusted by default. This feature is disabled by default.

Command Modes

Configuration mode (config)

Command History

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

Usage Guidelines

If the **ntp authenticate** command is specified, when a symmetric-active, broadcast, or multicast packet is received, the system will not synchronize to the peer unless the packet carries one of the authentication keys specified in the **ntp trusted-key** command.

Note This command does not authenticate peer associations configured via the **ntp server** and **ntp peer** commands. To authenticate NTP server and NTP peer associations, specify the **key** keyword.

Examples

The following example displays how to enable NTP authentication:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp authenticate
```

The following example displays how to disable NTP authentication:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp authenticate
```

Related Commands

Command	Description
ntp authentication-key	Configures an NTP authentication key for a device to synchronize to a time source after enabling the NTP authentication.

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

ntp authentication-key

To configure a Network Time Protocol (NTP) authentication key for a device to synchronize to a time source after enabling the NTP authentication, use the **ntp authentication-key** command. To remove the NTP authentication key, use the **no** form of this command.

ntp authentication-key *id* **md5** *key* [{**0** |**7**}]
no ntp authentication-key *id* **md5** *key* [{**0** |**7**}]

Syntax Description

id	Authentication key identifier. The range is from 1 to 65535.
md5	Specifies the MD5 algorithm for authentication.
key	Authentication key. The maximum key size is 15.
0	(Optional) Specifies the encryption type to be *Clear* text.
7	(Optional) Specifies the encryption type to be *Encrypted*.

Command Default

No NTP keys are configured by default. When configuring an authentication key the default CLI encryption type is *clear text*.

Command Modes

Configuration mode (config)

Command History

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

Usage Guidelines

Enable NTP authentication before configuring an NTP authentication key.

The device does not synchronize to a time source unless the source has one of these authentication keys and the key number is specified by the **ntp trusted-key** command.

Authentication keys are always stored in the switch configuration in the encrypted format. If a user configures a key as *clear text*, the key will automatically be converted before installation into the configuration.

Examples

The following example displays how to configure an NTP authentication key:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp authentication-key 42 md5 key1_12
```

The following example displays how to remove the NTP authentication key:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp authentication-key 42 md5 key1_12
```

Related Commands

Command	Description
show ntp authentication-keys	Displays a list of configured NTP authentication keys.

ntp commit

To apply pending Network Time Protocol (NTP) configuration to an NTP Cisco Fabric Services (CFS) enabled peers in a fabric, use the **ntp commit** command.

ntp commit

Syntax Description

This command has no other arguments or keywords.

Command Default

This command commits changes pending in the current NTP CFS session.

Command Modes

Configuration mode (config)

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

Once the **ntp commit** command is issued, the running configuration is modified on all switches that are part of the NTP CFS domain. Use the **copy running-config startup-config fabric** command to save the running configuration to the startup configuration on all the switches.

Examples

The following example displays how to commit changes to the active NTP configuration:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp commit
```

Related Commands

Command	Description
ntp abort	Aborts the NTP configuration.
ntp distribute	Enables CFS distribution for NTP.
show ntp pending-diff	Displays the differences between the pending NTP configuration changes and the active NTP configuration.
show ntp status	Displays the status of the NTP CFS distribution.

ntp distribute

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

ntp distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

NTP configuration distribution to other switches is disabled by default.

Command Modes

Configuration mode (config)

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

In order to enable NTP distribution with CFS, you must have already enabled CFS distribution for the device using the **cfs distribute** command.

If CFS is disabled for NTP, then NTP does not distribute any configuration changes and does not accept a distribution from other devices in the fabric.

The **ntp distribute** command enables NTP to distribute its configurations through CFS. To distribute an NTP configuration change, enter the change and then use the **ntp commit** command.

After CFS distribution is enabled for NTP, then the entry of an NTP configuration command locks the fabric for NTP until the **ntp commit** command is entered. During the lock, no changes can be made to the NTP configuration by any other device in the fabric except the device where the lock was activated.

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

Examples

The following example displays how to distribute the active NTP configuration to the fabric:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp distribute
```

Related Commands

Command	Description
cfs distribute	Globally enables CFS distribution for all applications on the device.
clear ntp session	Clears the application configuration session, discards pending changes, and releases the lock on a fabric.
ntp abort	Aborts the NTP configuration.
ntp allow	Enables processing of the control mode and private mode packets.

Command	Description
ntp commit	Commits the NTP configuration changes to the active configuration.
show cfs status	Displays the global CFS distribution status for the device.
show ntp pending-diff	Displays the differences between the pending NTP configuration changes and the active NTP configuration.
show ntp status	Displays the status of the NTP CFS distribution.

ntp logging

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

ntp logging
no ntp logging

Syntax Description

This command has no other arguments or keywords.

Command Default

NTP logging is disabled by default.

Command Modes

Configuration mode (config)

Command History

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

Examples

The following example displays how to enable NTP logging:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp logging
```

The following example displays how to disable NTP logging:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp logging
```

Related Commands

Command	Description
show ntp logging-status	Displays the NTP logging status.
show ntp statistics	Displays the NTP statistics.

ntp peer

To configure a device as a Network Time Protocol (NTP) peer, use the **ntp peer** command. To remove the device as an NTP peer, use the **no** form of this command.

ntp peer {*ip-address ipv6-address dns-name*} [**key** *id*] **[prefer]** [**maxpoll** *interval*] [**minpoll** *interval*]
no ntp peer {*ip-address ipv6-address dns-name*}

Syntax Description

ip-address	IPv4 address.
ipv6-address	IPv6 address.
dns-name	Domain Name Server (DNS) name.
key *id*	(Optional) Key ID. The range is from 1 to 65535.
prefer	(Optional) Specifies the given NTP peer as the preferred one.
maxpoll *interval*	(Optional) Maximum interval to poll a peer, in seconds. Default interval is 6.
minpoll *interval*	(Optional) Minimum interval to poll a peer, in seconds. Default interval is 4.

Command Default

No NTP peers are configured by default.

Command Modes

Configuration mode (config)

Command History

Release	Modification
5.0(1a)	Added the **key** *id* keyword.
2.0(x)	This command was introduced.

Usage Guidelines

The **ntp peer** command is part of the NTP Cisco Fabric Services (CFS) distribution.

An NTP server is an authoritative source of NTP updates. The local device will follow the time of a server, but the server will not update from the local device's time. NTP peers send out updates and also adjust to incoming peer updates so that all peers converge to the same time. A device may have associations with multiple servers or peers.

If you configure a key to be used while communicating with the NTP peer, make sure that the key exists as a trusted key on the device.

Examples

The following example displays how to configure an NTP peer:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp peer 190.0.2.1 key 123 prefer minpoll 4 maxpoll 10
```

The following example displays how to remove the NTP peer:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp peer 190.0.2.1
```

Related Commands

Command	Description
ntp server	Configures an NTP server.
show ntp peers	Displays all the NTP peers.
show ntp peer-status	Displays the status for all the server and peers.

ntp server

To configure a device as a Network Time Protocol (NTP) server, use the **ntp server** command. To remove the device as an NTP peer, use the **no** form of this command.

ntp server {*ip-address ipv6-address dns-name*} [**key** *id*][**prefer**][**maxpoll** *interval*][**minpoll** *interval*]
no ntp server {*ip-address ipv6-address dns-name*}

Syntax Description

ip-address	IPv4 address.
ipv6-address	IPv6 address.
dns-name	Domain Name Server (DNS) name.
key *id*	(Optional) Key ID. The range is from 1 to 65535.
prefer	(Optional) Specifies the given NTP peer as the preferred one.
maxpoll *interval*	(Optional) Maximum interval to poll a peer, in seconds. Default interval is 6.
minpoll *interval*	(Optional) Minimum interval to poll a peer, in seconds. Default interval is 4.

Command Default

No NTP server are configured by default.

Command Modes

Configuration mode (config)

Command History

Release	Modification
5.0(1a)	Added the **key** *id* keyword.
2.0(x)	This command was introduced.

Usage Guidelines

The **ntp server** command is part of the NTP Cisco Fabric Services (CFS) distribution.

An NTP server is an authoritative source of NTP updates. The local device will follow the time of a server, but the server will not update from the local device's time. NTP peers send out updates and also adjust to incoming peer updates so that all peers converge to the same time. A device may have associations with multiple servers or peers.

If you configure a key to be used while communicating with the NTP server, make sure that the key exists as a trusted key on the device.

Examples

The following example displays how to configure an NTP server:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp server 190.0.2.1 key 123 prefer minpoll 4 maxpoll 10
```

The following example displays how to remove the NTP server:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp server 190.0.2.1
```

Related Commands

Command	Description
ntp peer	Configures a device as an NTP peer.
show ntp peers	Displays all the NTP peers.
show ntp peer-status	Displays the status for all the server and peers.

ntp source-interface

To override the default source address of Network Time Protocol (NTP) packets sent from the switch, use the **ntp source-interface** command. To remove an NTP source interface, use the **no** form of this command.

ntp source-interface {**ethernet** *slot/port.sub-interface*|**mgmt** *number* |**port-channel** *number* }
no ntp source-interface {**ethernet** *slot/port.sub-interface*|**mgmt** *number* |**port-channel** *number* }

Syntax Description

ethernet *slot/port.sub-interface*	Ethernet interface.
mgmt *number*	Management interface (mgmt 0).
port-channel *number*	Port channel number.

Command Default

This default source address of NTP packets is mgmt0.

Command Modes

Configuration mode (config)

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

Only a single **ntp source-interface** command can be specified. All NTP packets sent through all interfaces will use the address specified by this command as the source address.

Examples

The following example displays how to configure an Ethernet interface:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp source-interface ethernet 2/2
```

The following example displays how to remove an Ethernet interface:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp source-interface ethernet 2/2
```

The following example displays how to configure the management 0 interface:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp source-interface mgmt 0
```

The following example displays how to remove the management 0 interface:

```
switch# configure
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp source-interface mgmt 0
```

The following example displays how to configure a port channel:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp source-interface port-channel 1
```

The following example displays how to remove the port channel:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp source-interface port-channel 1
```

Related Commands

Command	Description
show ntp source-interface	Displays information about the configured NTP source interface.

ntp trusted-key

To configure one or more keys that a time source must provide in its Network Time Protocol (NTP) packets in order for the device to synchronize to it, use the **ntp trusted-key** command. To remove the NTP trusted key, use the **no** form of this command.

ntp trusted-key *id*
no ntp trusted-key *id*

Syntax Description

id	Trusted key identifier. The range is from 1 to 65535.

Command Default

No trusted keys are configured by default.

Command Modes

Configuration mode (config)

Command History

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

Usage Guidelines

You must configure an NTP authentication key using the **ntp authentication-key** command before configuring an NTP trusted key. You must use the NTP authentication key as the NTP trusted key number.

This command provides protection against accidentally synchronizing the device to a time source that is not trusted.

Examples

The following example displays how to configure an NTP trusted key:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ntp trusted-key 42
```

The following example displays how to remove the NTP trusted key:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no ntp trusted-key 42
```

Related Commands

Command	Description
ntp authentication-key	Configures an NTP authentication key for a device to synchronize to a time source after enabling the NTP authentication.
show ntp authentication-keys	Displays a list of configured NTP authentication keys.
show ntp source-interface	Displays the status of NTP authentication.

ntp sync-retry

To retry synchronization with configured servers, use the **ntp sync-retry** command.

ntp sync-retry

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.1(1b)	Added a note.
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Note If the user changes the mgmt0 ip address, NX-OS should conditionally do an internal **ntp syncronization-retry**.

Examples

The following example displays the sup-fc0 message logs:

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

Related Commands

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

nxapi http port *port-number*

To configure an HTTP port to access the NX-API Developer Sandbox, use the **nxapi http port** *port-number* command in global configuration mode. To disable HTTP, use the **no** form of this command.

nxapi http port *port-number*
no nxapi http

Syntax Description

port	HTTP port number
port-number	Specifies the HTTP port number. The range is from 0 to 65535. **Note** The default HTTP port number to access the NX-API Developer Sandbox is 8080.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

The **feature nxapi** command must be used to enable the NX-API feature before you configure HTTP to access the NX-API Developer Sandbox.

Ensure that the *port-number* configured is not used by other services like SSH, Telnet.

The following example shows how to configure an HTTP port to access the NX-API Developer Sandbox:

```
switch# configure terminal
switch(config)# feature nxapi
switch(config)# nxapi http port 1010
```

Related Commands

Command	Description
feature nxapi	Enables NX-API.
nxapi sandbox	Enables the NX-API Developer Sandbox.
nxapi https port *port-number*	Configures an HTTPS port to access the NX-API Developer Sandbox.

nxapi https port *port-number*

To configure an HTTPS port to access the NX-API Developer Sandbox, use the **nxapi https** command in global configuration mode. To disable HTTPS, use the **no** form of this command.

nxapi https port *port-number*
no nxapi https

Syntax Description

port	HTTPS port number.
port-number	Specifies the HTTPS port number. The range is from 0 to 65535.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

The **feature nxapi** command must be used to enable the NX-API feature before you configure HTTPS to access the NX-API Developer Sandbox.

Ensure that the *port-number* configured is not used by other services like SSH, Telnet.

The following example shows how to configure an HTTPS port to access the NX-API Developer Sandbox:

```
switch# configure terminal
switch(config)# feature nxapi
switch(config)# nxapi https port 443
```

Related Commands

Command	Description
feature nxapi	Enables NX-API.
nxapi sandbox	Enables the NX-API Developer Sandbox.
nxapi http port *port-number*	Configures an HTTP port to access the NX-API Developer Sandbox.

nxapi sandbox

To enable the NX-API Developer Sandbox, use the **nxapi sandbox** command in global configuration mode. To disable the NX-API Developer Sandbox, use the **no** form of this command.

nxapi sandbox
no nxapi sandbox

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

The **feature nxapi** command must be used to enable the NX-API feature before you enable the NX-API Developer Sandbox.

The following example shows how to enable the NX-API Developer Sandbox:

```
switch# configure terminal
switch(config)# feature nxapi
switch(config)# nxapi sandbox
```

Related Commands

Command	Description
feature nxapi	Enables NX-API.

nwwn (DPVM database configuration submode)

To add a device to a dynamic port VSAN membership (DPVM) database using the nWWN, use the **nwwn** command in DPVM database configuration submode. To remove a device from a DPVM database using the nWWN, use the **no** form of the command.

nwwn *nwwn-id* **vsan** *vsan-id*
no nwwn *nwwn-id* **vsan** *vsan-id*

Syntax Description

nwwn-id	Specifies the node WWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh,* where *h* is a hexadecimal number.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

DPVM database configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Examples

The following example shows how to add an entry to the DPVM database:

```
switch# config terminal
switch(config)# dpvm database
switch(config-dpvm-db)# nwwn 11:22:33:44:55:66:77:88 vsan 1
```

The following example shows how to delete an entry from the DPVM database:

```
switch(config-dpvm-db)# no nwwn 11:22:33:44:55:66:77:88 vsan 1
```

Related Commands

Command	Description
dpvm database	Configures the DPVM database.
show dpvm	Displays DPVM database information.

nwwn (SAN extension configuration mode)

To configure the nWWN for the SAN extension tuner, use the **nwwn** command in SAN extension configuration submode.

nwwn *nwwn-id*

Syntax Description

nwwn-id	Specifies the nWWN address. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.

Command Default

None.

Command Modes

SAN extension configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to add an entry to the SAN extension tuner database:

```
switch# san-ext-tuner
switch(san-ext)# nwwn 20:42:00:0b:46:79:f1:80
```

Related Commands

Command	Description
san-ext-tuner	Enters SAN extension configuration mode.
show san-ext-tuner	Shows SAN extension tuner information.

O Commands

ocsp url

To configure the HTTP URL of the Online Certificate Status Protocol (OCSP) for the trust point CA, use the **ocsp url** command in trust point configuration submode. To discard the OCSP configuration, use the **no** form of the command.

ocsp url *url*
no ocsp url *url*

Syntax Description

url	Specifies the OCSP URL. The maximum size is 512 characters.

Command Default

None.

Command Modes

Trust point configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The MDS switch uses the OCSP protocol to check the revocation status of a peer certificate (presented to it during the security or authentication exchange for IKE or SSH, for example), only if the revocation checking methods configured for the trust point include OCSP as one of the methods. OCSP checks the certificate revocation status against the latest CRL on the CA using the online protocol, which generate network traffic and also requiring that the OCSP service of the CA be available online in the network.

If revocation checking is performed by the cached CRL at the MDS switch, no network traffic is generated. The cached CRL does not contain the latest revocation information.

You must authenticate the CA for the trust point before configuring the OCSP URL for it.

Examples

The following example shows how to specify the URL for OCSP to use to check for revoked certificates:

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# ocsp url http://admin-ca.cisco.com/ocsp
```

The following example shows how to remove the URL for OCSP:

```
switch(config-trustpoint)# no ocsp url http://admin-ca.cisco.com/ocsp
```

Related Commands

Command	Description
crypto ca crl-request	Configures a CRL or overwrites the existing one for the trust point CA.
revocation-check	Configures trust point revocation check methods.
show crypto ca crl	Displays configured CRLs.

odrt.bin

To preform offline data recovery of Cisco SME, use the odrt.bin command on Linux-based systems. This command allows you to recover data when the MSM-18/4 module or the Cisco MDS 9222i fabric switch is not available.

odrt.bin [--help] [--version] {**-h**|**-l**|**-r**|**-w**} {**if** *=input_device_or_file*|**of** *=output_device_or_file*|**kf** *=key_export_file*|**verbose** *=level*}

Syntax Description

--help	(Optional) Displays information on the tool.
--version	(Optional) Displays the version of the tool.
-h	Reads and prints the tape header information on the tape.
-l	Lists all SCSI devices.
-r	Reads the tape device and writes data to intermediate file(s).
-w	Reads the intermediate file(s) on disk and writes data to the tape.
if	Specifies the input device or file.
of	Specifies the output device or file.
kf	Specifies the volume group filename.
verbose	Specifies the level of verbose.

Command Default

None.

Command Modes

None. This command runs from the Linux shell.

Command History

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

Usage Guidelines

The **odrt.bin** command operates in the following steps:

- Tape-to-disk– In this mode, the **odrt.bin** command reads the encrypted data from the tape and stores it as intermediate files on the disk. This mode is invoked with the '-r' flag. The input parameter is the tape device name and filename on the disk is the output parameter.
- Disk-to-tape– In this mode, the **odrt.bin** command reads intermediate files on the disk, decrypts and decompresses (if applicable) the data and writes the clear-text data to the tape. The decryption key is obtained from the volume group file that is exported from the Cisco Key Management Center (KMC). This mode is invoked with the '-w' flag. The input parameter is the filename on the disk and tape device name is the output parameter. The volume group file name (key export file) is also accepted as a parameter. Key export password needs to be entered at the command prompt.

Examples

The following command reads and prints the Cisco tape header information on the tape:

```
odrt -h if=/dev/sg0
```

The following example read the data on tape into intermediate file(s) on disk:

```
odrt -r if=/dev/sg0 of=diskfile
```

The following command reads the encrypted/compressed data in intermediate file(s) and writes back the decrypted/decompressed data to the tape:

```
odrt -w if=diskfile of=/dev/sg0 kf=c1_tb1_Default.dat
```

A sample output of the odrt command follows:

```
[root@ips-host06 odrt]# ./odrt.bin -w if=c of=/dev/sg2
kf=sme_L700_IBMLTO3_Default.dat verbose=3
Log file: odrt30072
Please enter key export password:
Elapsed 0:3:39.28, Read 453.07 MB, 2.07 MB/s, Write 2148.27 MB, 9.80 MB/s
Done
```

open

To open a file or command pipeline and return a channel identifier in Tcl, use the **open** command.

open *filename*

Syntax Description

filename	The name of the file to be opened.

Command Default

None.

Command Modes

Interactive Tcl shell and Tcl script.

Command History

Release	Modification
NX-OS 5.1(1)	This command was introduced.

Usage Guidelines

This is a standard Tcl command documented in Tcl documentation with the following modifications:

Access to files and directories is limited to user space only. Access to system filespace and system commands is not permitted.

Examples

The following example shows that access is denied to system files:

```
switch-tcl# open "/etc/hosts" r
Permission denied. couldn't open "/etc/hosts": permission denied
switch-tcl#
```

The following examples shows that access is denied to system commands:

```
switch-tcl# open "| cat /etc/hosts" r
Permission denied. couldn't execute "cat": not owner
switch-tcl#
```

Related Commands

Command	Description
cli	Execute an NX-OS CLI command in Tcl verbosely.
clis	Execute an NX-OS CLI command in Tcl silently.

out-of-service

To put an interface out of service, use the **out-of-service** command in interface configuration submode. To restore the interface to service, use the **no** form of the command.

out-of-service [force]
no out-of-service [force]

Syntax Description

force	(Optional) Configures the interface that should be forced out of service.

Command Default

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
NX-OS 5.2(1)	This command was deprecated.
3.0(1)	This command was introduced.

Usage Guidelines

Before using the **out-of-service** command, you must disable the interface using the **shutdown** command.

When an interface is out of service, all the shared resources for the interface are released, as is the configuration associated with those resources.

Caution Taking interfaces out of service releases all the shared resources to ensure that they are available to other interfaces. This causes the configuration in the shared resources to revert to default when the interface is brought back into service. Also, an interface cannot come back into service unless the default shared resources for the port are available. The operation to free up shared resources from another port is disruptive.

Examples

The following example shows how to take an interface out of service:

```
switch# config terminal
switch(config)# interface fc 1/1
switch(config-if)#shutdown
switch(config-if)# out-of-service
Putting an interface into out-of-service will cause its shared resource
configuration to revert to default
Do you wish to continue(y/n)? [n]
```

The following example makes an interface available for service:

```
switch(config-if)# no out-of-service
```

Related Commands

Command	Description
shutdown	Disables an interface.
show interface	Displays the status of an interface.

out-of-service module

To perform a graceful shutdown of an integrated crossbar on the supervisor module of a Cisco MDS 9500 Series Director, use the **out-of-service module** command in EXEC mode.

out-of-service module *slot*

Syntax Description

slot	The *slot* refers to the chassis slot number for Supervisor-1 module or Supervisor-2 module where the integrated crossbar is located.

Command Default

None.

Command Modes

EXEC.

Command History

Release	Modification
NX-OS 5.2(1)	Applicable for supervisor module only.
3.0(1)	This command was introduced.

Usage Guidelines

Before removing a crossbar from an MDS 9500 Series Director, you must perform a graceful shutdown of the crossbar.

Note To reactivate the integrated crossbar, you must remove and reinsert or replace the Supervisor-1 or Supervisor-2 module.

For additional information about crossbar management, refer to the *Cisco MDS 9000 Family CLI Configuration Guide* .

Examples

The following example shows how to perform a graceful shutdown of the integrated crossbar:

```
switch# out-of-service module 2
```

Related Commands

Command	Description
out-of-service xbar	Performs a graceful shutdown of an external crossbar switching module in a Cisco MDS 9513 Director.
show module	Displays the status of a module.

out-of-service xbar

To perform a graceful shutdown of the external crossbar switching module of a Cisco MDS 9513 Director, use the **out-of-service xbar** command in EXEC mode.

out-of-service xbar *slot*
no out-of-service xbar *slot*

Syntax Description

slot	Specifies the external crossbar switching module slot number, either 1 or 2. The *slot* refers to the external crossbar switching module slot number.

Command Default

None.

Command Modes

EXEC.

Command History

Release	Modification
NX-OS 5.2(1)	This command was deprecated.
3.0(1)	This command was introduced.

Usage Guidelines

Before removing a crossbar from an MDS 9500 Series Director, you must perform a graceful shutdown of the crossbar.

The *slot* refers to the external crossbar switching module slot number.

Note To reactivate the external crossbar switching module, you must remove and reinsert or replace the crossbar switching module.

Caution Taking the crossbar out-of-service may cause supervisor switchover.

For additional information about crossbar management, refer to the *Cisco MDS 9000 Family CLI Configuration Guide* .

Examples

The following example shows how to perform a graceful shutdown of the external crossbar switching module of a Cisco MDS 9513 Director:

```
switch# out-of-service xbar 1
```

Related Commands

Command	Description
out-of-service module	Performs a graceful shutdown of an integrated crossbar on the supervisor module of a Cisco MDS 9500 Series Director.

Command	Description
show module	Displays the status of a module.

P Commands

passive-mode

To configure the required mode to initiate an IP connection, use the **passive-mode** command. To enable passive mode for the FCIP interface, use the no form of the command.

passive-mode
no passive-mode

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

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

By default, the active mode is enabled to actively attempt an IP connection.

If you enable the passive mode, the switch does not initiate a TCP connection and only waits for the peer to connect to it.

Examples

The following example enables passive mode on an FCIP interface:

```
switch# config terminal
switch(config)# interface fcip 1
switch(config-if)# passive-mode
```

Related Commands

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

password strength-check

To enable password strength checking, use the password strength-check command. To disable this feature, use the no form of the command.

password strength-check
no password strength-check

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

When you enable password strength checking, the NX-OS software only allows you to create strong passwords.

The characteristics for strong passwords included the following:

- At least 8 characters long
- Does not contain many consecutive characters (such as abcd)
- Does not contain many repeating characters (such as aaabb)
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

The following are examples of strong passwords:

- If2COM18
- 2004AsdfLkj30

Examples

The following example shows how to enable secure standard password:

```
switch(config)# password strength-check
switch(config)#
```

Related Commands

Command	Description
show password strength-check	Displays if the password strength check is enabled.

pathtrace

To display per-hop interface information along the paths between 2 devices, use the **pathtrace** command.

pathtrace {**domain** *id*|**fcid** *id*} **vsan** *id* [{**[reverse] [detail]**}]

Syntax Description

domain *id*	Traces the paths to all the edge devices in the domain ID. The range is from 1 to 239.
fcid *id*	Specifies the Fibre Channel ID of the destination N-port. The range is from 0x0 to 0xffffff.
vsan *id*	Specified the VSAN ID. The range is from 1 to 4094.
reverse	(Optional) Displays information about the reverse (or return) path.
detail	(Optional) Displays detailed information about each egress interface at every hop.

Command Default

None.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
6.2(5)	This command was introduced.

Usage Guidelines

- If the **pathtrace** command is executed in a path where devices do not support the Pathtrace feature, the pathtrace request packets are dropped and the command is not processed.
- The Pathtrace feature is supported only on Cisco MDS NX-OS Release 6.2(5) and later releases.
- The Pathtrace feature is not supported in Inter-VSAN Routing (IVR).

Depending on the keywords used, Pathtace displays the following information for every egress interface in a path:

Name	Description	Limitations
Speed/Spd	The operational speed of an active interface. It represents the capable bandwidth of an inactive interface.	Not displayed for internal interfaces.
TxRt/Tx	The bits transmitted per second.	Not displayed for internal interfaces.
RxRt/Rx	The bits received per second.	Not displayed for internal interfaces.
TxFrame	The number of frames transmitted.	Not displayed for internal interfaces.

Name	Description	Limitations
RxFrame	The number of frames received.	Not displayed for internal interfaces.
TxB_B/TxB2B	The transmit buffer-to-buffer credit that is remaining.	Not displayed for internal interfaces.
RxB_B/RxB2B	The receive buffer-to-buffer credit that is remaining.	Not displayed for internal interfaces.
Errors	The aggregate of ingress and egress errors.	Not displayed for internal interfaces.
Discard/Discards	The aggregate of ingress and egress frame discards.	Not displayed for internal interfaces.
CRC	The Cyclic Redundancy Check (CRC) errors on the incoming frames.	Not displayed for internal interfaces.
TxWait	An interface's total transmission waiting time due to nonavailability of transmit buffer-to-buffer credits.	Displays a percentage of transmit wait time for last 1 second, 1 minute, 1 hour, and last 72 hours.
ZoneDrops	The number of frames dropped due to access control list (ACL) rules.	Displays only for Cisco MDS 9700 48-Port 32-Gbps Fibre Channel Switching Module (DS-X9648-1536K9).
FibDrops	The number of frames dropped due to forwarding information base (FIB) rules.	Displays only for Cisco MDS 9700 48-Port 32-Gbps Fibre Channel Switching Module (DS-X9648-1536K9).

Examples

The following example shows how to trace the path between a switch in which the command is executed and an edge device, using the edge device's FCID:

```
switch# pathtrace fcid 0xca016c vsan 2000
switch# pathtrace fcid 0xca016c vsan 2000
The final destination port type is F_Port
------------------------------------------------------------------------
Hop Domain In-Port          Out-Port         Speed Cost  Switchname
------------------------------------------------------------------------
0   111    embedded         fc1/6            4G    250   switch1
1   202    fc1/6            fc1/1            2G    -     switch2
NOTE: The stats are displayed for the egress interface only
```

The following example shows how to trace both the forward path and the return path between a switch in which the command is executed and all the edge devices in domain 83 on the 'sw-fcip69' switch:

```
switch# pathtrace domain 83 vsan 70 reverse
```

```
The final destination port type is Embedded
--------------------------------------------------------------------------------
Hop Domain In-Port          Out-Port         Speed       Cost  Switchname
--------------------------------------------------------------------------------
0   144    embedded         vfc69(Eth1/8)    10.0G       100   sw-ioa-70
1   83     vfc69(Eth1/1)    embedded         -           -     sw-fcip69
2   83     embedded         vfc69(Eth1/1)    10.0G       100   sw-fcip69
3   144    vfc69(Eth1/8)    embedded         -           -     sw-ioa-70

NOTE: The stats are displayed for the egress interface only
```

The following example shows how to display detailed information about the interfaces (both the forward path and the return path) between a switch in which the command is executed and an edge device, using the edge device's FCID:

```
switch# pathtrace fcid 0xca016c vsan 2000 reverse detail
The final destination port type is F_Port
--------------------------------------------------------------------------------
Hop 0       Domain In-Port          Out-Port         Speed Cost  Switchname
            111    embedded         fc1/6            4G    250   switch1
--------------------------------------------------------------------------------
Stats for egress port: fc1/6
    TxRt(B/s): 2944
    RxRt(B/s): 3632
        TxB_B: 32
        RxB_B: 32
      TxFrame: 137467
      RxFrame: 137475
       Errors: 0
      Discard: 0
          CRC: 0
--------------------------------------------------------------------------------
Hop 1       Domain In-Port          Out-Port         Speed Cost  Switchname
            202    fc1/6            fc1/1            2G    -     switch2
--------------------------------------------------------------------------------
Stats for egress port: fc1/1
    TxRt(B/s): 1424
    RxRt(B/s): 1528
        TxB_B: 0
        RxB_B: 32
      TxFrame: 711
      RxFrame: 649
       Errors: 0
      Discard: 15
          CRC: 0
--------------------------------------------------------------------------------
Hop 2       Domain In-Port          Out-Port         Speed Cost  Switchname
            202    embedded         fc1/6            4G    250   switch2
--------------------------------------------------------------------------------
Stats for egress port: fc1/6
    TxRt(B/s): 3632
    RxRt(B/s): 2952
        TxB_B: 32
        RxB_B: 32
      TxFrame: 137476
      RxFrame: 137467
       Errors: 0
      Discard: 0
          CRC: 0
--------------------------------------------------------------------------------
Hop 3       Domain In-Port          Out-Port         Speed Cost  Switchname
            111    fc1/6            embedded         -     -     switch1
```

```
--------------------------------------------------------------------------------
Stats for egress port: embedded
    TxRt(B/s): -
    RxRt(B/s): -
        TxB_B: -
        RxB_B: -
      TxFrame: -
      RxFrame: -
       Errors: -
      Discard: -
          CRC: -
NOTE: The stats are displayed for the egress interface only
```

The following example shows how to trace the path between a switch in which the **pathtrace** command is executed and all the edge devices in the specified domain and VSAN:

```
switch# pathtrace domain 83 vsan 70
The final destination port type is Embedded
--------------------------------------------------------------------------------
Hop Domain In-Port          Out-Port         Speed       Cost  Switchname
--------------------------------------------------------------------------
0   144    embedded         vfc69(Eth1/8)    10.0G       100   sw-ioa-70
1   83     vfc69(Eth1/1)    embedded         -           -     sw-fcip69

NOTE: The stats are displayed for the egress interface only
```

Note

- In the output, *embedded* indicates that the respective port is an HBA interface in an edge device.
- Some of the terminologies used in the multipath outputs are defined in the following table:

Term	Description
FCIP	
InputRate(B/s)	The number of bytes received per second on the in port of an FCIP link.
OutputRate(B/s)	The number of bytes received per second on the out port of an FCIP link.
InputFrames(/sec)	The number of frames received per second on the in port of an FCIP link.
OutputFrames(/sec)	The number of frames received per second on the out port of an FCIP link.
vFC	
FcoeOut(Oct)	The number of egress FCoE octets on a vFC interface.
FcoeIn(Oct)	The number of ingress FCoE octets on a vFC interface.
FcoeOutPkt	The number of egress FCoE packets on a vFC interface.
FcoeInPkt	The number of ingress FCoE packets on a vFC interface.

Related Commands

Command	Description
FCtrace	Traces the path to a destination device by displaying the corresponding switch's pWWN at every hop.

peer (DMM job configuration submode)

To add peer SSM information to a job, use the **peer** command in DMM job configuration submode. To remove the peer SSM information from a job, use the **no** form of the command.

peer *ip-address*
no peer *ip-address*

Syntax Description

ip-address	Specifies the peer SSM IP address. The format for the IP address is *A.B.C.D.*

Command Default

None.

Command Modes

DMM job configuration submode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

In a dual-fabric topology, the migration job runs on an SSM in each fabric. The two SSMs exchange messages over the management IP network, so each SSM needs the IP address of the peer.

Examples

The following example shows how to add peer SSM information to a 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)# peer 224.2.1.2
switch(config-dmm-job)#
```

Related Commands

Command	Description
show dmm ip-peer	Displays the IP peer of a DMM port.
show dmm job	Displays job information.

peer-info ipaddr

To configure the peer information for the FCIP interface, use the **peer-info ipaddr** command. To remove the peer information for the FCIP interface, use the no form of the command.

peer-info ipaddr *address* [**port** *number*]
no peer-info ipaddr *address* [**port** *number*]

Syntax Description

ipaddr *address*	Configures the peer IP address.
port *number*	Configures a peer port. The range is 1 to 65535.

Command Default

None.

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.

The basic FCIP configuration uses the peer's IP address to configure the peer information. You can also use the peer's port number, port profile ID, or port WWN to configure the peer information. If you do not specify a port, the default 3225 port number is used to establish connection.

Examples

The following command assigns an IP address to configure the peer information. Since no port is specified, the default port number, 3225, is used:

```
switch# config terminal
switch(config)# interface fcip 10
switch(config-if)# peer-info ipaddr 209.165.200.226
```

The following command deletes the assigned peer port information:

```
switch(config-if)# no peer-info ipaddr 209.165.200.226
```

The following command assigns the IP address and sets the peer TCP port to 3000. The valid port number range is from 0 to 65535:

```
switch(config-if)# peer-info ipaddr 209.165.200.226 port 3000
```

The following command deletes the assigned peer port information:

```
switch(config-if)# no peer-info ipaddr 209.165.200.226 port 2000
```

Related Commands

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

periodic-inventory notification

To enable the periodic inventory notification message dispatches, use the **periodic-inventory notification** command Call Home configuration submode. To revert to the default state, use the **no** form of the command.

periodic-inventory notification [**interval** *days*]
no periodic-inventory notification

Syntax Description

interval *days*	(Optional) Specifies the notification interval. The range is 1 to 30.

Command Default

Disabled.

The initial default interval is 7 days.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable periodic inventory notification and use the default interval:

```
switch# config terminal
switch(config)# callhome
switch(config-callhome)# periodic-inventory notification
```

The following example shows how to enable periodic inventory notification and set the interval to 10 days:

```
switch# config terminal
switch(config)# callhome
switch(config-callhome)# periodic-inventory notification interval 10
```

Related Commands

Command	Description
callhome	Enters Call Home configuration submode.
show callhome	Displays Call Home configuration information.

permit (IPv6-ACL configuration)

To configure permit conditions for an IPv6 access control list (ACL), use the permit command in IPv6-ACL configuration submode. To remove the conditions, use the **no** form of the command.

permit {*ipv6-protocol-number*|**ipv6**} {*source-ipv6-prefix*/*prefix-length*|**any**|**host** *source-ipv6-address*} {*dest-ipv6-prefix*/*prefix-length*|**any**|**host** *dest-ipv6-address*} **[log-deny]**
permit icmp {*source-ipv6-prefix*/*prefix-length*|**any**|**host** *source-ipv6-address*} {*dest-ipv6-prefix* /*prefix-length*|**any**|**host** *dest-ipv6-address*} [*icmp-type*] [*icmp-code*] **[log-deny]**
permit tcp {*source-ipv6-prefix*/*prefix-length*|**any**|**host** *source-ipv6-address*} [{*source-port-operator source-port-number*|**range** *source-port-number source-port-number*}] {*dest-ipv6-prefix*/*prefix-length*|**any**|**host** *dest-ipv6-address*} [{*dest-port-operator dest-port-number*|**range** *dest-port-number dest-port-number*}] **[established] [log-deny]**
permit udp {*source-ipv6-prefix*/*prefix-length*|**any**|**host** *source-ipv6-address*} [{*source-port-operator source-port-number*|**range** *source-port-number source-port-number*}] {**dest-ipv6-prefix**/**prefix-length**|**any**|**host dest-ipv6-address**} [{**dest-port-operator dest-port-number**|**range dest-port-number dest-port-number**}] **[log-deny]**
no permit {*ipv6-protocol-number*|**ipv6**|**icmp**|**tcp**|**udp**}

Syntax Description

ipv6-protocol-number	Specifies an IPv6 protocol number. The range is 0 to 255.
ipv6	Applies the ACL to any IPv6 packet.
source-ipv6-prefix/prefix-length	Specifies a source IPv6 network or class of networks. The format is *X:X:X::X/n* .
any	Applies the ACL to any source or destination prefix.
host *source-ipv6-address*	Applies the ACL to the specified source IPv6 host address. The format is *X:X:X::X* .
dest-ipv6-prefix /prefix-length	Specifies a destination IPv6 network or class of networks. The format is *X:X:X::X/n* .
host *dest-ipv6-address*	Applies the ACL to the specified destination IPv6 host address. The format is *X:X:X::X* .
log-deny	(Optional) For packets that are dropped, creates an informational log message about the packet that matches the entry. The message includes the input interface.
icmp	Applies the ACL to any Internet Control Message Protocol (ICMP) packet.
icmp-type	Specifies an ICMP message type. The range is 0 to 255.
icmp-code	Specifies an ICMP message code. The range is 0 255.
tcp	Applies the ACL to any TCP packet.
source-port-operator	Specifies an operand that compares the source ports of the specified protocol. The operands are **lt** (less than), **gt** (greater than), and **eq** (equals).

source-port-number	Specifies the port number of a TCP or UDP port. The number can be from 0 to 65535. A range requires two port numbers.
udp	Applies the ACL to any UDP packet.
dest-port-operator	Specifies an operand that compares the destination ports of the specified protocol. The operands are **lt** (less than), **gt** (greater than), and **eq** (equals).
dest-port-operator	Specifies the port number of a TCP or UDP port. The number can be from 0 to 65535. A range requires two port numbers.
range	Specifies a range of ports to compare for the specified protocol.
established	(Optional) Indicates an established connection, which is defined as a packet whole SYN flag is not set.

Command Default

None.

Command Modes

IPv6-ACL configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The following guidelines can assist you in configuring an IPv6-ACL. For complete information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide* .

- You can apply IPv6-ACLs to VSAN interfaces, the management interface, Gigabit Ethernet interfaces on IPS modules and MPS-14/2 modules, and Ethernet PortChannel interfaces. However, if IPv6-ACLs are already configured in a Gigabit Ethernet interface, you cannot add this interface to a Ethernet PortChannel group.

Caution Do not apply IPv6-ACLs to just one member of a PortChannel group. Apply IPv6-ACLs to the entire channel group.

- Use only the TCP or ICMP options when configuring IPv6-ACLs on Gigabit Ethernet interfaces.
- Configure the order of conditions accurately. Because the IPv6-ACL filters are applied sequentially to the IP flows, the first match determines the action taken. Subsequent matches are not considered. Be sure to configure the most important condition first. If no conditions match, the software drops the packet.

Examples

The following example configures an IPv6-ACL called List, enters IPv6-ACL submode, and adds an entry that permits IPv6 traffic from any source address to any destination address:

```
switch# config terminal
switch(config)# ipv6 access-list List1
sswitch(config-ipv6-acl)# permit tcp any any
```

The following example removes a permit condition set for any destination prefix on a specified UDP host:

```
switch# config terminal
switch(config)# ipv6 access-list List1
switch(config-ipv6-acl)# no
 permit udp host 2001:db8:200d::4000 any
```

The following example removes the IPv6-ACL called List1 and all its entries:

```
switch# config terminal
switch(config)# no ipv6 access-list List1
```

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6 ACL and enters IPv6-ACL configuration submode.
deny	Configures deny conditions for an IPv6 ACL.

phone-contact

To configure the telephone contact number with the Call Home function, use the **phone-contact** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

phone-contact [*number*]
no phone-contact [*number*]

Syntax Description

number	(Optional) Configures the customer's phone number. Allows up to 17 alphanumeric characters in international phone format. **Note** Do not use spaces. Use the + prefix before the number.

Command Default

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the telephone contact number with the Call Home function:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# phone-contact +1-800-123-4567
```

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.

ping

To diagnose basic network connectivity, use the **ping** command in EXEC mode.

ping [ipv6] {*host-nameip-address*} [**count** *repeat-count*] [**interface** {**gigabitethernet** *slot*/*port*|**mgmt** *number*|**port-channel** *number*|**vsan** *vsan-id*}] [**size** *size* [**timeout** *timeout*]]

Syntax Description

ipv6	Sends IPv6 echo messages.
host-name	Specifies the host name of system to ping. Maximum length is 64 characters.
ip-address	Specifies the address of the system to ping.
count *repeat-count*	Specifies the repeat count. The range is 0 to 64.
interface	Specifies the interface on which the ping packets are to be sent.
gigabitethernet *slot*/*port*	Specifies a Gigabit Ethernet slot and port number.
mgmt *number*	Specifies the management interface.
port-channel *number*	Specifies a PortChannel number. The range is 1 to 256.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
size *size*	Specifies the size. The range is 10 to 2000.
timeout *timeout*	Specifies the timeout. The range is 1 to 10.

Command Default

Prompts for input fields.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **ipv6** argument.

Usage Guidelines

The ping (Packet Internet Groper) program sends an echo request packet to an address, and then awaits a reply. The ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

Verify connectivity to the TFTP server using the ping command.

To abnormally terminate a ping session, type the **Ctrl-C** escape sequence.

Examples

The following example pings the system 192.168.7.27:

```
switch# ping 192.168.7.27
```

```
PING 192.168.7.27 (192.168.7.27): 56 data bytes
64 bytes from 192.168.7.27: icmp_seq=0 ttl=255 time=0.4 ms
64 bytes from 192.168.7.27: icmp_seq=1 ttl=255 time=0.2 ms
64 bytes from 192.168.7.27: icmp_seq=2 ttl=255 time=0.2 ms
64 bytes from 192.168.7.27: icmp_seq=3 ttl=255 time=0.2 ms
--- 209.165.200.226 ping statistics ---
13 packets transmitted, 13 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.4 ms
```

The following command shows the prompts that appear when you enter the **ping** command without an IP address:

```
switch# ping
Target IP address: 209.165.200.226
Repeat count [5]: 4
Datagram size [100]: 5
Timeout in seconds [2]: 1
Extended commands [n]: 3
PING 209.165.200.226 (209.165.200.226) 5(33) bytes of data.
--- 209.165.200.226 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3017ms
```

policy

To enter IKE policy configuration and configure a policy for the IKE protocol, use the **policy** command in IKE configuration submode. To delete the policy, use the **no** form of the command.

policy *priority*
no policy *priority*

Syntax Description

priority	Specifies the priority for the IKE policy. The range is 1 to 255, where 1 is the high priority and 255 is the lowest.

Command Default

None.

Command Modes

IKE configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Examples

The following example shows how to configure a policy priority number for the IKE protocol:

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# policy 1
switch(config-ike-ipsec-policy)#
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

port

To assign the TCP port number of a Gigabit Ethernet interface to the FCIP profile or a listener peer port for a ISCSI interface, use the **port** command. Use the **no** form of the command to negate the command or revert to factory defaults.

port *number*
no port *number*

Syntax Description

port *number*	Configures a peer port. The range is 1 to 65535.

Command Default

Disabled

Command Modes

Fcip profile configuration submode.

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Associates the profile with the assigned local port number. If a port number is not assigned for a FCIP profile, the default TCP port 3225 is used.

Examples

The following example configures port 5000 on FCIP interface 5:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)# port 5000
```

The following example configures port 4000 on ISCSI interface 2/1:

```
switch# config terminal
switch(config)# interface iscsi 2/1
switch(config-profile)# port 4000
```

Related Commands

Command	Description
show fcip profile	Displays information about the FCIP profile.
interface fcip *interface_number* use-profile *profile-id*	Configures the interface using an existing profile ID from 1 to 255.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

portaddress

To enable the FICON feature in a specified VSAN, use the **ficon vsan** command in configuration mode. To disable the feature or to revert to factory defaults, use the **no** form of the command.

portaddress *portaddress* **block name** *string* **prohibit portaddress** *portaddress*
no portaddress *portaddress* **block name** *string* **prohibit portaddress** *portaddress*

Syntax Description

portaddress	Specifies the FICON port number for this interface. The range is 0 to 254.
block	Blocks a port address.
name *string*	Configures a name for the port address. Maximum length is 24 characters.
prohibit portaddress	Prohibits communication with a port address.

Command Default

None.

Command Modes

FICON configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The **shutdown**/**no shutdown** port state is independent of the **block**/**no block** port state. If a port is shutdown, unblocking that port will not initialize the port.

You cannot block or prohibit CUP port (0XFE).

If you prohibit ports, the specified ports are prevented from communicating with each other. Unimplemented ports are always prohibited.

Examples

The following example disables a port address and retains it in the operationally down state:

```
switch# config terminal
switch(config)# ficon vsan 2
switch(config-ficon)# portaddress 1
switch(config-ficon-portaddr)# block
```

The following example enables the selected port address and reverts to the factory default of the port address not being blocked:

```
switch(config-ficon-portaddr)# no block
```

The following example prohibits port address 1 in VSAN 2 from talking to ports 3:

```
switch(config-ficon-portaddr)# prohibit portaddress 3
```

The following example removes port address 5 from a previously-prohibited state:

```
switch(config-ficon-portaddr)# no prohibit portaddress 5
```

The following example assigns a name to the port address:

```
switch(config-ficon-portaddr)# name SampleName
```

The following example deletes a previously configured port address name:

```
switch(config-ficon-portaddr)# no name SampleName
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.

port-channel persistent

To convert an automatically created PortChannel to a persistent PortChannel, use the **port-channel persistent** command in EXEC mode.

port-channel *port-channel number* **persistent**

Syntax Description

port-channel number	Specifies the PortChannel number. The range is 1 to 256.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(3)	Added usage guideline.
2.0(x)	This command was introduced.

Usage Guidelines

The auto mode support is not available after 4.x. Any previously automatically created PortChannel needs to be made persistent by using the port-channel persistent command. This command needs to be run on both sides of the auto Port Channel.

Examples

The following example shows how to change the properties of an automatically created channel group to a persistent channel group:

```
switch# port-channel 10 persistent
```

Related Commands

Command	Description
show interface port-channel	Displays PortChannel interface information.
show port-channel	Displays PortChannel information.

port-group-monitor activate

To activate the specified Port Group Monitor policy, use the port-group-monitor activate command. To deactivate the Port Group Monitor poliy, use the no form of the command.

port-group-monitor activate name
no port-group-monitor activate name

Syntax Description

name	(Optional) Specifies the name of the port group policy. The maximum size is 32 characters.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to activate the Port Group Monitor policy:

```
switch(config)# port-group-monitor activate pgmon
switch(config)#
```

The following example shows how to deactivate the Port Group Monitor policy:

```
switch(config)# no port-group-monitor activate pgmon
switch(config)#
```

Related Commands

Command	Description
show port-group-monitor	Displays Port Group Monitor information.

port-group-monitor enable

To enable the Port Group Monitor feature, use the port-group-monitor enable command. To disable this feature, use the no form of the command.

port-group-monitor enable
no port-group-monitor enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enable.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to enable Port Group Monitor:

```
switch(config)# port-group-monitor enable
switch(config)#
```

The following example shows how to disable Port Group Monitor:

```
switch(config)# no port-group-monitor enable
switch(config)#
```

Related Commands

Command	Description
show port-group-monitor	Displays Port Group Monitor information.

port-group-monitor name

To create the Port Group Monitor policy, use the port-group-monitor name command. To delete Port Group Monitor policy, use the no form of the command.

port-group-monitor name *policy-name*
no port-group-monitor name *policy-name*

Syntax Description

policy-name	Displays the policy name. Maximum size is 32 characters.

Command Default

Rising threshold is 80, falling threshold is 20, and interval is 60.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to create Port Group Monitor policy name:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-group-monitor name pgmon
switch(config-port-group-monitor)#
```

The following example shows how to delete Port Group Monitor policy:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# no port-group-monitor name pgmon
switch(config)#
```

Related Commands

Command	Description
port-group-monitor activate	Activates the default port-group-monitor policy.
monitor counter	Configure monitoring of a specific counter within a Port Group Monitor policy.
counter	Configure individual counter in a port-group-monitor policy to use non-default values.
show port-group-monitor	Displays Port Group Monitor information.

port-license

To make a port eligible or ineligible to acquire a port activation license on a Cisco MDS 9124 switch, use the **port-license** command.

port-license acquire
no port-license acquire

Syntax Description

acquire	Grants a license to a port.

Command Default

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

If a port already has a license, then no action is taken and the port-license command returns successfully. If a license is unavailable, then the port will remain unlicensed.

Note This command is supported on the Cisco MDS 9124 switch only.

Examples

The following example shows how to make a port eligible to acquire a license:

```
switch# config t
switch (config)# interface fc1/1
switch (config-if)# port-license
```

The following example shows how to acquire a license for a port, and then copies the configuration to the startup configuration so that the new licensing configuration is maintained:

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)#
switch(config-if)# port-license acquire
switch(config-if)# end
switch# copy running-config startup-config
```

Related Commands

Command	Description
show port-licenses	Displays port licensing information for a Cisco MDS 9124 switch.

port-monitor activate

To activate the specified port monitor policy, use port-monitor activate command. To deactivate the policy, use the **no** form of the command.

port-monitor activate [{*name*}]
no port-monitor activate [{*name*}]

Syntax Description

name	(Optional) Name of PMON port policy.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

If no name is given, the port monitor activates the default policy. Presently one policy is activated on one port type. Two policies can be active but on different port types. If the specified policy is not active, it is a redundant operation.

Examples

The following example shows how to activate the port monitor default policy:

```
switch(config)# port-monitor activate
switch(config)#
```

The following example shows how to activate the port monitor Cisco policy:

```
switch(config)# port-monitor activate pmon_policy
switch(config)#
```

Related Commands

Command	Description
show port-monitor	Displays all port monitor policies.

port-monitor check-interval

To check errors at a lesser time interval compared to a poll interval, use the **port-monitor check-interval** command. To disable check-interval, use the no form of the command.

port-monitor check-interval *seconds*
no port-monitor check-interval *seconds*

Syntax Description

seconds	Specifies the check-interval time in seconds.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
7.3(1)D1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the check interval time to 30 seconds:

```
switch# configure terminal
switch(config)# port-monitor check-interval 30
```

Related Commands

Command	Description
show port-monitor	Displays all port monitor policies.

port-monitor enable

To enable the user to activate or deactivate policies, use the port-monitor enable command. To disable port monitor policies, use the no form of the command.

port-monitor enable
no port-monitor enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

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 enable port monitor:

```
switch(config)# port-monitor enable
switch(config)# no port-monitor enable
```

Related Commands

Command	Description
show port-monitor	Displays all port monitor policies.

port-monitor name

To configure a new port monitor policy and enters port monitor configuration mode, use the port-monitor name command. To delete port monitor policy, use the no form of the command.

port-monitor name *policy-name*
no port-monitor name *policy-name*

Syntax Description

policy-name	Displays the policy name.

Command Default

By default 16 individual counters are added and it defaults to port-type all.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

To enable the monitoring of various counters the following basic steps need to be done:

- Configure the port-monitor policy name
- Configure the types of ports included in the policy
- Configure any counters with non-default values that are needed
- Turn off the monitoring of any counters that are not needed (and are on by default) and turn on the monitoring of any counters that are needed if they are by default turned off
- Activate port-monitor policy

Examples

The following example shows how to create a user defined policy by name *cisco* and to assign the default values to the name:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-monitor name pmon_policy
switch(config-port-monitor)# show port-monitor pmon_policy
Policy Name  : pmon_policy
Admin status : Not Active
Oper status  : Not Active
Port type    : All Ports

Counter                  Threshold  Interval Rising Threshold      event Falling Threshold
     event  Warning Threshold    PMON Portguard
-------                  ---------  -------- -----------------      ----- ------------------
    -----  ------------------    --------------
Link Loss                Delta      60       5                     4     1
     4      Not enabled           Not enabled
Sync Loss                Delta      60       5                     4     1
     4      Not enabled           Not enabled
Signal Loss              Delta      60       5                     4     1
     4      Not enabled           Not enabled
Invalid Words            Delta      60       1                     4     0
```

```
     4      Not enabled           Not enabled
Invalid CRC's             Delta      60       5                    4     1
     4      Not enabled           Not enabled
State Change              Delta      60       100                  2     0
     4      Not enabled           Not enabled
TX Discards               Delta      60       200                  4     10
     4      Not enabled           Not enabled
LR RX                     Delta      60       5                    4     1
     4      Not enabled           Not enabled
LR TX                     Delta      60       5                    4     1
     4      Not enabled           Not enabled
Timeout Discards          Delta      60       200                  4     10
     4      Not enabled           Not enabled
Credit Loss Reco          Delta      1        1                    4     0
     4      Not enabled           Not enabled
TX Credit Not Available   Delta      1        10%                  4     0%
     4      Not enabled           Not enabled
RX Datarate               Delta      60       80%                  4     20%
     4      Not enabled           Not enabled
TX Datarate               Delta      60       80%                  4     20%
     4      Not enabled           Not enabled
TX-Slowport-Oper-Delay    Absolute   1        50ms                 4     0ms
     4      Not enabled           Not enabled
TXWait                    Delta      1        40%                  4     0%
     4      Not enabled           Not enabled
```

Related Commands

Command	Description
counter	Displays the individual counter.
monitor-counter	Configure the monitoring of a specific counter within a port-monitor policy.
port-monitor activate	Configures the specified port monitor policy.
port-type	Configures port type policies.
show port-monitor	Displays all port monitor policies.

port-security

To configure port security features and reject intrusion attempts, use the **port-security** command in configuration mode. Use the **no** form of the command to negate the command or revert to factory defaults.

port-security {**activate vsan** *vsan-id* [{**force**|**no-auto-learn**}]|**auto-learn vsan** *vsan-id*|**database vsan** *vsan-id* {**any-wwn**|**pwwn** *wwn*|**nwwn** *wwn*|**swwn** *wwn*} [{**fwwn** *wwn*|**interface** {**fc** *slot/port*|**port-channel** *number*}|**swwn wwn** [**interface** {**fc slot**/**port**|**port-channel number**}]}]}
no port-security {**activate vsan** *vsan-id* [{**force**|**no-auto-learn**}]|**auto-learn vsan** *vsan-id*|**database vsan** *vsan-id* {**any-wwn**|**pwwn** *wwn*|**nwwn** *wwn*|**swwn** *wwn*} [{**fwwn** *wwn*|**interface** {**fc** *slot/port*|**port-channel** *number*}|**swwn wwn** [**interface** {**fc slot**/**port**|**port-channel number**}]}]}

Syntax Description

activate	Activates a port security database for the specified VSAN and automatically enables auto-learn.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
force	(Optional) Forces the database activation.
no-auto-learn	(Optional) Disables the autolearn feature for the port security database.
auto-learn	Enables auto-learning for the specified VSAN.
database	Enters the port security database configuration mode for the specified VSAN.
any-wwn	Specifies any WWN to login to the switch.
nwwn *wwn*	Specifies the node WWN as the Nx port connection.
pwwn *wwn*	Specifies the port WWN as the Nx port connection.
swwn *wwn*	Specifies the switch WWN as the xE port connection.
fwwn *wwn*	Specifies a fabric WWN login.
interface	Specifies the device or switch port interface through which each device is connected to the switch.
fc *slot/port*	Specifies a Fibre Channel interface by the slot and port.
port-channel *number*	Specifies a PortChannel interface. The range is 1 to 128.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Release	Modification
2.0(x)	Add the optional **swwn** keyword to the subcommands under the **port-security database vsan** command.

Usage Guidelines

When you activate the port security feature, the **auto-learn** option is also automatically enabled. You can choose to activate the port-security feature and disable autolearn using the **port-security activate vsan** *number* **no-auto-learn** command. In this case, you need to manually populate the port security database by individually securing each port.

If the **auto-learn** option is enabled on a VSAN, you cannot activate the database for that VSAN without the **force** option.

Examples

The following example activates the port security database for the specified VSAN, and automatically enables autolearning:

```
switch# config terminal
switch(config)# port-security activate vsan 1
```

The following example deactivates the port security database for the specified VSAN, and automatically disables auto-learn:

```
switch# config terminal
switch(config)# no port-security activate vsan 1
```

The following example disables the auto-learn feature for the port security database in VSAN 1:

```
switch# config terminal
switch(config)# port-security activate vsan 1 no-auto-learn
```

The following example enables auto-learning so the switch can learn about any device that is allowed to access VSAN 1. These devices are logged in the port security active database:

```
switch# config terminal
switch(config)# port-security auto-learn vsan 1
```

The following example disables auto-learning and stops the switch from learning about new devices accessing the switch. Enforces the database contents based on the devices learnt up to this point.

```
switch# config terminal
switch(config)# no port-security auto-learn vsan 1
```

The following example enters the port security database mode for the specified VSAN:

```
switch# config terminal
switch(config)# port-security database vsan 1
switch(config-port-security)#
```

The following example configures any WWN to login through the specified interfaces:

```
switch(config-port-security)# any-wwn interface fc1/1 - fc1/8
```

The following example configures the specified pWWN to only log in through the specified fWWN.

```
switch(config-port-security)# pwwn 20:11:00:33:11:00:2a:4a fwwn 20:81:00:44:22:00:4a:9e
```

The following example deletes the specified pWWN configured in the previous step:

```
switch(config-port-security)# no pwwn 20:11:00:33:11:00:2a:4a fwwn 20:81:00:44:22:00:4a:9e
```

The following example configures the specified pWWN to only log in through the specified sWWN:

```
switch(config-port-security)# pwwn 20:11:00:33:11:00:2a:4a swwn 20:00:00:0c:85:90:3e:80
```

The following example deletes the specified pWWN configured in the previous step:

```
switch(config-port-security)# no pwwn 20:11:00:33:11:00:2a:4a swwn 20:00:00:0c:85:90:3e:80
```

The following example configures the specified nWWN to log in through the specified fWWN:

```
switch(config-port-security)# nwwn 26:33:22:00:55:05:3d:4c fwwn 20:81:00:44:22:00:4a:9e
```

The following example configures the specified pWWN to login through any port on the local switch:

```
switch(config-port-security)# pwwn 20:11:33:11:00:2a:4a:66
```

The following example configures the specified sWWN to only login through PortChannel 5:

```
switch(config-port-security)# swwn 20:01:33:11:00:2a:4a:66 interface port-channel 5
```

The following example configures any WWN to log in through the specified interface:

```
switch(config-port-security)# any-wwn interface fc3/1
```

The following example deletes the wildcard configured in the previous step:

```
switch(config-port-security)# no any-wwn interface fc2/1
```

The following example deletes the port security configuration database from the specified VSAN:

```
switch# config terminal
switch(config)# no port-security database vsan 1
switch(config)#
```

The following example forces the VSAN 1 port security database to activate despite conflicts:

```
switch(config)# port-security activate vsan 1 force
```

Related Commands

Command	Description
show port-security database	Displays configured port security information.

port-security abort

To discard the port security Cisco Fabric Services (CFS) distribution session in progress, use the **port-security abort** command **in configuration mode.**

port-security abort vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to discard a port security CFS distribution session in progress:

```
switch# config terminal
switch(config)# port-security abort vsan 33
```

Related Commands

Command	Description
port-security distribute	Enables CFS distribution for port security.
show port-security	Displays port security information.

port-security commit

To apply the pending configuration pertaining to the port security Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **port-security commit** command in configuration mode.

port-security commit vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to commit changes to the active port security configuration:

```
switch# config terminal
switch(config)# port-security commit vsan 13
```

Related Commands

Command	Description
port-security distribute	Enables CFS distribution for port security.
show port-security	Displays port security information.

port-security database

To copy the port security database or to view the difference within the port security database, use the **port-security database** command in EXEC mode.

port-security database {**copy**|**diff** {**active**|**config**}} **vsan** *vsan-id*

Syntax Description

copy	Copies the active database to the configuration database.
diff	Provides the difference between the active and configuration port security database.
active	Writes the active database to the configuration database.
config	Writes the configuration database to the active database.
vsan *vsan-id*	Specifies the VSAN ID. The ranges is 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

If the active database is empty, the port-security database is empty.

Use the **port-security database diff active** command to resolve conflicts.

Examples

The following example copies the active to the configured database:

```
switch# port-security database copy vsan 1
```

The following example provides the differences between the active database and the configuration database:

```
switch# port-security database diff active vsan 1
```

The following example provides information on the differences between the configuration database and the active database:

```
switch# port-security database diff config vsan 1
```

Related Commands

Command	Description
port-security database	Copies and provides information on the differences within the port security database.

Command	Description
show port-security database	Displays configured port security information.

port-security distribute

To enable Cisco Fabric Services (CFS) distribution for port security, use the **port-security distribute** command. To disable this feature, use the **no** form of the command.

port-security distribute
no port-security distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to distribute the port security configuration to the fabric:

```
switch# config terminal
switch(config)# port-security distribute
```

Related Commands

Command	Description
port-security commit	Commits the port security configuration changes to the active configuration.
show port-security	Displays port security information.

port-security enable

To enable port security, use the **port-security enable** command **in configuration mode.** To disable port security, use the **no** form of the command.

port-security enable
no port-security enable

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

Issuing the **port-security enable** command enables the other commands used to configure port security.

Examples

The following example shows how to enable port security:

```
switch# config terminal
switch(config)# port-security enable
```

The following example shows how to disable port security:

```
switch# config terminal
switch(config)# no port-security enable
```

Related Commands

Command	Description
show port-security	Displays port security information.

port-track enable

To enable port tracking for indirect errors, use the **port-track enable** command in configuration mode. To disable this feature, use the **no** form of the command.

port-track enable
no port-track enable

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

The software brings the linked port down when the tracked port goes down. When the tracked port recovers from the failure and comes back up again, the tracked port is also brought up automatically (unless otherwise configured).

Examples

The following example shows how to enable port tracking:

```
switch# config terminal
switch(config)# port-track enable
```

The following example shows how to disable port tracking:

```
switch# config terminal
switch(config)# no port-track enable
```

Related Commands

Command	Description
show interface fc	Displays configuration and status information for a specified Fibre Channel interface.
show interface port-channel	Displays configuration and status information for a specified PortChannel interface.

port-track force-shut

To force a shutdown of a tracked port, use the **port-track force-shut** command in interface configuration submode. To reenable the port tracking, use the **no** form of the command.

port-track force-shut
no port-track force-shut

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

Use the **port-track force-shut** to keep the linked port down, even though the tracked port comes back up. You must explicitly bring the port up when required using the **no port-track force-shut** command.

Examples

The following example shows how to force the shutdown of an interface and the interfaces that it is tracking:

```
switch# config terminal
switch(config)# interface fc 1/2
no port-track force-shut
```

Related Commands

Command	Description
port-track enable	Enables port tracking.
show interface fc	Displays configuration and status information for a specified Fibre Channel interface.
show interface port-channel	Displays configuration and status information for a specified PortChannel interface.

port-track interface

To enable port tracking for specific interfaces, use the **port-track interface** command **in interface configuration submode.** To disable this feature, use the **no** form of the command.

port-track interface {**fc** *slot/port*|**fcip** *port*|**gigabitethernet** *slot/port*|**port-channel** *port*} [**vsan** *vsan-id*]
no port-track interface {**fc** *slot/port*|**fcip** *port*|**gigabitethernet** *slot/port*|**port-channel** *port*} [**vsan** *vsan-id*]

Syntax Description

fc *slot*/*port*	Specifies a Fibre Channel interface.
fcip *port*	Specifies a FCIP interface.
gigabitethernet *slot*/*port*	Specifies a Gigabit Ethernet interface.
port-channel *port*	Specifies a PortChannel interface. The range is 1 to 128.
vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

When the ports that an interface is tracking goes down, the interface also goes down. When the tracked port comes backup, the linked interface also comes back up. Use the **port-track force-shut** command to keep the linked interface down.

Examples

The following example shows how to enable port tracking for specific interfaces:

```
switch# config terminal
switch(config)# interface fc 1/2
switch(config-if)# port-track interface port-channel 2
switch(config-if)# port-track interface fcip 5
```

Related Commands

Command	Description
port-track enable	Enables port tracking.
port-track force-shut	Forcefully shuts an interface for port tracking.
show interface fc	Displays configuration and status information for a specified Fibre Channel interface.

Command	Description
show interface port-channel	Displays configuration and status information for a specified PortChannel interface.

port-type

To configure the port types that a port-monitor policy monitors, use **port-type** command. To revert to the default port type, use the **no** form of the command.

port-type {**all | trunks | access-port**}
no port-type {**all | trunks | access-port**}

Syntax Description

all	Configures both trunk ports and access ports, except NP and TNP ports.
trunks	Configures only trunk ports (E and TE ports).
access-port	Configures only access ports (F and TF ports). NP and TNP ports are not supported in port monitor.

Command Default

The default port type is **all**.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

The default policy uses its own internal port type, which is the same as all ports.

Examples

The following example shows how to configure port monitoring for access ports:

```
switch# configure
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-monitor name cisco
switch(config-port-monitor)# port-type access-port
trying to get name
name is cisco
sending port type access
```

The following example shows how to configure port monitoring for all ports:

```
switch(config-port-monitor)# port-type all
trying to get name
name is cisco
sending port type all
```

The following example shows how to configure port monitoring for trunk ports:

```
switch(config-port-monitor)# port-type trunks
trying to get name
name is cisco
sending port type trunks
```

Note Currently, port monitor cannot monitor NP and TNP ports.

Related Commands

Command	Description
show port-monitor	Displays all port monitor policies.

power redundancy-mode (MDS 9500 switches)

To configure the capacity of the power supplies on the Cisco MDS 9500 Family of switches, use the **power redundancy-mode** command in configuration mode. Use the **no** form of the command to negate the command or revert to factory defaults.

power redundancy-mode {**combined [force]**|**redundant**}
no power redundancy-mode {**combined [force]**|**redundant**}

Syntax Description

combined	Configures power supply redundancy mode as combined.
force	Forces combined mode without prompting.
redundant	Configures power supply redundancy mode as redundant.

Command Default

Redundant mode.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If power supplies with different capacities are installed in the switch, the total power available differs based on the configured mode:

- In **redundant** mode, the total power is the lesser of the two power supply capacities. This reserves enough power to keep the system powered on in case of a power supply failure. This is the recommended or default mode.
- In **combined** mode, the total power is twice the lesser of the two power supply capacities. In case of a power supply failure, the entire system could be shut down, depending on the power usage at that time.
- When a new power supply is installed, the switch automatically detects the power supply capacity. If the new power supply has a capacity that is lower than the current power usage in the switch and the power supplies are configured in **redundant** mode, the new power supply will be shut down.
- When you change the configuration from **combined** to **redundant** mode and the system detects a power supply that has a capacity lower than the current usage, the power supply is shut down. If both power supplies have a lower capacity than the current system usage, the configuration is not allowed.

Examples

The following examples demonstrate how the power supply redundancy mode could be set:

```
switch(config)# power redundancy-mode combined
WARNING: This mode can cause service disruptions in case of a power supply failure. Proceed
 ? [y/n] y
switch(config)# power redundancy-mode redundant
```

Related Commands

Command	Description
copy running-config startup-config	Copies all running configuration to the startup configuration.
show environment power	Displays status of power supply modules, power supply redundancy mode, and power usage summary.

power redundancy-mode (MDS 9700 switch)

To configure the capacity of the power supplies on the Cisco MDS 9700 Family of switches, use the **power redundancy-mode** command in configuration mode. Use the **no** form of the command to negate the command or revert to factory defaults.

power redundancy-mode {**combined [force]**|**insrc-redundant**|**ps-redundant**|**redundant**}
no power redundancy-mode {**combined [force]**|**insrc-redundant**|**ps-redundant**|**redundant**}

Syntax Description

combined	Configures power supply redundancy mode as combined.
force	Forces combined mode without prompting.
insrc-redundant	Configure power supply redundancy mode as grid/AC input source redundant.
ps-redundant	Configure power supply redundancy mode as PS redundant.
redundant	Configures power supply redundancy mode as redundant.

Command Default

Redundant mode.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to configure the power supply redundancy mode as grid/AC input source redundant:

```
switch(config)# power redundancy-mode insrc-redundant
switch(config)# 2014 May 29 12:40:22 mds9706 %PLATFORM-4-PFM_PS_RED_MODE_CHG: Power redundancy
 mode changed to insrc-redundant
switch(config)# show environment power
Power Supply:
Voltage: 50 Volts
Power                                Actual        Total
Supply    Model                      Output     Capacity    Status
                                    (Watts )     (Watts )
-------  -------------------  -----------  -----------  --------------
1        DS-CAC97-3KW               333 W       3000 W     Ok
2        DS-CAC97-3KW               345 W       3000 W     Ok
3        DS-CAC97-3KW               345 W       3000 W     Ok
4        DS-CAC97-3KW               337 W       3000 W     Ok
                                   Actual        Power
Module    Model                      Draw    Allocated    Status
                                    (Watts )     (Watts )
-------  -------------------  -----------  -----------  --------------
1        DS-X9848-480K9             354 W        500 W    Powered-Up
```

```
3        DS-X97-SF1-K9              107 W        190 W    Powered-Up
4        DS-X97-SF1-K9              105 W        190 W    Powered-Up
6        DS-X9448-768K9             403 W        650 W    Powered-Up
Xb1      DS-X9706-FAB1               48 W         85 W    Powered-Up
Xb2      DS-X9706-FAB1               47 W         85 W    Powered-Up
Xb3      DS-X9706-FAB1               48 W         85 W    Powered-Up
Xb4      DS-X9706-FAB1               48 W         85 W    Powered-Up
Xb5      DS-X9706-FAB1               48 W         85 W    Powered-Up
Xb6      DS-X9706-FAB1               48 W         85 W    Powered-Up
fan1     DS-C9706-FAN                29 W        300 W    Powered-Up
fan2     DS-C9706-FAN                29 W        300 W    Powered-Up
fan3     DS-C9706-FAN                33 W        300 W    Powered-Up
N/A - Per module power not available
Power Usage Summary:
--------------------
Power Supply redundancy mode (configured)                InSrc-Redundant
Power Supply redundancy mode (operational)               InSrc-Redundant
Total Power Capacity (based on configured mode)               6000 W
Total Power of all Inputs (cumulative)                       12000 W
Total Power Output (actual draw)                              1360 W
Total Power Allocated (budget)                                3090 W
Total Power Available for additional modules                  2910 W
switch(config)#
```

The following example shows how to configure the power supply redundancy mode as PS redundant:

```
switch(config)# power redundancy-mode ps-redundant
switch(config)# 2014 May 29 12:40:22 mds9706 %PLATFORM-4-PFM_PS_RED_MODE_CHG: Power redundancy
 mode changed to ps-redundant
switch(config)# show environment power
Power Supply:
Voltage: 50 Volts
Power                               Actual        Total
Supply    Model                     Output     Capacity    Status
                                   (Watts )     (Watts )
-------  ------------------  -----------  -----------  --------------
1        DS-CAC97-3KW              333 W       3000 W     Ok
2        DS-CAC97-3KW              345 W       3000 W     Ok
3        DS-CAC97-3KW              345 W       3000 W     Ok
4        DS-CAC97-3KW              341 W       3000 W     Ok
                                  Actual        Power
Module    Model                     Draw    Allocated    Status
                                   (Watts )     (Watts )
-------  ------------------  -----------  -----------  --------------
1        DS-X9848-480K9            364 W        500 W    Powered-Up
3        DS-X97-SF1-K9             107 W        190 W    Powered-Up
4        DS-X97-SF1-K9             105 W        190 W    Powered-Up
6        DS-X9448-768K9            403 W        650 W    Powered-Up
Xb1      DS-X9706-FAB1              48 W         85 W    Powered-Up
Xb2      DS-X9706-FAB1              47 W         85 W    Powered-Up
Xb3      DS-X9706-FAB1              48 W         85 W    Powered-Up
Xb4      DS-X9706-FAB1              48 W         85 W    Powered-Up
Xb5      DS-X9706-FAB1              48 W         85 W    Powered-Up
Xb6      DS-X9706-FAB1              48 W         85 W    Powered-Up
fan1     DS-C9706-FAN               26 W        300 W    Powered-Up
fan2     DS-C9706-FAN               29 W        300 W    Powered-Up
fan3     DS-C9706-FAN               33 W        300 W    Powered-Up
N/A - Per module power not available
Power Usage Summary:
--------------------
Power Supply redundancy mode (configured)                PS-Redundant
Power Supply redundancy mode (operational)               PS-Redundant
Total Power Capacity (based on configured mode)               9000 W
Total Power of all Inputs (cumulative)                       12000 W
```

```
Total Power Output (actual draw)                             1364 W
Total Power Allocated (budget)                               3090 W
Total Power Available for additional modules                 5910 W
switch(config)#
```

Related Commands

Command	Description
copy running-config startup-config	Copies all running configuration to the startup configuration.
show environment power	Displays status of power supply modules, power supply redundancy mode, and power usage summary.

poweroff module

To power off individual modules in the system, use the **poweroff module** command in configuration mode. Use the **no** form of this command to power up the specified module.

poweroff module *slot*
no poweroff module *slot*

Syntax Description

slot	Specifies the slot number for the module.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use the **poweroff module** command to power off individual modules. The **poweroff module** command cannot be used to power off supervisor modules.

Examples

The following example powers off and powers up module 1:

```
switch# config terminal
switch(config)# poweroff module 1
switch(config)#
switch(config)# no poweroff module 1
switch(config)#
```

Related Commands

Command	Description
copy running-config startup-config	Copies all running configuration to the startup configuration.
show module	Displays information for a specified module.

priority

To configure the priority in a QoS policy map class, use the **priority** command in QoS policy class map configuration submode. To disable this feature, use the **no** form of the command.

priority {**high**|**low**|**medium**}
no priority {**high**|**low**|**medium**}

Syntax Description

high	Configures the frames matching the class-map as high priority.
low	Configures the frames matching the class-map as low priority.
medium	Configures the frames matching the class-map as medium priority.

Command Default

The default priority is low.

Command Modes

QoS policy map class configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Before you can configure the priority in a QoS policy map class you must first:

- Enable the QoS data traffic feature using the **qos enable** command.
- Configure a QoS class map using the **qos dwrr-q** command.
- Configure a QoS policy map using the **qos policy-map** command.
- Configure a QoS policy map class using the **class** command.

Examples

The following example shows how to select the QoS policy class-map1 and configure the frame priority as high:

```
switch(config-pmap)# class class-map1
switch(config-pmap-c)# priority high
Operation in progress. Please check class-map parameters
```

Related Commands

Command	Description
class	Configure a QoS policy map class.
qos class-map	Configures a QoS class map.
qos enable	Enables the QoS data traffic feature on the switch.
qos policy-map	Configures a QoS policy map.
show qos	Displays the current QoS settings.

priority-flow-control long-distance

To enable the long distance Priority Flow Control (PFC), use the **long-distance** command. To disable this feature, use the **no** form of the command.

priority-flow-control long-distance
no priority-flow-control long-distance

Syntax Description

This command has no arguments or keywords.

Command Default

Default value for **long-distance** is set to False.

Command Modes

Interface Configuration mode.

Command History

Release	Modification
6.2(9)	Added the long-distance keyword to the syntax description.

Usage Guidelines

This command does not require a license.

Examples

The following example shows how to enable the long distance priority flow control:

```
switch(config)#interface ethernet-port-channel 1023
switch(config-if)# priority-flow-control long-distance
switch(config-if)#
```

The following example shows how to disable the long distance priority flow control:

```
switch(config)#interface ethernet-port-channel 1023
switch(config-if)# no priority-flow-control long-distance
switch(config-if)#
```

Related Commands

Command	Description
show sys int eth-qos port-node ethernet *intf*	Displays all the attributes of the interface including long distance.

priority-flow-control mode

To enable the mode Priority Flow Control (PFC), use the **priority-flow-control mode** command. To disable this feature, use the **no** form of the command.

priority-flow-control mode {**auto**|**off**|**on**}
no priority-flow-control mode {**auto**|**off**|**on**}

Syntax Description

auto	Sets the PFC mode to automatic.
off	Sets the PFC mode to off.
on	Sets the PFC mode to on.

Command Default

Default value for **mode** is set to auto.

Command Modes

Interface Configuration mode.

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following example shows how to set the PFC mode to on:

```
switch# configure terminal
switch(config)# interface ethernet 2/5
switch(config-if)# priority-flow-control mode on
switch(config-if)#
```

The following example shows how to set the PFC mode to off:

```
switch# configure terminal
switch(config)# interface ethernet 2/5
switch(config-if)# priority-flow-control mode off
```

switch(config-if)#

Related Commands

Command	Description
show interface priority-flow-control	Displays the status of priority flow control (PFC) on all interfaces.

purge fcdomain fcid

To purge persistent FCIDs, use the **purge fcdomain fcid** command in EXEC mode.

purge fcdomain fcid vsan *vsan-id*

Syntax Description

vsan *vsan-id*	Indicates that FCIDs are to be purged for a VSAN ID. The range is 1 to 4093.

Command Default

None.

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 purge all dynamic unused FCIDs in VSAN 4:

```
switch# purge fcdomain fcid vsan 4
switch#
```

The following example shows how to purge all dynamic unused FCIDs in VSANs 4, 5, and 6:

```
switch# purge fcdomain fcid vsan 3-5
switch#
```

purge module

To delete configurations in the running configuration for nonexistent modules, use the **purge module** command in EXEC mode.

purge module *slot* **running-config**

Syntax Description

slot	Specifies the module slot number.
running-config	Purges the running configuration from the specified module.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command cannot be issued on a supervisor module.

Examples

The following example displays the output of the **purge module** command issued on the module in slot 8:

```
switch# purge module 8 running-config
switch#
```

pwc

To view your present working context (PWC), use the **pwc** command in any mode.

pwc

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

All.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows the present working context:

```
            switch# config t
switch(config)# islb initiator ip-address 120.10.10.2
switch(config-islb-init)# pwc
(config t) -> (islb initiator ip-address 120.10.10.2)
```

Related Commands

Command	Description
pwd	Displays the current directory location.

pwd

To display the current directory location, use the **pwd** command in EXEC mode.

pwd

Syntax Description

This command has no keywords or arguments.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example changes the directory and displays the current directory:

```
switch# cd bootflash:logs
switch# pwd
bootflash:/logs
```

Related Commands

Command	Description
cd	Changes the current directory to the specified directory.
dir	Displays the contents of a directory.

pwwn (DPVM database configuration submode)

To add a device to a dynamic port VSAN membership (DPVM) database using the pWWN, use the **pwwn** command in DPVM database configuration submode. To remove a device from a DPVM database using the pWWN, use the **no** form of the command.

pwwn *pwwn-id* **vsan** *vsan-id*
no pwwn *pwwn-id* **vsan** *vsan-id*

Syntax Description

pwwn-id	Specifies the port WWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh,* where *h* is a hexadecimal number.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

DPVM database configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Examples

The following example shows how to add an entry to the DPVM database:

```
switch# config terminal
switch(config)# dpvm database
switch(config-dpvm-db)# pwwn 11:22:33:44:55:66:77:88 vsan 1
```

The following example shows how to delete an entry from the DPVM database:

```
switch(config-dpvm-db)# no pwwn 11:22:33:44:55:66:77:88 vsan 1
```

Related Commands

Command	Description
dpvm database	Configures the DPVM database.
show dpvm	Displays DPVM database information.

pwwn (fcdomain database configuration submode)

To map a pWWN to a persistent FC ID for IVR, use the **pwwn** command in IVR fcdomain database configuration submode. To remove the mapping for the pWWN, use the **no** form of the command.

pwwn *pwwn-id fc-id*
no pwwn *pwwn-id*

Syntax Description

pwwn-id	Specifies the pWWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
fc-id	Specifies the FC ID of the device.

Command Default

None.

Command Modes

fcdomain database configuration submode.

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

Only one FC ID can be mapped to a pWWN.

Examples

The following example shows how to map the pWWN to the persistent FC ID:

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# native-autonomous-fabric-num 20 native-vsan 30 domain 15
switch(config-fcdomain-fcid)# pwwn 11:22:33:44:55:66:77:88 0x123456
```

The following example shows how to remove the mapping between the pWWN and the FC ID:

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# native-autonomous-fabric-num 20 native-vsan 30 domain 15
switch(config-fcdomain-fcid)# no pwwn 11:22:33:44:55:66:77:88
```

Related Commands

Command	Description
ivr fcdomain database autonomous-fabric-num	Creates IVR persistent FC IDs.
native-autonomous-fabric-num	Creates an IVR persistent FC ID database entry.
show ivr fcdomain database	Displays IVR fcdomain database entry information.

pwwn (fc-management database configuration submode)

To configure the device port WWN, use the **pwwn** command. To disable this feature, use the **no** form of the command.

pwwn *dev_pwwn* **feature** {**all**|**fcs**|**fdmi**|**unzoned-ns**|**zone**} **operation** {**both**|**read**|**write**}
no pwwn *dev_pwwn* **feature** {**all**|**fcs**|**fdmi**|**unzoned-ns**|**zone**} [**operation** {**both**|**read**|**write**}]

Syntax Description

dev-pwwn	The WWN of the device. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
feature	Specifies the name of the feature.
all	Enables or disables all FC-CT queries.
fcs	Enables or disables the FC-CT query for the fabric configuration server.
fdmi	Enables or disables the FC-CT query for Fabric Device Common Interface (FDMI).
unzoned-ns	Enables or disables the FC-CT query for unzoned name server.
zone	Enables or disables the FC-CT query for zone server.
operation	(Optional) Specifies the read and write management FC-CT query.
both	Specifies both read and write query.
read	Specifies the get query.
write	Specifies the write query.

Command Default

None.

Command Modes

FC-management mode.

Command History

Release	Modification
6.2(9)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure an entry in the FC management security database:

```
switch(config)# fc-management database vsan 1
switch(config-fc-mgmt)#
switch(config-fc-mgmt)# pwwn 1:1:1:1:1:1:1:1 feature all operation both
Successful.
switch(config-fc-mgmt)#
switch(config-fc-mgmt)# pwwn 2:2:2:2:2:2:2:2 feature all operation read
Successful.
```

```
switch(config-fc-mgmt)#
switch(config-fc-mgmt)# pwwn 3:3:3:3:3:3:3:3 feature all operation write
Successful.
switch(config-fc-mgmt)#
switch(config-fc-mgmt)# show fc-management database
Fc-Management Security Database
---------------------------------------------------------------
VSAN PWWN FC-CT Permissions per FC services
---------------------------------------------------------------
1 01:01:01:01:01:01:01:01 Zone(RW), Unzoned-NS(RW), FCS(RW), FDMI(RW)
1 02:02:02:02:02:02:02:02 Zone(R), Unzoned-NS(R), FCS(R), FDMI(R)
1 03:03:03:03:03:03:03:03 Zone(W), Unzoned-NS(W), FCS(W), FDMI(W)
---------------------------------------------------------------
Total 3 entriesswitch(config-fc-mgmt)#
```

Related Commands

Command	Description
fc-management database	Configures the Fibre Channel Common Transport (FC-CT) management security database.

pwwn (SDV virtual device configuration submode)

To add a pWWN to a virtual device, use the **pwwn** command in SDV virtual device configuration submode. To remove a pWWN from a virtual device, usethe **no** form of the command.

pwwn *pwwn-name* **[primary]**
no pwwn *pwwn-name* **[primary]**

Syntax Description

pwwn-name	Specifies the pWWN of a real device. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
primary	Configures the virtual device as a real device.

Command Default

None.

Command Modes

SDV virtual device configuration submode.

Command History

Release	Modification
3.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to add a pWWN to a virtual device:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# sdv virtual-device name sqa2 vsan 1
switch(config-sdv-virt-dev)# pwwn 21:00:00:04:cf:cf:45:40
```

Related Commands

Command	Description
sdv enable	Enables or disables SAN device virtualization.
show sdv statistics	Displays SAN device virtualization statistics.

Q Commands

qos class-map

To create and define a traffic class with match criteria that will be used to identify traffic, use the **qos class-map** command in configuration mode. To remove a previously-configured class, use the no form of the command.

qos class-map *class* [{**match-all**|**match-any**}]
no qos class-map *class*

Syntax Description

class-name	Specifies a class map name. Maximum length is 63 alphanumeric characters.
match-all	(Optional) Specifies a logical AND operator for all matching statements in this class. (default).
match-any	(Optional) Specifies a logical OR operator for all matching statements in this class.

Command Default

match-all

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can access this command only if you enable the QoS data traffic feature using the **qos enable** command.

Examples

The following example shows how to create a QoS class map and enter class map configuration mode:

```
switch# config terminal
switch(config)# qos class-map MyClass1
switch(config-cmap)#
```

Related Commands

Command	Description
show qos	Displays configured QoS information.

qos control

To configure the QOS for control and data packets, use the **qos control** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

qos control *value* **data** *value*
no qos control *value* **data** *value*

Syntax Description

value	Applies the control DSCP value to all FCIP frames in the control TCP connection.
data *value*	Applies the data DSCP value applies to all FCIP frames in the data TCP connection.

Command Default

Enabled.

Command Modes

Interface configuration mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Use this command to cause FCIP to mark outbound packets with the DSCP values desired. This will allow the IP network to apply QOS policies appropriately.

Examples

The following example configures the QOS for control and data packets:

```
switch# config terminal
switch(config)# interface fcip 2
switch(config-if)# qos control 1 data 62
switch(config-if)#
```

Related Commands

Command	Description
show interface fcip	Displays the FCIP interface including QoS settings.

qos control priority

To enable the QoS priority assignment for control traffic feature on the Cisco MDS 9000 family of switches, use the **qos control priority** command in configuration mode. To revert to the factory default, use the no form of the command.

qos control priority 0
no qos priority control 0

Syntax Description

0	Specifies the lowest priority. To revert to the highest priority, use the **no** form of the command.

Command Default

Enabled and priority 7 are the defaults.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example sets the QoS priority assignment to the highest level.

```
switch# config terminal
switch(config)# no qos control priority 0
```

Related Commands

Command	Description
show qos	Displays configured QoS information.

qos dwrr-q

To associate a weight with a deficit weighted round robin (DWRR) scheduler queue, use the **qos dwrr-q** command in configuration mode. To remove a previously configured class, use the no form of the command.

qos dwrr-q {**high**|**low**|**medium**} **weight** *value*
no qos dwrr-q {**high**|**low**|**medium**} **weight** *value*

Syntax Description

high	Assigns the DWRR queue high option to DWRR queues.
low	Assigns the DWRR queue low option to DWRR queues.
medium	Assigns the DWRR queue medium option to DWRR queues.
weight *value*	Specifies DWRR queue weight.

Command Default

10

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

You can access this command only if you enable the QoS data traffic feature using the **qos enable** command.

Examples

The following example specifies the DWRR queue priority:

```
switch# config terminal
switch(config)# qos dwrr-q high weight 50
```

The following example reverts to the default value of 10:

```
switch(config)# no qos dwrr-q high weight 50
```

Related Commands

Command	Description
show qos	Displays configured QoS information.

qos enable

To enable the QoS priority assignment for data traffic feature on the Cisco MDS 9000 family of switches, use the **qos enable** command in configuration mode. To disable the QoS priority assignment for control traffic feature, use the no form of the command.

qos enable
no qos enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example disables the QoS priority assignment feature:

```
switch# config terminal
switch(config)# qos enable
```

Related Commands

Command	Description
show qos	Displays configured QoS information.

qos policy-map

To specify the class of service, use the **qos policy-map** command in configuration mode. To remove a previously configured class, use the no form of the command.

qos policy-map *policy-name*
no qos policy-map *policy-name*

Syntax Description

policy-name	Specifies a policy map name. Maximum length is 63 alphanumeric characters.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

You can access this command only if you enable the QoS data traffic feature using the **qos enable** command.

As an alternative, you can map a class map to a Differentiated Services Code Point (DSCP). The DSCP is an indicator of the service level for a specified frame. The DSCP value ranges from 0 to 63. A dscp value of 46 is disallowed.

Examples

The following example creates a policy map called MyPolicy and places you in the policy-map submode:

```
switch(config)# qos policy-map MyPolicy
switch(config-pmap)#
```

Related Commands

Command	Description
qos enable	Enables the QoS data traffic feature on the switch.
show qos	Displays configured QoS information.

qos priority

To configure the quality of server (QoS) priority attribute in a zone attribute group, use the **qos priority** commandn **zone attribute configuration submode.** To revert to the default, use the **no** form of the command.

qos priority {**high**|**low**|**medium**}
no qos priority {**high**|**low**|**medium**}

Syntax Description

high	Specifies high priority.
low	Specifies low priority.
medium	Specifies medium priority.

Command Default

Low.

Command Modes

Zone attribute configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to set the QoS priority attribute for a zone attribute group:

```
switch# config terminal
switch(config)# zone-attribute-group name admin-attributes vsan 10
switch(config-attribute-group)# qos priority medium
```

Related Commands

Command	Description
show zone-attribute-group	Displays zone attribute group information.
zone-attribute-group name	Configures zone attribute groups.

qos service

To apply a service policy, use the **qos service** command in configuration mode. To remove a previously configured class, use the no form of the command.

qos service policy *policy-name* **vsan** *vsan-id*
no qos service policy *policy-name* **vsan** *vsan-id*

Syntax Description

policy*policy-name*	Associates a policy map with the VSAN.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

You can access this command only if you enable the QoS data traffic feature using the **qos enable** command.

Examples

The following example applies a configured policy to VSAN 3:

```
switch(config)# qos service policy MyPolicy vsan 3
Operation in progress. Please check policy-map parameters
```

The following example deletes a configured policy that was applied to VSAN 7:

```
switch(config)# no qos service policy OldPolicy vsan 7
Operation in progress. Please check policy-map parameters
```

Related Commands

Command	Description
show qos	Displays configured QoS information.

quiesce

To gracefully shut down an ISL in a PortChannel, use the **quiesce** command in configuration mode. To disable this feature, use the no form of the command.

quiesce interface fc *slot / port*
no queisce interface fc *slot / port*

Syntax Description

interface fc *slot/port*	Specifies the interface to be quiesced.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(2b)	This command was deprecated and the functionality integrated into the **shutdown** command.

Usage Guidelines

The following conditions return an error:

- The interface is not part of PortChannel.
- The interface is not up.
- The interface is the last operational interface in the PortChannel:

Examples

The following example gracefully shuts down the one end of the ISL link in a PortChannel:

```
switchA# quiesce interface fc 2/1
WARNING: this command will stop forwarding frames to the specified interfaces. It is intended
 to be used to gracefully shutdown interfaces in a port-channel. The procedure is:
1. quiesce the interfaces on both switches.
2. shutdown the interfaces administratively.
Do you want to continue? (y/n)  [n] y
```

Related Commands

Command	Description
show interface	Displays interface configuration and status information.

R Commands

radius abort

To discard a RADIUS Cisco Fabric Services (CFS) distribution session in progress, use the **radius abort** command in configuration mode.

radius abort

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to discard a RADIUS CFS distribution session in progress:

```
switch# config terminal
switch(config)# radius abort
```

Related Commands

Command	Description
radius distribute	Enables CFS distribution for RADIUS.
show radius	Displays RADIUS CFS distribution status and other details.

radius commit

To apply the pending configuration pertaining to the RADIUS Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **radius commit** command in configuration mode.

radius commit

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

After the "radius commit" is done the running configuration has been modified on all switches participating in radius distribution. You can then use the "copy running-config startup-config fabric" command to save the running-config to the startup-config on all the switches in the fabric.

Examples

The following example shows how to apply a RADIUS configuration to the switches in the fabric:

```
switch# config terminal
switch(config)# radius commit
```

Related Commands

Command	Description
radius distribute	Enables CFS distribution for RADIUS.
show radius	Displays RADIUS CFS distribution status and other details.

radius distribute

To enable Cisco Fabric Services (CFS) distribution for RADIUS, use the **radius distribute** command. To disable this feature, use the **no** form of the command.

radius distribute
no radius distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable RADIUS fabric distribution:

```
switch# config terminal
switch(config)# radius distribute
```

Related Commands

Command	Description
radius commit	Commits temporary RADIUS configuration changes to the active configuration.
show radius	Displays RADIUS CFS distribution status and other details.

radius-server deadtime

To set a periodic time interval where a nonreachable (nonresponsive) RADIUS server is monitored for responsiveness, use the **radius-server deadtime** command. To disable the monitoring of the nonresponsive RADIUS server, use the **no** form of the command.

radius-server deadtime *time*
no radius-server deadtime *time*

Syntax Description

time	Specifies the time interval in minutes. The range is 1 to 1440.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Setting the time interval to zero disables the timer. If the dead time interval for an individual RADIUS server is greater than zero (0), that value takes precedence over the value set for the server group.

When the dead time interval is 0 minutes, RADIUS server monitoring is not performed unless the RADIUS server is part of a server group and the dead time interval for the group is greater than 0 minutes.

Examples

The following example shows how to set a duration of 10 minutes:

```
switch# config terminal
switch(config)# radius-server deadtime 10
```

Related Commands

Command	Description
deadtime	Sets a time interval for monitoring a nonresponsive RADIUS server.
show radius-server	Displays all configured RADIUS server parameters.

radius-server directed-request

To specify a RADIUS server to send authentication requests to when logging in, use the **radius-server directed-request** command. To revert to sending the authentication request to the configured group, use the **no** form of the command.

radius-server directed-request
no radius-server directed-request

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The user can specify the username@servername during login. The user name is sent to the server name for authentication.

Examples

The following example shows how to specify a RADIUS server to send authentication requests to when logging in:

```
switch# config terminal
switch(config)# radius-server directed-request
```

Related Commands

Command	Description
show radius-server	Displays all configured RADIUS server parameters.
show radius-server directed request	Displays a directed request RADIUS server configuration.

radius-server host

To configure RADIUS server parameters, use the **radius-server host** command. Use the **no** form of this command to revert to the factory defaults.

radius-server host {*server-name*|*ipv4-address*|*ipv6-address*} [**key** [{**0**|**7**}] *shared-secret*] **[accounting]** [**acct-port** *port-number*] [**auth-port** *port-number*] **[authentication]** [**retransmit** *count*] [**test** {**idle-time** *time*|**password** *password*|**username** *name*}] [**timeout** *seconds* [**retransmit** *count*]]
no radius-server host {*server-name*|*ipv4-address*|*ipv6-address*} [**key** [{**0**|**7**}] *shared-secret*] **[accounting]** [**acct-port** *port-number*] [**auth-port** *port-number*] **[authentication]** [**retransmit** *count*] [**test** {**idle-time** *time*|**password** *password*|**username** *name*}] [**timeout** *seconds* [**retransmit** *count*]]

Syntax Description

server-name	Specifies the RADIUS server DNS name. Maximum length is 253 characters.
ipv4-address	Specifies the RADIUS server IP address in the format *A.B.C.D* .
ipv6-address	Specifies the RADIUS server IP address in the format *X:X::X* .
auth-port *port-number*	(Optional) Configures the RADIUS server port for authentication.
acct-port *port-number*	(Optional) Configures the RADIUS server port for accounting.
authentication	Configures authentication.
retransmit *count*	(Optional) Configures the number of times the switch tries to connect to a RADIUS server(s) before reverting to local authentication. The range is 1 to five times and the default is 1 time.
accounting	(Optional) Configures accounting.
key	(Optional) Configures the RADIUS server shared secret key.
0	(Optional) Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the RADIUS client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the RADIUS client and server.
shared-secret	Configures a preshared key to authenticate communication between the RADIUS client and server.
test	(Optional) Configures parameters to send test packets to the RADIUS server.
idle-time*time*	Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.
password*password*	Specifies a user password in the test packets. The maximum size is 32.
username*name*	Specifies a user name in the test packets. The maximum size is 32.
timeout *seconds*	(Optional) Specifies the timeout (in seconds) between retransmissions to the RADIUS server. The default is 1 second and the valid range is 1 to 60 seconds.

Command Default

Idle-time is not set. Server monitoring is turned off.

Timeout is 1 second.

Username is test.

Password is test.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 4.1(3)	Changed the command output.
1.0(2)	This command was introduced.
3.0(1)	Added the *ipv6-address* argument and the **test** option.

Usage Guidelines

When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

Examples

The following example configures RADIUS server authentication parameters:

```
switch# config terminal
switch(config)# radius-server host 10.10.2.3 key HostKey
switch(config)# radius-server host 10.10.2.3 auth-port 2003

switch(config)# radius-server host 10.10.2.3 acct-port 2004
switch(config)# radius-server host 10.10.2.3 accounting
switch(config)# radius-server host radius2 key 0 abcd
switch(config)# radius-server host radius3 key 7 1234
switch(config)# radius-server host 10.10.2.3 test idle-time 10
switch(config)# radius-server host 1.1.1.1 test username user1 password pass idle-time 1
switch(config)# radius-server host 10.10.2.3 test username tester
switch(config)# radius-server host 10.10.2.3 test password 2B9ka5
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server key

To configure a global RADIUS shared secret, use the **radius-server key** command. Use the **no** form of this command to removed a configured shared secret.

radius-server key [{**0**|**7**}] *shared-secret*
no radius-server key [{**0**|**7**}] *shared-secret*

Syntax Description

0	(Optional) Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the RADIUS client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the RADIUS client and server.
shared-secret	Configures a preshared key to authenticate communication between the RADIUS client and server.

Command Default

No RADIUS key is configured.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You need to configure the RADIUS preshared key to authenticate the switch to the RADIUS server. The length of the key is restricted to 65 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all RADIUS server configurations on the switch. You can override this global key assignment by explicitly using the **key** option in the **radius-server host** command. Global key configuration is exempted from CFS distribution.

Examples

The following examples provide various scenarios to configure RADIUS authentication:

```
switch# config terminal
switch(config)# radius-server key AnyWord
switch(config)# radius-server key 0 AnyWord
switch(config)# radius-server key 7 public
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server retransmit

To globally specify the number of times the switch should try a request with a RADIUS server, use the **radius-server retransmit** command. To revert to default value, use the **no** form of the command.

radius-server retransmit *count*
no radius-server retransmit *count*

Syntax Description

count	Configures the number of times the switch tries to connect to a RADIUS server(s) before reverting to local authentication. The range is 1 to 5 times.

Command Default

1 retransmission

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures the number of retransmissions to 3:

```
switch# config terminal
switch(config)# radius-server retransmit 3
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server test

To configure the test parameter for an individual server, use the radius-server test command. To disable this feature, use the no form of the command.

radius-server test {{**username** *username*|{[**password** *password* [**idle-time** *time*]]|[**idle-time** *time*]}}|**password** *password* [**idle-time** *time*]|**idle-time** *time*}
no radius-server test {{**username** *username*|{[**password** *password* [**idle-time** *time*]]|[**idle-time** *time*]}}|**password** *password* [**idle-time** *time*]|**idle-time** *time*}

Syntax Description

username	Specifies the username in test packets.
user name	Specifies the username. The maximum size is 32 characters.
password	(Optional) Specifies the user password in test packets.
password	Specifies the user password. The maximun size is 32 characters.
idle-time	(Optional) Specifies the time interval for monitoring the server.
time period	Specifies the time period in minutes. The range is from 1 to 4440.

Command Default

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

Defaults will be used for anything not provided by CLI. Also doing a "no" of any parameters will revert it back to default.

Examples

The following example shows how to display the username in test packets:

```
switch# config t
switch(config)# radius-server test username test idle-time 0
switch(config)# radius-server test username test password test idle-time 0
switch(config)#
```

The following example shows how to display the time interval for monitoring the server:

```
switch(config)# radius-server test idle-time 0
switch(config)#
```

The following example shows how to display the user password in test packets:

```
switch(config)# radius-server test password test idle-time 0
switch(config)#
```

Related Commands

Command	Description
show radius-server	Displays all configured RADIUS server parameters.

radius-server timeout

To specify the time between retransmissions to the RADIUS servers, use the **radius-server timeout** command. You can revert the retransmission time to its default by issuing the **no** form of the command.

radius-server timeout *seconds*
no radius-server timeout *seconds*

Syntax Description

seconds	Specifies the time (in seconds) between retransmissions to the RADIUS server. The range is 1 to 60 seconds.

Command Default

1 second

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures the timeout value to 30 seconds:

```
switch# config terminal
switch(config)# radius-server timeout 30
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

rate-mode bandwidth-fairness

To enable or disable bandwidth fairness among ports in a port group, use the **rate-mode bandwidth-fairness** command in configuration mode. To disable bandwidth fairness, use the **no** form of the command.

rate-mode bandwidth-fairness module *module-id*
no rate-mode bandwidth-fairness module *module-id*

Syntax Description

module *module-id*	Specifies the module number.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.1(2)	This command was introduced.

Usage Guidelines

Enter the command separately for each module you want to enable or disable bandwidth fairness.

Note This feature is only supported on 48-port and 24-port 4-Gbps Fibre Channel switching modules.

Examples

The following example shows how to enable bandwidth fairness for a module:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rate-mode bandwidth-fairness module 1
```

The following example shows how to disable bandwidth fairness for a module:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# no rate-mode bandwidth-fairness module 1
```

Related Commands

Command	Description
show module bandwidth-fairness	Displays bandwidth fairness status.

rate-mode oversubscription-limit

To enable or disable restrictions on oversubscription ratios, use the rate-mode oversubscription-limit command.

rate-mode oversubscription-limit module *module number*
no rate-mode oversubscription-limit module *module number*

Syntax Description

module *module-number*	Identifies the specific module on which oversubscription ratio restrictions will be enabled or disabled.

Command Default

Oversubscription ratios are restricted for all 24-port and 48-port switching modules.

Command Modes

Configuration mode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When restrictions on oversubscription ratios are disabled, the bandwidth allocation among the shared ports is proportionate to the configured speed (if the configured speed is auto, then bandwidth is allocated assuming a speed of 4 Gbps).

You must explicitly shut down and take out of service shared ports before disabling oversubscription ratio restrictions on them.

The configuration is not saved to the startup configuration unless you explicitly enter the **copy running-config startup-config** command.

Caution You must enable restrictions on oversubscription ratios before you can downgrade modules to a previous release.

Examples

The following example disables restrictions on oversubscription ratios for a module (there are only dedicated ports, so a shutdown is not necessary):

```
switch# config t
switch(config)# no rate-mode oversubscription-limit module 2
```

The following example shows how to view the status of a module's oversubscription ratios:

```
switch# show running-config
version 3.1(1)
...
no rate-mode oversubscription-limit module 2
interface fc2/1
  switchport speed 2000
interface fc2/1
...
```

Related Commands

Command	Description
copy running-config startup-config	Saves the new oversubscription ratio configuration to the startup configuration.
show port-resources module	Displays the rate mode status of ports.

read command-id

To configure a SCSI read command for a SAN tuner extension N port, use the **read command-id** command.

read command-id *cmd-id* **target** *pwwn* **transfer-size** *bytes* [**outstanding-ios** *value* [{**continuous**|**num-transactions** *number*}]]

Syntax Description

cmd-id	Specifies the command identifier. The range is 0 to 2147483647.
target *pwwn*	Specifies the target port WWN. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
transfer-size *bytes*	Specifies the transfer size in multiples of 512 bytes. The range is 512 to 8388608.
outstanding-ios *value*	(Optional) Specifies the number of outstanding I/Os. The range is 1 to 1024.
continuous	(Optional) Specifies that the command is performed continuously.
num-transactions *number*	(Optional) Specifies a number of transactions. The range is 1 to 2147483647.

Command Default

None.

Command Modes

SAN extension N port configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To stop a SCSI read command in progress, use the **stop** command.

Examples

The following example configures a continuous SCSI read command:

```
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)# read command-id 100 target 22:22:22:22:22:22:22:22 transfer-size
512000 outstanding-ios 2 continuous
```

Related Commands

Command	Description
nport pwwn	Configures a SAN extension tuner N port.
san-ext-tuner	Enables the SAN extension tuner feature.
show san-ext-tuner	Displays SAN extension tuner information.
stop	Cancels a SCSI command in progress on a SAN extension tuner N port.

read-only

To configure the read-only attribute in a zone attribute group, use the **read-only** command **in zone attribute configuration submode.** To revert to the default, use the **no** form of the command.

read-only
no read-only

Syntax Description

This command has no other arguments or keywords.

Command Default

Read-write.

Command Modes

Zone attribute configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

This command only configures the read-only attribute for enhanced zoning. To enable broadcast zoning for basic mode, use the **attribute read-only** subcommand after entering zone configuration mode using the **zone name** command.

Examples

The following example shows how to set the read-only attribute for a zone attribute group:

```
switch# config terminal
switch(config)# zone-attribute-group name admin-attributes vsan 10
switch(config-attribute-group)# read-only
```

Related Commands

Command	Description
show zone-attribute-group	Displays zone attribute group information.
zone mode enhanced vsan	Enables enhanced zoning for a VSAN.
zone name	Configures zone attributes.
zone-attribute-group name	Configures zone attribute groups.

reload

To reload the entire switch, an active supervisor module, a standby supervisor module, or a specific module, or to force a netboot on a given module, use the **reload** command in EXEC mode.

reload [**module** *module-number* **force-dnld**]

Syntax Description

module *module-number*	(Optional) Reloads a specific module or active/standby supervisor module.
force-dnld	(Optional) Reloads, initiates netboot, and forces the download of the latest module firmware version to a specific module.

Command Default

Reboots the entire switch.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use the **reload** command to reboot the system, or to reboot a specific module, or to force a netboot on a specific module. The **reload** command used by itself, powers down all the modules and reboots the supervisor modules.

Use the **reload module** *module-number* command, if the given slot has a module or standby supervisor module, to power-cycle that module. If the given slot has an active supervisor module, then it causes the currently active supervisor module to reboot and the standby supervisor module becomes active.

The **reload module** *module-number* **force-dnld** command is similar to the previous command. This command forces netboot to be performed. If the slot contains a module, then the module netboots with the latest firmware and updates its corresponding flash with this image.

Examples

The following example uses **reload** to reboot the system:

```
switch# reload
This command will reboot the system. (y/n)? y
```

The following example uses reload to initiate netboot on a specific module:

```
switch# reload module 8 force-dnld
```

The following example uses **reload** to reboot a specific module:

```
switch# reload module 8
reloading module 8 ...
```

The following example uses **reload** to reboot an active supervisor module:

```
switch# reload module 5
This command will cause supervisor switchover. (y/n)? y
```

Related Commands

Command	Description
copy system:running-config nvram:startup-config	Copies any file from a source to a destination.
install	Installs a new software image.

revocation-check

To configure trust point revocation check methods, use the **revocation-check** command in trust point configuration submode. To discard the revocation check configuration, use the **no** form of the command.

revocation-check {**crl** [{**none**|**ocsp** [**none**]}]|**none**|**ocsp** [{**crl** [**none**]|**none**}]}
no revocation-check {**crl** [{**none**|**ocsp** [**none**]}]|**none**|**ocsp** [{**crl** [**none**]|**none**}]}

Syntax Description

crl	Specifies the locally stored certificate revocation list (CRL) as the place to check for revoked certificates.
none	(Optional) Specifies that no checking be done for revoked certificates.
ocsp	(Optional) Specifies the Online Certificate Status Protocol (OCSP) for checking for revoked certificates.

Command Default

By default, the revocation checking method for a trust point is CRL.

Command Modes

Trust point configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You must authenticate the CA and configure the OCSP URL before configuring OCSP as a revocation checking method.

The revocation checking configuration allows one or more of the methods to be specified as an ordered list for revocation checking. During peer certificate verification, each method is tried in the specified order until one method succeeds by providing the revocation status. When none is specified as the method, it means that there is no need to check the revocation status, which treats the peer certificate as not revoked. If none is the first method specified in the method list, subsequent methods are not allowed to be specified because checking is not required.

Examples

The following example shows how to check for revoked certificates using OCSP on a URL that must have been previously configured:

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# revocation-check oscp
```

The following example shows how to check for revoked certificates in the locally stored CRL:

```
switch(config-trustpoint)# revocation-check crl
```

The following example shows how to check revocation status first using locally cached CRL and then, if needed, using OCSP. If CRL is not yet cached locally, only OCSP checking is attempted:

```
switch(config-trustpoint)# revocation-check crl ocsp
```

The following example shows how to do no checking for revoked certificates:

```
switch(config-trustpoint)# revocation-check none
```

Related Commands

Command	Description
crypto ca crl-request	Configures a CRL or overwrites the existing one for the trust point CA.
ocsp url	Configures details of the trust point OSCP.
show crypto ca crl	Displays configured CRLs.

rlir preferred-cond fcid

To specify a preferred host to receive Registered Link Incident Report (RLIR) frames, use the **rlir preferred-cond fcid** command in configuration mode. To remove a preferred host, use the **no** form of the command.

rlir preferred-cond fcid *fc-id* **vsan** *vsan-id*
no rlir preferred-cond fcid *fc-id* **vsan** *vsan-id*

Syntax Description

fcid *fc-id*	Specifies the FC ID. The format is **0x**>*hhhhhh* .
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

By default, the MDS switch sends RLIR frames to one of the hosts in the VSAN with the register function set to “conditionally receive” if no hosts have the register function set to “always receive.”

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(3)	This command was introduced.

Usage Guidelines

The MDS switch sends RLIR frames to the preferred host only if it meets the following conditions:

- No host in the VSAN is registered for RLIR with the registration function set to “always receive.” If one or more hosts in the VSAN are registered as “always receive,” then RLIR sends only to these hosts and not to the configured preferred host.
- The preferred host is registered with the registration function set to “conditionally receive.”

Note If all registered hosts have the registration function set to “conditionally receive,” then the preferred host receives the RLIR frames.

You can specify only one RLIR preferred host per VSAN.

Examples

The following example specifies FC ID 0x654321 as the RLIR preferred host for VSAN 2:

```
switch# config t
switch(config)# rlir preferred-cond fcid 0x654321 vsan 2
```

The following example removes FC ID 0x654321 as the RLIR preferred host for VSAN 2:

```
switch# config t
switch(config)# no rlir preferred-cond fcid 0x654321 vsan 2
```

Related Commands

Command	Description
show rlir	Displays information about RLIR, Link Incident Record Registration (LIRR), and Distribute Registered Link Incident Record (DRLIR) frames.
clear rlir	Clears the RLIRs.
debug rlir	Enables RLIR debugging.

rmdir

To delete an existing directory from the flash file system, use the **rmdir** command in EXEC mode.

rmdir [{**bootflash:**|**slot0:**|**volatile:**}] *directory*

Syntax Description

bootflash:	(Optional) Source or destination location for internal bootflash memory.
slot0:	(Optional) Source or destination location for the CompactFlash memory or PCMCIA card.
volatile:	(Optional) Source or destination location for volatile file system.
directory	Name of the directory to remove.

Command Default

Uses the current default directory.

Command Modes

EXEC Mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command is only valid on flash file systems.

The **rmdir** command deletes an existing directory at the current directory level or at a specified directory level. The directory must be empty to be deleted.

Examples

The following example deletes the directory called test in the slot0 directory:

```
switch# rmdir slot0:test
```

The following example deletes the directory called test at the current directory level. If the current directory is slot0:mydir, this command deletes the slot0:mydir/test directory.

```
switch# rmdir delete
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
mkir	Creates a new directory in the flash file system.

rmon alarm

To configure a 32 bit remote monitoring (RMON) alarm, use the **rmon alarm** command **in configuration mode.** To delete an RMON alarm, use the **no** form of the command.

rmon alarm *alarm-number mib-object sample-interval* {**absolute|delta**} **rising-threshold** *value* [*rising-event*] **falling-threshold** *value* [*falling-event*] [**owner** *alarm-owner*]
no rmon alarm *alarm-number*

Syntax Description

alarm-number	Specifies the RMON alarm number. The range is 1 to 65535.
mib-object	Specifies the MIB object to monitor. Maximum length is 80 characters. **Note** The MIB object identifier must be fully numbered, dotted-decimal notation, not the text string description.
sample-interval	Specifies the sample interval in seconds. The range is 1 to 2147483647.
absolute	Tests each sample directly.
delta	Tests the difference (delta) between the current and previous sample.
rising-threshold *value*	Specifies the rising threshold value. The range is –2147483648 to 2147483647.
rising-event	(Optional) Specifies the event to trigger on rising threshold crossing. The range is 1 to 65535. If no event is specified, event 0 is used.
falling-threshold *value*	Specifies the falling threshold value. The range is –2147483648 to 2147483647.
falling-event	(Optional) Specifies the event to trigger on rising threshold crossing. The range is 1 to 65535. If no event is specified, event 0 is used.
owner *alarm-owner*	(Optional) Specifies an owner for the alarm. Maximum size is 80 characters.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

Use the rmon event command to configure the events for alarms.

The maximum number of RMON alarms currently is only configurable through the device manager and threshold manager GUI. A CLI command is not available to change this maximum value.

Note We recommend setting alarm sample intervals to 30 seconds or higher to prevent excessive load on the system.

Examples

The following example configures a 32-bit alarm number 20 for ifInErrors (OID 1.3.6.1.2.1.2.2.1.14) on interface fc 1/1. The sample interval is 30 seconds and delta samples are tested. The rising threshold is 15 errors per sample window; reaching this level triggers event 1. The falling threshold is 0 errors in the sample window which triggers event 0 (no action). The owner is 'ifInErrors.fc1/1@test'.

```
switch# config terminal
switch(config)# rmon alarm 20 1.3.6.1.2.1.2.2.1.14.16777216 30 delta rising-threshold 15
1 falling-threshold 0 owner ifInErrors.fc1/1@test
```

Related Commands

Command	Description
rmon event	Configures an RMON event.
rmon hcalarm	Configures the 64-bit RMON alarm.
show rmon	Displays RMON configuration and logging information.
show snmp host	Displays the SNMP trap destination information.
snmp-server host	Specifies the recipient of an SNMP notification.

rmon event

To configure a remote monitoring (RMON) event, use the **rmon event** command **in configuration mode.** To delete an RMON event, use the **no** form of the command.

rmon event *event-number* [{**description** *text* [**owner** *owner-name*]|**log** [**trap** *community-string*] [**description** *text*] [**owner** *owner-name*]|**trap** *community-string* [**description** *text*] [**owner** *owner-name*]|**owner** *owner-name*}]
no rmon event *event-number*

Syntax Description

event-number	Specifies the RMON event number. The range is 1 to 65535.
description *text*	(Optional) Specifies a description of the event. Maximum length is 80 characters.
owner *owner-name*	(Optional) Specifies an owner for the alarm. Maximum length is 80 characters.
log	(Optional) Generates an RMON log entry in the onboard RMON log when the event is triggered by an alarm.
trap *community-string*	(Optional) Generates an SNMP trap with the specified community name when the event is triggered by an alarm. The maximum length is 32 characters.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
4.1(1b)	Modified the command output.
2.0(x)	This command was introduced.

Usage Guidelines

You can trigger the events created by this command with alarms configured using the **rmon alarm** or **rmon hcalarm** commands

The log option logs the event to a local log file on the MDS switch. The trap option uses the onboard SNMP agent to send an SNMP trap to a remote NMS.

Note Events can be used by both **rmon alarm** (32-bit) and **hcalarm** (64-bit) commands.

Examples

The following example configures RMON event1 to log the onboard RMON log and send an SNMP trap to public community trap destinations. The description is public and is owned by switchname.

```
switch# config terminal
rmon event 1 log trap public description FATAL(1) owner !switchname
switch(config)#
```

The following example configures RMON event3 to log the onboard RMON log and send an SNMP trap to public community trap destinations. The description is error and is owned by switchname:

```
switch# config terminal
rmon event 3 log trap public description ERROR(3) owner !switchname
switch(config)#
```

The following example configures RMON event4 to log the onboard RMON log and send an SNMP trap to public community trap destinations. The description is warning and is owned by switchname:

```
switch# config terminal
rmon event 4 log trap public description WARNING(4) owner !switchname
switch(config)#
```

The following example configures RMON event5 to log the onboard RMON log and send an SNMP trap to public community trap destinations. The description is information and is owned by switchname:

```
switch# config terminal
rmon event 4 log trap public description INFORMATION(5) owner !switchname
switch(config)#
```

The following example configures RMON event 2 to log the onboard RMON log and send an SNMP trap to public community trap destinations. The description is CriticalErrors and is owned by test:

```
switch# config terminal
switch(config)# rmon event 2 log trap public description CriticalErrors owner
 test
```

Related Commands

Command	Description
rmon alarm	Configures a 32-bit RMON alarm.
rmon hcalarm	Configures a 64-bit RMON alarm.
show rmon	Displays RMON configuration and logging information.

rmon hcalarm

To configure a 64-bit remote monitoring (RMON) high-capacity alarm (hcalarm), use the **rmon hcalarm** command in configuration mode. To delete an RMON hcalarm, use the **no** form of the command.

rmon hcalarm *alarm-number mib-object sample-interval* {**absolute**|**delta**} {**rising-threshold-high** *value* **rising-threshold-low** *value* [*rising-event*] [**falling-threshold-high** *value* **falling-threshold-low** *value* [*falling-event*]]|**falling-threshold-high** *value* **falling-threshold-low** *value* [*falling-event*]} [**owner** *alarm-owner*]
no rmon hcalarm *alarm-number mib-object sample-interval* {**absolute**|**delta**} {**rising-threshold-high** *value* **rising-threshold-low** *value* [*rising-event*] [**falling-threshold-high** *value* **falling-threshold-low** *value* [{*falling-event*}]]|**falling-threshold-high** *value* **falling-threshold-low** *value* [*falling-event*]} [**owner** *alarm-owner*]

Syntax Description

alarm-number	Specifies the RMON hcalarm number. The range is 1 to 65535.
mib-object	Specifies the MIB object to monitor. Maximum length is 80 characters. **Note** The MIB object identifier must be fully numbered, dotted-decimal notation, not the text string description.
sample-interval	Specifies the sample interval in seconds. The range is 1 to 65535.
absolute	Tests each sample directly.
delta	Tests the difference (delta) between the current and previous sample.
rising-threshold-high *value*	Configures the upper 32 bits of the 64-bit rising threshold value. The range is 0 to 4294967295.
rising-threshold-low *value*	Configures the lower 32 bits of the 64-bit rising threshold value. The range is 0 to 4294967295.
rising-event	(Optional) Specifies the event to trigger on rising threshold crossing. The range is 1 to 65535.
falling-threshold-high *value*	Configures the upper 32 bits of the 64-bit falling threshold value. The range is 0 to 4294967295.
falling-threshold-low *value*	Configures the lower 32 bits of the 64-bit falling threshold value. The range is 0 to 4294967295.
falling-event	(Optional) Specifies the event to trigger on falling threshold crossing. The range is 0 to 65535.
owner *alarm-owner*	(Optional) Specifies an owner for the alarm. Maximum size is 80 characters.

Command Default

64-bit alarms.

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Event number 0 is a predefined null (or no operation) event. When no event is specified by the user in an alarm this event is automatically used by the system. The event causes no action to be taken when triggered, however, the alarm is still reset. The event cannot be redefined by the user. It is a predefined event and you can only create events in the range from 1 to 65535.

To configure a high-capacity RMON alarm, use the CISCO-HC-ALARM-MIB.

The maximum number of RMON alarms is currently configurable through the device manager and threshold manager GUI. A CLI command is not available to change this maximum value.

Note We recommand setting alarm sample intervals to 30 seconds or higher to prevent excessive load on the system.

Examples

The following example configures 64-bit alarm number 2 for ifHCInOctets (OID 1.3.6.1.2.1.31.1.1.1.6) on interface fc 12/1. The sample interval is 30 seconds and delta samples are tested. The rising threshold is 240,000,000,000 bytes per sample window (an average of 8,000,000,000 bytes per second); reaching this level triggers event 4. The falling threshold is 180,000,000,000 bytes in the sample window (an average of 6,000,000,000 bytes per second) which triggers event 0 (no action) and resets the alarm. The owner is 'ifHCInOctets.fc12/1@test'.

```
switch# config terminal
switch#(config) rmon hcalarm 2 1.3.6.1.2.1.31.1.1.1.6.22544384 30 delta  rising-threshold-high
 55 rising-threshold-low 3776798720 4 falling-threshold-high 41  falling-threshold-low
3906340864 owner ifHCInOctets.fc12/1@test
```

Related Commands

Command	Description
rmon alarm	Configures a 32-bit RMON alarm.
rmon event	Configures an RMON event.
rmon hcalarm	Configures a 64-bit RMON alarm.
show rmon	Displays RMON configuration and logging information.
show snmp host	Displays the SNMP trap destination information.
snmp-server host	Specifies the recipient of an SNMP notification.

role abort

To discard an authorization role Cisco Fabric Services (CFS) distribution session in progress, use the **role abort** command in configuration mode.

role abort

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to discard an authorization role CFS distribution session in progress:

```
switch# config terminal
switch(config)# role abort
```

Related Commands

Command	Description
role distribute	Enables CFS distribution for authorization roles.
show role	Displays authorization role information.

role commit

To apply the pending configuration pertaining to the authorization role Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **role commit** command in configuration mode.

role commit

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Note Once the "role commit" is done the running configuration has been modified on all switches participating in the role distribution. You can then use the "copy running-config startup-config fabric" command to save the running-config to the startup-config on all the switches in the fabric.

Examples

The following example shows how to apply an authorization role configuration to the switches in the fabric:

```
switch# config terminal
switch(config)# role commit
```

Related Commands

Command	Description
role distribute	Enables CFS distribution for authorization roles.
show role	Displays authorization roles information.

role distribute

To enable Cisco Fabric Services (CFS) distribution for authorization roles, use the **role distribute** command. To disable this feature, use the **no** form of the command.

role distribute
no role distribute

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable fabric distribution for authorization roles:

```
switch# config terminal
switch(config)# role distribute
```

Related Commands

Command	Description
role commit	Commits temporary to the authorization role configuration changes to the active configuration.
show role	Displays authorization role information.

role name

To configure and assign users to a new role or to modify the profile for an existing role, use the **role name** command in configuration mode. Use the **no** form of this command to delete a configured role.

role name [**max-length 64**] [*name*] [**description** *user description*] [{**rule** *number* **permit clear feature** *name*|**permit config feature** *name*|**permit debug feature** *name*|**permit show feature** *name*}] [{**rule** *number* **deny clear feature** *name*|**deny config feature** *name*|**deny debug feature** *name*|**deny exec feature** *name*|**deny show feature** *name*}]
no role name *name* [**description** *user description*] [{**rule** *number* **permit clear feature** *name*|**permit config feature** *name*|**permit debug feature** *name*|**permit show feature** *name*}] [{**rule** *number* **deny clear feature** *name*|**deny config feature** *name*|**deny debug feature** *name*|**deny exec feature** *name*|**deny show feature** *name*}]

Syntax Description

max-length 64	(Optional) Allows the user to configure role name length of 64 characters. The default role name length is 16 characters.
name	Name of the role to be created or modified. The maximum string length is 64.
description	(Optional) Adds a description for the role. The maximum size is 128.
user description	(Optional) Adds description of users to the role.
rule *number*	(Optional) Enters the rule keyword. The rule number is from 1 to 256.
permit	(Optional) Adds commands to the role.
deny	(Optional) Removes commands from the role.
clear	(Optional) Cleas commands.
feature *name*	Enters the feature name. The maximum size of the feature name is 32.
config	(Optional) Configures commands.
debug	(Optional) Debug commands
show	(Optional) Show commands
exec	(Optional) Exec commands

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Users are assigned roles. Roles are assigned rules. Roles are a group of rules defining a user's access to certain commands. The rules within roles can be assigned to permit or deny access to the following commands:

- **clear**— Clear commands
- **config**— Configuration commands
- **debug**— Debug commands
- **exec**— EXEC commands
- **show**— Show commands

These commands can have **permit** or **deny** options within that command line.

Examples

The following example shows how to assign users to a new role:

```
switch# config terminal
switch(config)#role name max-length 64
switch(config)# role name techdocs
switch(config-role)#
switch(config)#
switch(config-role)# description Entire Tech. Docs. group
switch(config-role)# no
 description
switch# config terminal
switch(config)# role name sangroup
switch(config-role)#
switch(config-role)# rule 1 permit config
switch(config-role)# rule 2 deny config feature fspf
switch(config-role)# rule 3 permit debug feature zone
switch(config-role)# rule 4 permit exec feature fcping
switch(config-role)# no rule 4
switch(config)# no role name sangroup
switch(config)# no role name max-length 64
Role: network-operator
Description: Predefined Network Operator group. This role cannot be modified
Access to Show commands and selected Exec commands
```

Related Commands

Command	Description
show role	Displays all roles configured on the switch including the rules based on each role.

rsakeypair

To configure and associate the RSA key pair details to a trust point, use the **rsakeypair** command in trust point configuration submode. To disassociate the RSA key pair from the trust point, use the **no** form of the command.

rsakeypair *key-pair-label* [{*key-pair-size*}]
no rsakeypair *key-pair-label* [*key-pair-size*]

Syntax Description

key-pair-label	Specifies a name for the RSA key pair. The maximum size is 64 characters.
key-pair-size	(Optional) Specifies a size for the RSA key pair. The size can range from 512 to 2048.

Command Default

The default key pair size is 512 if the key pair is not already generated.

Command Modes

Trust point configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Only one RSA key pair can be associated with a trust point CA, even though the same key pair can be associated with many trust point CAs. This association must occur before enrolling with the CA to obtain an identity certificate. If the key pair had been generated previously (using the **crypto key generate** command), then the key pair size, if specified, should be the same as that was used during generation. If the specified key pair is not yet generated, it will be generated during enrollment using the **crypto ca enroll** command.

The **no** form of the **rsakeypair** command disassociates (but never destroys) the key pair from the trust point. Before issuing the **no rsakeypair** command, first remove the identity certificate, if present, from the trust point CA. Doing so ensures the consistency of the association between the identity certificate and the key pair for a trust point

Examples

The following example shows how to associate an RSA key pair to a trust point:

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# rsakeypair adminid-key
```

The following example shows how to disassociate an RSA key pair from a trust point:

```
switch(config-trustpoint)# no rsakeypair adminid-key
```

Related Commands

Command	Description
crypto ca enroll	Requests certificates for the switch's RSA key pair created for the trust point CA.

Command	Description
crypto key generate rsa	Configures RSA key pair information.
show crypto key mypubkey rsa	Displays information about configured RSA key pairs.

rscn

To configure a registered state change notification (RSCN), a Fibre Channel service that informs Nx ports about changes in the fabric, use the **rscn** command in configuration mode.

rscn {**multi-pid**|**suppress domain-swrscn**} **vsan** *vsan-id*

Syntax Description

multi-pid	Sends RSCNs in multi-PID format.
suppress domain-swrscn	Suppresses transmission of domain format SW-RCSNs.
vsan *vsan-id*	Configures VSAN information or membership. The ID of the VSAN is from 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures RSCNs in multi-PID format:

```
switch# config terminal
switch(config)# rscn multi-pid vsan 1
```

Related Commands

Command	Description
show rscn src-table	Displays state change registration table.
show rscn statistics	Displays RSCN statistics.

rscn abort vsan

To cancel a Registered State Change Notification (RSCN) configuration on a VSAN, use the **rscn abort vsan** command in configuration mode. To reverse the cancellation, use the **no** form of the command.

rscn abort vsan *vsan-id*
no rscn abort vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN where the RSCN configuration should be cancelled. The ID of the VSAN is from 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example cancels an RSCN configuration on VSAN 1:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn abort vsan 1
```

Related Commands

Command	Description
clear rscn session vsan	Clears the RSCN session for a specified VSAN.
rscn commit vsan	Commits a pending RSCN configuration on a specified VSAN.
rscn distribute	Enables the distribution of an RSCN configuration.
rscn event-tov	Configures an RSCN event timeout.
show rscn	Displays the RSCN configuration information.

rscn coalesce swrscn vsan

To enable coalescing of Switch Registered State Change Notification (SWRSCN) before sending, use the **rscn coalesce swrscn vsan** command in configuration mode. To disable coalesce SWRSCN, use the **no** form of the command.

rscn coalesce swrscn vsan *vsan-id* [**delay** *milliseconds*]
no rscn coalesce swrscn vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN ID range. The range is from 1 to 4093.
delay	Specifies the delay in milliseconds to achieve swrscn coalesce.
milliseconds	Specifies the Swrscn coalesce delay in milliseconds (default 500ms). The range is from 100 to 2000.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(7)	This command was introduced.

Usage Guidelines

This feature can be enabled in a fabric where all the switches are MDS and are running 6.2(7) and above.

Examples

The following example shows how to enable coalesce SWRSCN:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn coalesce swrscn vsan 1
```

switch(config)#

The following example shows how to configure 100 milliseconds delay for coalesce SWRSCN:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn coalesce swrscn vsan 1 delay 100
switch(config)#
```

rscn commit vsan

To apply a pending Registered State Change Notification (RSCN) configuration, use the **rscn commit vsan** command in configuration mode. To discard a pending RSCN configuration, use the **no** form of the command.

rscn commit vsan *vsan-id*
no rscn commit vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN where the RSCN configuration should be committed. The ID of the VSAN is from 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

If you commit the changes made to the active database, the configuration is committed to all the switches in the fabric. On a successful commit, the configuration change is applied throughout the fabric and the lock is released.

Note Once the "rscn commit" is done the running configuration has been modified on all switches participating in rscn distribution. You can then use the "copy running-config startup-config fabric" command to save the running-config to the startup-config on all the switches in the fabric.

Examples

The following example commits an RSCN configuration on VSAN 1:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn commit vsan 1
```

Related Commands

Command	Description
clear rscn session vsan	Clears the RSCN session for a specified VSAN.
rscn abort vsan	Cancels a pending RSCN configuration on a specified VSAN.
rscn distribute	Enables the distribution of an RSCN configuration.
rscn event-tov	Configures an RSCN event timeout.
show rscn	Displays RSCN configuration information.

rscn distribute

To enable distribution of a Registered State Change Notification (RSCN) configuration, use the **rscn distribute** command in configuration mode. To disable the distribution, use the **no** form of the command.

rscn distribute
no rscn distribute

Syntax Description

This command has no arguments or keywords.

Command Default

RSCN timer distribution is disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The RSCN timer configuration must be the same on all switches in the VSAN; otherwise, the link will not come up. Cisco Fabric Service (CFS) automatically distributes the RSCN timer configuration to all switches in a fabric. Only the RSCN timer configuration distributed.

Note For the CFS distribution to operate correctly for the RSCN timer configuration, all switches in the fabric must be running Cisco SAN-OS Release 3.0(1) or later.

Examples

The following example enables the distribution of an RSCN configuration:

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

Related Commands

Command	Description
clear rscn session vsan	Clears the RSCN session for a specified VSAN.
rscn abort vsan	Cancels a pending RSCN configuration on a specified VSAN.
rscn commit vsan	Applies a pending RSCN configuration.
rscn event-tov	Configures an RSCN event timeout.
show rscn	Displays RSCN configuration information.

rscn event-tov

To configure an event timeout value for a Registered State Change Notification (RSCN) on a specified VSAN, use the **rscn event-tov** command in configuration mode. To cancel the event timeout value and restore the default value, use the **no** form of the command.

rscn event-tov *timeout* **vsan** *vsan-id*
no rscn event-tov *timeout* **vsan** *vsan-id*

Syntax Description

timeout	Specifies an event timeout value in milliseconds. The range is 0 to 2000.
vsan-id	Specifies a VSAN where the RSCN event timer should be used. The ID of the VSAN is from 1 to 4093.

Command Default

The default timeout values are 2000 milliseconds for Fibre Channel VSANs and 1000 milliseconds for FICON VSANs.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Before changing the timeout value, you must enable RSCN configuration distribution using the **rscn distribute** command.

The RSCN timer is registered with Cisco Fabric Services (CFS) during initialization and switchover. For high availability, if the RSCN timer distribution crashes and restarts or a switchover occurs, it resumes normal functionality from the state prior to the crash or switchover.

Note You can determine configuration compatibility when downgrading to an earlier Cisco MDS SAN-OS release using the **show incompatibility system** command. You must disable RSCN timer distribution support before downgrading to an earlier release.

Examples

The following example configures an RSCN event timeout value on VSAN 1:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn event-tov 20 vsan 1
Successful. Commit should follow for command to take effect.
```

Related Commands

Command	Description
rscn abort vsan	Cancels a pending RSCN configuration on a specified VSAN.

Command	Description
rscn commit vsan	Applies a pending RSCN configuration.
rscn distribute	Enables distribution of an RSCN configuration.
clear rscn session vsan	Clears the RSCN session for a specified VSAN.
show rscn	Displays RSCN configuration information.

rscn permit type nport event switch-config

To enable Registered State Change Notification (RSCN) on management port IP address changes or switch name changes, use the **rscn permit type nport event switch-config** command. To disable RSCN, use the **no** form of the command.

rscn permit type nport event switch-config vsan *vsan-id*
no rscn permit type nport event switch-config vsan *vsan-id*

Syntax Description

vsan	Specifies the VSAN.
vsan-id	Specifies the VSAN ID. The range is from 1 to 4093.

Command Default

RSCN will not be sent on management port IP address changes or switch name changes.

Command Modes

Configuration mode.

Command History

Release	Modification
5.2(8)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable RSCN on management port changes:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn permit type nport event switch-config vsan 1
switch(config)#
```

Related Commands

Command	Description
show rscn	Displays RSCN configuration information.

rspan-tunnel

To associate and bind the SPAN tunnel (ST) port with the RSPAN tunnel, use the **rspan-tunnel** command.

rspan-tunnel interface fc-tunnel *tunnel-id*
rspan-tunnel interface fc-tunnel *tunnel-id*

Syntax Description

rspan-tunnel	Configures the remote SPAN (RSPAN) tunnel.
interface	Specifies the interface to configure this tunnel.
fc-tunnel *tunnel-id*	Specifies the FC tunnel interface. The range is 1 to 255.

Command Default

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

The interface is not operationally up until the Fibre Channel tunnel mapping is configured in the source and destination switches.

Examples

The following example configures an interface to associate and bind the ST port with the RSPAN tunnel and enables traffic flow trough this interface:

```
switchS# config t
switchS(config)# interface fc2/1
switchS(config-if)# rspan-tunnel interface fc-tunnel 100
switchS(config-if)# no shutdown
```

rule

show rscn	Displays RSCN configuration information.

To specify the tape volume group regular expression, use the **rule** command. To disable this feature, use the **no** form of the command.

rule {*range* **range**|**regexp** *regular expression*}
no rule {**range** *range*|**regexp** *regular expression*}

Syntax Description

range *range*	Specifies the crypto tape volume barcode range. The maximum length is 32 characters.
regexp *regular expression*	Specifies the volume group regular expression. The maximum length is 32 characters.

Command Default

None.

Command Modes

Cisco SME crypto tape volume group configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example specifies the volume group regular expression:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# tape-bkgrp tbg1
switch(config-sme-cl-tape-bkgrp)# tape-volgrp tv1
switch(config-sme-cl-tape-bkgrp-volgrp)#rule regexp r1
```

Related Commands

Command	Description
show sme cluster	Displays information about Cisco SME cluster.
tape-bkgrp *groupname*	Configures crypto backup group.
tape-volgrp *volume groupname*	Configures crypto backup volume group.

run-script

To execute the commands specified in a file, use the **run-script** command.

run-script [{**bootflash:**|**slot0:**|**volatile:**}] *filename*

Syntax Description

bootflash:	(Optional) Source or destination location for internal bootflash memory.
slot0:	(Optional) Source or destination location for the CompactFlash memory or PCMCIA card.
volatile:	(Optional) Source or destination location for volatile file system.
filename	Name of the file containing the commands.

Command Default

Uses the current default directory.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Updated the Usage Guidelines and Examples with information about user-defined variables.

Usage Guidelines

To use this command, be sure to create the file and specify commands in the required order.

The **run-script** command accepts user-defined variables as parameters.

Examples

The following example executes the CLI commands specified in the testfile that resides in the slot0 directory:

```
switch# show file slot0:testfile
conf t
interface fc 1/1
no shutdown
end
sh interface fc1/1
```

In response to the **run-script** command, this is the file output:

```
switch# run-script slot0:testfile
'conf t'
Enter configuration commands, one per line. End with CNTL/Z.
'interface fc 1/1'
'no shutdown'
'end'
'sh interface fc1/1'
fc1/1 is down (Fcot not present)
    Hardware is Fibre Channel
    Port WWN is 20:01:00:05:30:00:48:9e
    Admin port mode is auto, trunk mode is on
```

```
    vsan is 1
    Beacon is turned off
    Counter Values (current):
      0 frames input, 0 bytes, 0 discards
      0 runts, 0 jabber, 0 too long, 0 too short
      0 input errors, 0 CRC, 0 invalid transmission words
      0 address id, 0 delimiter
      0 EOF abort, 0 fragmented, 0 unknown class
      0 frames output, 0 bytes, 0 discards
      Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
      Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits
    Counter Values (5 minute averages):
      0 frames input, 0 bytes, 0 discards
      0 runts, 0 jabber, 0 too long, 0 too short
      0 input errors, 0 CRC, 0 invalid transmission words
      0 address id, 0 delimiter
      0 EOF abort, 0 fragmented, 0 unknown class
      0 frames output, 0 bytes, 0 discards
      Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
   Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits
```

The following example shows how you can pass user-defined variables to the **run-script** command:

```
switch# run-script bootflash:test2.vsh var1="fc1/1" var2="brief"
switch # show interface $(var1) $(var2)
--------------------------------------------------------------------------------
Interface Vsan Admin Admin Status SFP Oper Oper Port
Mode Trunk Mode Speed Channel
Mode (Gbps)
--------------------------------------------------------------------------------
fc1/1 1 auto on sfpAbsent -- -- --
```

S Commands

salt (sa configuration submode)

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

salt salt
no salt salt

Syntax Description

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

Command Default

None.

Command Modes

Configuration submode

Command History

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

Usage Guidelines

None.

Examples

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

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

Related Commands

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

san-ext-tuner enable

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

san-ext-tuner enable

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

santap module

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

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

Syntax Description

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

Command Default

Disabled.

The IO-timeout is 10 seconds.

Lun-size-handling is Enabled.

Command Modes

onfiguration mode.

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

scaling batch enable

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

scaling batch enable
no scaling batch enable

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Cisco SME cluster onfiguration submode

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to enable Cisco SME scalability:

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

Related Commands

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

scheduler

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

scheduler {**aaa-authentication** [**username** *username*] **password** [{**0**|**7**}] *password*|**job name** **job-name**|**logfile size** **filesize**|**schedule name** **schedule-name**}
no scheduler {**aaa-authentication** [**username** *username*] **password** [{**0**|**7**}] *password*|**job name** **job-name**|**logfile size** **filesize**|**schedule name** **schedule-name**}

Syntax Description

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

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

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

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

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

Examples

The following example shows how to enable the scheduler command:

```
switch# config t
```

switch(config)# feature scheduler

switch(config)#

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

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

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

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

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

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

The following example shows how to specify scheduler logfile size:

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

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

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

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

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

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

```
switch(config)# scheduler job name my_job
switch(config-job)# cli var name timestamp $(TIMESTAMP);copy running-config
```

```
bootflash:/$(SWITCHNAME)-cfg.$(timestamp);copy bootflash:/$(SWITCHNAME)-cfg.$(timestamp)
tftp://1.2.3.4/
switch(config-job)# exit
switch(config)#
```

Related Commands

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

scsi-flow distribute

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

scsi-flow distribute
no scsi-flow distribute

Syntax Description

This command has no arguments or keywords.

Command Default

SCSI flow distribution is enabled.

Command Modes

Configuration mode

Command History

Release	Modification
2.0(2)	This command was introduced.

Usage Guidelines

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

Examples

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

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

The following example disables distribution of SCSI flow services:

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

Related Commands

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

scsi-flow flow-id

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

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

Syntax Description

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

Command Default

SCSI flow services are disabled.

Command Modes

Configuration mode

Command History

Release	Modification
2.0(2)	This command was introduced.

Usage Guidelines

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

Examples

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

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

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

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

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

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

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

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

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

The following example configures SCSI flow 4 with write acceleration:

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

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

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

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

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

Related Commands

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

scsi-target

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

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

Syntax Description

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

Command Default

SCSI target discovery for each option is on.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

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

Examples

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

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

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

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

The following example configures an SCSI target discovery:

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

The following example removes a SCSI target discovery:

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

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

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

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

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

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

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

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

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

Related Commands

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

sdv abort vsan

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

sdv abort vsan *vsan-id*

Syntax Description

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

Command Default

Disabled.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

sdv commit vsan

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

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

Syntax Description

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

Command Default

Disabled.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

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

Examples

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

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

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

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

Related Commands

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

sdv enable

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

sdv enable
no sdv enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to enable SDV:

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

The following example shows how to disable SDV:

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

Related Commands

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

sdv virtual-device name

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

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

Syntax Description

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

Command Default

Disabled.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

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

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

Related Commands

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

secure-erase abort job

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

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

Syntax Description

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

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

secure-erase create algorithm

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

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

Syntax Description

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

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

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

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

Related Commands

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

secure-erase create job

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

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

Syntax Description

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

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

A Secure Erase job contains the following information:

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

Examples

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

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

Related Commands

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

secure-erase create-vi vsan

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

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

Syntax Description

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

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
create job	Creates a Secure Erase job.

secure-erase destroy algorithm

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

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

Syntax Description

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

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to destroy an algorithm:

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

Related Commands

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

secure-erase destroy job

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

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

Syntax Description

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

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

secure-erase destroy-vi vsan

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

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

Syntax Description

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

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to destroy a VSAN:

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

Related Commands

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

secure-erase start job

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

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

Syntax Description

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

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

secure-erase stop job

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

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

Syntax Description

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

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

secure-erase validate job

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

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

Syntax Description

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

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None

Examples

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

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

Related Commands

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

security-mode

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

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

Syntax Description

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

Command Default

None.

Command Modes

Cisco SME cluster configuration submode

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example sets the security mode to basic:

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

The following example sets the security mode to advanced:

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

Related Commands

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

send

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

send *message-text*

Syntax Description

message-text	Specifies the text of your message.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This message is restricted to 80 alphanumeric characters with spaces.

Examples

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

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

server

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

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

Syntax Description

ipaddress or DNS name	Specifies LDAP server name.

Command Default

None.

Command Modes

Configuration submode

Command History

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

Usage Guidelines

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

Examples

The following example shows how to configure LDAP server name:

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

Related Commands

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

server (configure session submode)

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

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

Syntax Description

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

Command Default

None.

Command Modes

Configure session submode

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

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

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

Related Commands

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

server (DMM job configuration submode)

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

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

Syntax Description

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

Command Default

None.

Command Modes

DMM job configuration submode

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

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

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

Related Commands

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

server (iSNS profile configuration mode)

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

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

Syntax Description

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

Command Default

None.

Command Modes

iSNS profile configuration submode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

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

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

Related Commands

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

server (radius configuration)

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

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

Syntax Description

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

Command Default

None.

Command Modes

RADIUS configuration submode

Command History

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

Usage Guidelines

None.

Examples

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

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

Related Commands

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

server (tacacs+ configuration)

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

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

Syntax Description

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

Command Default

None.

Command Modes

TACACS+ configuration submode

Command History

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

Usage Guidelines

None.

Examples

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

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

Related Commands

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

set (IPsec crypto map configuration submode)

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

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

Syntax Description

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

Command Default

None.

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

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

Command Modes

IPsec crypto map configuration submode

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

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

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

set interface preference-strict
no set interface preference-strict

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Fibre Channel route-map configuration submode.

Command History

Release	Modification
3.0(3)	This command was introduced.

Usage Guidelines

None.

Examples

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

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

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

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

Related Commands

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

setup

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

setup

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

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

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

Examples

The following example shows how to enter switch setup mode:

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

setup ficon

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

setup ficon

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

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

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

Examples

The following example shows how to enter switch setup mode:

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

setup sme

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

setup sme

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

shared-keymode

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

shared-keymode
no shared-keymode

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Cisco SME cluster configuration submode

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

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

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

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

Examples

The following example specifies the shared key mode:

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

The following example specifies the shared unique keymode:

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

Related Commands

Command	Description
show sme cluster	Displays Cisco SME cluster information.

shutdown

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

shutdown [force]
no shutdown [force]

Syntax Description

force	(Optional) Forces the shutdown of the mgmt 0 interface.

Command Default

None.

Command Modes

Interface configuration submode

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 submode.
show interface	Displays interface information.

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.

Command Default

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.

shutdown (interface configuration submode)

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

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Interface configuration submode

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

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

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

Examples

The following example enables a Cisco SME interface:

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

The following example disables a Cisco SME interface:

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

Related Commands

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

site-id

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

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

Syntax Description

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

Command Default

None.

Command Modes

Call Home configuration submode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

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

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

Related Commands

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

sleep

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

sleep *seconds*

Syntax Description

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

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command is useful within scripts.

Examples

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

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

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

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

```
switch# sleep 30
```

You will see the switch prompt return after 30 seconds.

sme

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

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

Syntax Description

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

Command Default

Disabled.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

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

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

Examples

The following example shows how to configure a cluster:

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

snmp port

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

snmp port control
no snmp port control

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP control of FICON configurations is enabled.

Command Modes

FICON configuration submode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example prohibits SNMP users from configuring FICON parameters:

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

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

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

Related Commands

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

snmp-server

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

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

Syntax Description

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

Command Default

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

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

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

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

Related Commands

Command	Description
show snmp	Displays SNMP information.

snmp-server aaa exclusive-behavior enable

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

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

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

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

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

Related Commands

Command	Description
show snmp	Displays SNMP information.

snmp-server community

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

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

Syntax Description

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

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

The following example sets the SNMP server community string:

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

Related Commands

Command	Description
show snmp	Displays SNMP information.

snmp-server contact

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

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

Syntax Description

line	(Optional) Modifies the system contact.

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to modify the server contact:

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

Related Commands

Command	Description
show snmp	Displays SNMP information.

snmp-server enable traps

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

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

Syntax Description

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

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

Command Default

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

Command Modes

Configuration mode

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

The following example enables all SNMP entity notifications:

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

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

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

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

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

Related Commands

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

snmp-server enable traps fcdomain

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

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

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

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

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

Related Commands

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

snmp-server enable traps link cisco

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

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

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

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

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

Related Commands

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

snmp-server enable traps zone

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

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

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to enable SNMP zone traps:

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

Related Commands

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

snmp-server globalEnforcePriv

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

snmp-server globalEnforcePriv
no snmp-server globalEnforcePriv

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
2.1(0)	This command was introduced.

Usage Guidelines

None.

Examples

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

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

Related Commands

Command	Description
show snmp	Displays SNMP information.

snmp-server host

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

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

Syntax Description

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

Command Default

Sends SNMP traps.

Command Modes

Configuration mode

Command History

Release	Modification
1.0(3)	This command was introduced.

Usage Guidelines

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

Examples

The following example specify the recipient of an SNMP notification:

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

Related Commands

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

snmp-server location

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

snmp-server location
no snmp-server location

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

The following example sets the SNMP server community string:

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

Related Commands

Command	Description
show snmp	Displays SNMP information.

snmp-server tcp-session

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

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

Syntax Description

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

Command Default

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

Command Modes

Configuration mode

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

None.

Examples

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

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

Related Commands

Command	Description
show snmp	Displays SNMP information.

snmp-server traps entity fru

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

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

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

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

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

Related Commands

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

snmp-server user

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

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

Syntax Description

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

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

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

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

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

Examples

The following example sets the user authentication and SNMP engine ID for a notification target user:

```
switch# config terminal
switch(config)# snmp-server user notifUser network-admin auth sha abcd1234 engineID
00:12:00:00:09:03:00:05:48:00:74:30
```

The following example sets the user information:

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

Related Commands

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

source

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

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

Syntax Description

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

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

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

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

Related Commands

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

span max-queued-packets

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

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

Syntax Description

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

Command Default

15.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

This command is supported only on a ISOLA platform.

Examples

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

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

Related Commands

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

span session

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

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

Syntax Description

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

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure a SPAN session:

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

The following example shows how to delete a SPAN session:

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

Related Commands

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

span session source interface

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

interface

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

Syntax Description

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

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

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

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

Related Commands

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

special-frame

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

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

Syntax Description

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

Command Default

Disabled.

Command Modes

Interface configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

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

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

Examples

The following example configures the special frames:

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

Related Commands

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

ssh

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

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

Syntax Description

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

Command Default

The default user name is admin.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

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

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

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

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

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

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

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

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

Related Commands

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

ssh key

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

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

Syntax Description

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

Command Default

The default key-pair modulus is 1024 bits.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

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

Examples

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

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

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

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

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

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

Related Commands

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

ssh server enable

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

ssh server enable
no ssh server enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

None.

Examples

The following example enables the SSH server:

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

The following example disables the SSH server:

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

Related Commands

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

ssl

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

ssl kmc
no ssl kmc

Syntax Description

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

Command Default

None.

Command Modes

Cisco SME cluster configuration mode submode

Command History

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

Usage Guidelines

None.

Examples

The following example enables SSL:

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

ssm enable feature

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

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

Syntax Description

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

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

Command Default

Disabled.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Related Commands

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

ssm upgrade delay

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

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

Syntax Description

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

Command Default

None.

Command Modes

Configuration mode

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

static (iSCSI initiator configuration and iSLB initiator configuration)

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

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

Syntax Description

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

Command Default

None.

Command Modes

iSCSI initiator configuration submode

iSLB initiator configuration submode

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

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

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

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

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

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

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

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

Related Commands

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

stop

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

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

Syntax Description

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

Command Default

None.

Command Modes

SAN extension N port configuration submode

Command History

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

Usage Guidelines

None.

Examples

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

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

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

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

Related Commands

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

storage (DMM job configuration submode)

To add a storage port to a DMM job, use the **storage** command in DMM job configuration submode.

storage vsan *vsan-id* **pwwn** *port-wwn* {**existing**|**new**}

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
pwwn *port-wwn*	Specifies the world-wide name of the storage port. The format is hh:hh:hh:hh:hh:hh:hh:hh, where h is a hexadecimal number.
existing	Specifies a port on the existing storage.
new	Specifies a port on the new storage.

Command Default

None.

Command Modes

DMM job configuration submode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to add storage information to a DMM job:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# dmm module 3 job 1 create
Started New DMM Job Configuration.
Do not exit sub-mode until configuration is complete and committed
switch(config-dmm-job)# storage vsan 3 pwwn 1d:22:3a:21:3c:44:3b:51 existing
switch(config-dmm-job)#
```

Related Commands

Command	Description
show dmm ip-peer	Displays job information.
show dmm srvr-vt-login	Enables DMM.

streetaddress

To configure the street address with the Call Home function, use the **streetaddress** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

streetaddress *street-address*
no streetaddress *street-address*

Syntax Description

street-address	Specifies the customer's street address where the equipment is located. Allows up to 256 alphanumeric characters in free format for the street number, city, state, and zip (combined).

Command Default

None.

Command Modes

Call Home configuration submode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the street address in the Call Home configuration:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# streetaddress 1234 Picaboo Street, AnyCity, AnyState, 12345
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destinations.
show callhome	Displays configured Call Home information.

suspend

To suspend a switched port analyzer (SPAN) session, use the **suspend** command in SPAN session configuration submode. To disable the suspension, use the **no** form of the command.

suspend
no suspend

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

SPAN session configuration submode

Command History

Release	Modification
6.2(1)	This command was deprecated.
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to suspend a SPAN session:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# span session 1
switch(config-span)# suspend
switch(config-span)# do show span session 1
Session 1 (admin suspended)
   Destination is not configured
   No session filters configured
   Ingress (rx) sources are
     fc3/13,
   Egress (tx) sources are
     fc3/13,
switch(config-span)#
```

The following example shows how to disable the suspension of the SPAN session:

```
switch(config-span)# no suspend
```

Related Commands

Command	Description
destination interface	Configures a SPAN destination interface.
show span session	Displays specific information about a SPAN session.
source	Configures a SPAN source.

Command	Description
span session	Selects or configures the SPAN session and changes to SPAN configuration submode.
switchport	Configures the switch port mode on the Fibre Channel interface.

switchname

To change the name of the switch, use the **switchname** command in configuration mode. To revert the switch name to the default name, use the no form of the command.

switchname *name*
no switchname *name*

Syntax Description

name	Specifies a switch name. Maximum length is 32 characters.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example changes the name of the switch to myswitch1:

```
switch# config terminal
switch(config)# switchname myswitch1
```

The following example changes the name of the switch to the default:

```
myswitch1(config)# no switchname
```

Related Commands

Command	Description
snmp-server	Sets the contact information, switch location, and switch name within the limit of 20 characters (without spaces).

switchport auto-negotiate

To enable autonegotiation on an Ethernet-based SAN extension interface, use the **switchport auto-negotiate** command. To disable autonegotiation, use the **no** form of this command.

switchport auto-negotiate
no switchport auto-negotiate

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.1(1)	This command was introduced.

Usage Guidelines

This command is available only on Ethernet-based SAN extension interfaces, specifically Gigabit Ethernet and IPS type interfaces. It is not available on FCoE Ethernet interfaces or the management interface.

Examples

The following example shows how to enable autonegotiation on a Gigabit Ethernet interface:

```
switch# configure terminal
switch(config)# interface gigabitethernet 2/2
switch(config-if)# switchport auto-negotiate
```

Related Commands

Command	Description
show interface	Displays an interface status and statistics.

switchport beacon

To enable the beacon LED on an interface, use the **switchport beacon** command. To disable the beacon LED on the interface, use the **no** form of this command.

switchport beacon
no switchport beacon

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable the beacon LED on an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport beacon
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport description

To specify the description for an interface, use the **switchport description** command. To delete the interface description, use the **no** form of this command.

switchport description *text*
no switchport description *text*

Syntax Description

text	Specifies the interface description. Maximum length is 254 characters.

Command Default

None.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to add a description to an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport description Host Linux4943 port 2
```

Related Commands

Command	Description
show interface description	Displays descriptions from all interfaces.

switchport duplex

To specify the Ethernet duplex mode as full, half, or autonegotiate on a management interface, use the **switchport duplex** command. To return the interface to the default mode, use the **no** form of this command.

switchport duplex {**auto**|**full**|**half**}
no switchport duplex {**auto**|**full**|**half**}

Syntax Description

auto	Specifies the duplex mode as autonegotiate.
full	Specifies the duplex mode as full.
half	Specifies the duplex mode as half.

Command Default

The default duplex of the management interface is full.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 4.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to set the duplex mode to auto on a management interface:

```
switch# configure terminal
switch(config)# interface mgmt 0
switch(config-if)# switchport duplex auto
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport encap

To send SPAN traffic through the fabric to a remote switch the SD port must be connected to a neighbor switch and the egress traffic encapsulated in EISL encapsulation to conform to the interswitch frame format. To configure EISL encapsulation on an interface, use the **switchport encap** command. To remove the configuration, use the **no** form of this command.

switchport encap eisl
no switchport encap eisl

Syntax Description

eisl	Specifies extended ISL (EISL) encapsulation on an interface.

Command Default

Disabled.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines

This command sets the egress frame format of an interface in the SD port mode. When enabled, all egress frames are encapsulated in the EISL frame format.

Examples

The following example shows how to configure EISL encapsulation on an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport encap eisl
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.
show span session	Displays the status of SPAN sessions.

switchport fcbbscn

Credit recovery on Fibre Channel links is facilitated by the buffer to buffer state change notification feature. This allows loss of credits on a link to be detected and recovered. To enable buffer to buffer state change notification on an interface, use the **switchport fcbbscn** command. To disable notification, use the **no** form of this command.

switchport fcbbscn
no switchport fcbbscn

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 3.0(1)	This command was introduced.

Usage Guidelines

Caution This command causes traffic disruption on the specified interface.

Examples

The following example shows how to enable buffer to buffer credit recovery on an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport fcbbscn
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport fcrxbbcredit

Each Fibre Channel interface may be assigned receive buffer to buffer credits from 3 types of buffer pools. To configure receive buffer to buffer credits on an interface, use the **switchport fcrxbbcredit** command. To remove the configuration, use the **no** form of this command.

switchport fcrxbbcredit {*std_bufs* [**mode** {**E**|**Fx**}]|**default**|**performance-buffers** {**default***perf_bufs*}|**extended** *ext_bufs*}
no switchport fcrxbbcredit {*std_bufs* [**mode** {**E**|**Fx**}]|**default**|**performance-buffers** {**default** *perf_bufs*}|**extended** *ext_bufs*}

Syntax Description

std_bufs	Specifies count of standard B2B credits. The range is 1 to 500.
mode	(Optional) Restricts the standard receive B2B credit to the specified port mode.
E	Specifies Inter-Switch Link port mode.
Fx	Specifies fixed F and F-loop port modes.
performance-buffers	Configures receive performance buffer allocation on the port.
default	Specifies to use the default credits depending on the port type and capabilities.
perf_bufs	Specifies performance receive B2B credits. The range is 1 to 145.
extended	Configures extended B2B credits.
ext_bufs	Specifies count of extended receive B2B credits. The range is 256 to 4095.

Command Default

None.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 2.0(1b)	Added the **extended** keyword to the syntax.
NX-OS 1.1(1)	This command was introduced.

Usage Guidelines

Caution This command causes traffic disruption on the specified interface.

Configure the **feature fcrxbbcredit extended** command to enable access to the **switchport fcrxbbcredit** command. The **switchport fcrxbbcredit** command will not be available until the extended credit feature is enabled.

Extended buffer to buffer credits are intended for long haul links where a high RTT causes more frames to be in flight than normal at linerate. They are advertised to the link peer and require an ENTERPRISE_PKG license.

Performance buffers are intended to absorb short bursts on higher speed ingress interfaces destined for lower speed or mildly congested egress interfaces. They are internal to the switch and are not advertised to the link peer. They are only available in 12-port 4-Gbps and 4-port 10 Gbps switching modules.

Examples

The following example shows how to configure default credits on an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport fcrxbbcredit default
```

Related Commands

Command	Description
feature fcrxbbcredit extended	Enables extended receive B2B credits.
show interface	Displays interface status and statistics.

switchport fcrxbufsize

To configure the maximum size of the receive data buffer on an interface, use the **switchport fcrxbufsize** command. To remove the configuration, use the **no** form of this command.

switchport fcrxbufsize *buffer-size*
no switchport fcrxbufsize *buffer-size*

Syntax Description

buffer-size	Specifies maximum frame size for the interface. The range is 256 to 2112 bytes.

Command Default

The default receive data buffer size is 2112 bytes.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines

Caution This command causes traffic disruption on the specified interface.

Examples

The following example shows how to set the frame size for an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport fcrxbufsize 256
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport fec

To configure the Forward Error Correction (FEC) on an interface, use the **switchport fec** command. To remove the configuration, use the **no** form of this command.

switchport fec
no switchport fec

Syntax Description

fec	Configures the FEC state on an interface.

Command Default

Disabled.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 6.2(7)	This command was introduced.

Usage Guidelines

Caution This command causes traffic disruption on the specified interface.

Note This command is only accepted on ports with the speed fixed to 16 Gbps and FEC already enabled.

Use the **switchport fec** command in the interface configuration mode to configure FEC on an interface.

Note FEC TTS is supported on the DS-X9448-768K9 Generation 5 module in Cisco MDS NX-OS Release 6.2(11c) and later 6.2(11x) releases, and Cisco MDS NX-OS Release 6.2(15) and later releases. It is not supported in Cisco MDS NX-OS Release 6.2(13).

Examples

The following example shows how to configure FEC on a Fibre Channel interface:

```
switch# config t
switch(config)# interface fc 1/1
switch(config-if)# switchport fec
```

Related Commands

Command	Description
show interface fc	Displays the status of the specified Fibre Channel interface.

switchport fec tts

To configure the Forward Error Correction (FEC) and the Transmitter Training Signal (TTS) on an interface, use the **switchport fec tts** command. To remove the configuration, use the **no** form of this command.

switchport fec [tts]
no switchport fec [tts]

Syntax Description

tts	(Optional) Enables Transmitter Training Signal (TTS) allowing negotiation of FEC capability.

Command Default

Disabled.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 6.2(11c)	This command was introduced.

Usage Guidelines

Caution This command causes traffic disruption on the specified interface.

Note This command is only accepted on ports with the speed fixed to 16 Gbps and FEC already enabled.

Use the **switchport fec tts** command only after configuring FEC using the **switchport fec** command.

The TTS is not used by 4 and 8-Gbps Fibre Channel ports. From 32 Gbps and higher, its use is mandatory. For 16 Gbps Fibre Channel ports, EA variants must transmit the TTS during the link speed negotiation, but the use of it by the receiver is optional, and EL variants must not use TTS.

Note FEC TTS is supported on the DS-X9448-768K9 Generation 5 module in Cisco MDS NX-OS Release 6.2(11c) and later 6.2(11x) releases and Cisco MDS NX-OS Release 6.2(15) and later releases. It is not supported in Cisco MDS NX-OS Release 6.2(13).

Examples

The following example show how to configure FEC with TTS on an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport fec
switch(config-if)# switchport fec tts
```

Related Commands

Command	Description
show interface fc	Displays the status of the specified Fibre Channel interface.

switchport fill-pattern

To configure the link fill pattern on an interface, use the **switchport fill-pattern** command.

switchport fill-pattern {**IDLE** |**ARBFF**} **speed 8000**

Syntax Description

IDLE	Configures the fill pattern as IDLE.
ARBFF	Configures the fill pattern as ARBff.
speed	Select speed to apply setting to.
8000	Specifies 8-Gbps link speed.

Command Default

The default setting for the link fill pattern is ARBff.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 5.2(6)	This command was introduced.

Usage Guidelines

⚠

Caution This command causes traffic disruption on the specified interface.

Examples

The following example shows how to configure the fill pattern as ARBff on an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport fill-pattern ARBFF speed 8000
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport ignore

To prevent the detection of certain error events from disabling Fibre Channel interfaces, use the **switchport ignore** command. To revert to the default settings, use the **no** form of this command.

switchport ignore {**bit-errors**| **interrupt-thresholds**}
no switchport ignore {**bit-errors**| **interrupt-thresholds**}

Syntax Description

bit-errors	Ignore the bit errors.
interrupt-thresholds	Ignore interrupt thresholds.

Command Default

None.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 6.2	The **interrupt-thresholds** keyword was added.
NX-OS 2.1(1a)	This command was introduced.

Usage Guidelines

The bit error rate threshold is used by the switch to detect an increased error rate before performance degradation seriously affects traffic.

Bit errors can occur for the following reasons:

- Faulty or bad cable
- Faulty or bad GBIC or SFP
- GBIC or SFP is specified to operate at 1 Gbps, but is used at 2 Gbps
- Short haul cable is used for long haul or long haul cable is used for short haul
- Momentary sync loss
- Loose cable connection at one or both ends
- Improper GBIC or SFP connection at one or both ends

A bit error rate threshold is detected when 15 error bursts occur in a 5-minute period. By default, the switch disables the interface when the threshold is reached. After fixing the source of the bit errors, an affected interface should be re-enabled with the **shutdown** and **no shutdown** command sequence.

Interrupts thresholds are used by the switch to detect excessive internal interrupts before they affect switch performance.

Interrupt thresholds can occur because of continuous primitive sequence (NOS/OLS/LR/LRR).

Note Regardless of the setting of the **switchport ignore bit-errors** command, the switch generates a syslog message when bit error threshold events are detected.

Examples

The following example shows how to prevent the detection of bit error events from disabling an interface:

```
switch# configure terminal
switch(config)# interface fc1/1
switch(config-if)# switchport ignore bit-errors
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport ingress-rate

To configure the port rate limit for a specified interface, use the **switchport ingress-rate** command in interface configuration mode. Use the **no** form of the command to delete the configured switch port information.

switchport ingress-rate *limit*
no switchport ingress-rate *limit*

Syntax Description

limit	Specifies the ingress rate limit as a percentage. The range is 1 to 100.

Command Default

Disabled.

Command Modes

Interface configuration submode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Access this command from the switch(config-if)# submode. This command is only available if the following conditions are true:

- The QoS feature is enabled using the **qos enable** command.
- The command is entered in a Cisco MDS 9100 series switch.

Examples

The following example configures the ingress rate limit on a Fibre Channel interface:

```
switch# config terminal
switch(config)# interface fc 2/5
switch(config-if)# switchport ingress-rate 5
```

Related Commands

Command	Description
show interface fc	Displays an interface configuration for a specified Fibre Channel interface.

switchport initiator id

To configure the iSCSI initiator ID mode, use the **switchport initiator id** command in interface configuration submode. To delete the iSCSI initiator ID mode, use the **no** form of the command.

switchport initiator id {*ip-addressname*}
no switchport initiator id {*ip-addressname*}

Syntax Description

ip-address	Identifies initiators using the IP address.
name	Identifies initiators using the specified name.

Command Default

The iSCSI initiator ID mode is disabled.

Command Modes

Interface configuration submode under the **iscsi interface x/x** command

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures the iSCSI initiator ID mode for an iSCSI interface:

```
switch# config terminal
switch(config)# interface iscsi 2/5
switch(config-if)# switchport initiator id ip-address
switch(config-if)# switchport initiator name
```

Related Commands

Command	Description
show interface iscsi	Displays an interface configuration for a specified iSCSI interface.

switchport max-npiv-limit

To configure the maximum number of logins that are allowed on a nontrunking interface, use the **switchport max-npiv-limit** command. To remove the configuration, use the **no** form of this command.

switchport max-npiv-limit *max-npivs*
no switchport max-npiv-limit *max-npivs*

Syntax Description

max-npivs	Specifies the maximum logins for the interface. The range is from 1 to 256.

Command Default

None.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 6.2(7)	This command was introduced.

Usage Guidelines

Note Both **switchport max-npiv-limit** and **switchport trunk-max-npiv-limit** commands can be configured on a port or Port Channel. The current port mode determines the type of configuration used. If the port is nontrunking, the **max-npiv-limit** setting is used. If the port is trunking, the **trunk-max-npiv-limit** setting is used.

If a login limit is reached on a port and it receives a login request, then a syslog message is logged and the login rejected.

Examples

The following example shows how to configure the maximum number of logins on an F-port to 4:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport max-npiv-limit 4
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.
switchport trunk-max-npiv-limit	Configures the maximum number of logins that are allowed on a trunk port.

switchport mode

To configure the Fibre Channel mode of an interface, use the **switchport mode** command. To remove the configuration, use the **no** form of this command.

switchport mode {**E**|**F**|**FL**|**Fx**|**NP**|**SD**|**ST**|**auto**}
no switchport mode {**E**|**F**|**FL**|**Fx**|**NP**|**SD**|**ST**|**auto**}

Syntax Description

E	Configures fixed Inter-Switch Link port mode.
F	Specifies fixed F port mode.
FL	Specifies fixed F-loop port mode.
Fx	Specifies fixed F and F-loop port modes.
NP	Specifies fixed N port virtualizer mode.
SD	Specifies fixed SPAN destination port mode.
ST	Specifies fixed trunked SPAN port mode.
auto	Specifies autosense mode.

Command Default

The default port mode is auto.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 4.1(3)	Added the **F** and **NP** port mode.
NX-OS 3.0(1)	Added the **ST** option to the syntax.
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines

Caution This command causes traffic disruption on the specified interface.

A port must be in dedicated mode before it can be set to **E** mode.

Examples

The following example shows how to configure fixed Inter-Switch Link mode on an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport mode E
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.
show port-resources	Displays the rate mode of module ports.

switchport mtu

To configure the Ethernet layer maximum transmission unit (MTU) on an Ethernet-based SAN extension interface, use the **switchport mtu** command. To remove the configuration, use the **no** form of this command.

switchport mtu *size*
no switchport mtu *size*

Syntax Description

size	Specifies the MTU size in bytes. The range is 576 to 9216.

Command Default

The default size is 1500 bytes.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines

This command is available only on Ethernet-based SAN extension interfaces, specifically Gigabit Ethernet and IPS type interfaces. It is not available on FCoE Ethernet interfaces or the management interface.

Examples

The following example shows how to configure the Ethernet MTU to 3000 bytes on a Gigabit Ethernet interface:

```
switch# configure terminal
switch(config)# interface gigabitethernet 2/2
switch(config-if)# switchport mtu 3000
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport owner

To configure a descriptive owner string on an interface, use the **switchport owner** command. To remove the configuration, use the **no** form of this command.

switchport owner *owner*
no switchport owner

Syntax Description

owner	(Optional) Specifies the owner. The maximum length of the string is 80 characters.

Command Default

None.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the owner string on an interface:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch (config)# interface fc1/1
Switch (config-if)# switchport owner StorageOps
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport promiscuous-mode

To enable promiscuous mode on an Ethernet-based SAN extension interface, use the **switchport promiscuous-mode** command. To disable the promiscuous mode, use the **no** form of this command.

switchport promiscuous-mode {**off**|**on**}
no switchport promiscuous-mode {**off**|**on**}

Syntax Description

off	Disables promiscuous mode on an interface.
on	Enables promiscuous mode on an interface.

Command Default

Disabled.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.1(1)	This command was introduced.

Usage Guidelines

This command is available only on Ethernet-based SAN extension interfaces, specifically Gigabit Ethernet and IPS type interfaces. It is not available on FCoE Ethernet interfaces or the management interface.

Examples

The following example enables promiscuous mode on a Gigabit Ethernet interface:

```
switch# configure terminal
switch(config)# interface gigabitethernet 2/2
switch(config-if)# switchport promiscuous-mode on
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport proxy-initiator

To configure the iSCSI proxy initiator mode on an iSCSI interface, use the **switchport proxy-initiator** command in interface configuration submode. To delete the iSCSI proxy initiator mode, use the **no** form of the command.

switchport proxy-initiator [**nwwn** *wwn* **pwwn** *wwn*]
no switchport proxy-initiator [**nwwn** *wwn* **pwwn** *wwn*]

Syntax Description

nwwn *wwn*	(Optional) Specifies the node WWN.
pwwn *wwn*	(Optional) Specifies the port WWN.

Command Default

The iSCSI proxy initiator mode is disabled.

Command Modes

Interface configuration submode under the **iscsi interface x/x** command

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

When you do not include the WWNs in the command, the IPS port dynamically assigns a pWWN and nWWN to the proxy initiator.

Caution Enabling proxy initiator mode on an iSCSI interface that is part of an iSLB VRRP group impacts load balancing on the interface.

Examples

The following example configures the iSCSI proxy initiator mode for a iSCSI interface using WWNs:

```
switch# config terminal
switch(config)# interface iscsi 2/5
switch(config-if)# switchport proxy-initiator nwwn 11:11:11:11:11:11:11:11 pwwn
22:22:22:22:22:22:22:22
```

The following example configures the iSCSI proxy initiator mode for a iSCSI interface without WWNs:

```
switch# config terminal
switch(config)# interface iscsi 2/5
switch(config-if)# switchport proxy-initiator
```

The following example deletes the iSCSI proxy initiator mode for a iSCSI interface:

```
switch(config-if)# switchport proxy-initiator
```

Related Commands

Command	Description
show interface iscsi	Displays an interface configuration for a specified iSCSI interface.

switch-priority

To configure the switch priority with the Call Home function, use the **switch-priority** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

switch-priority *priority-value*
no switch-priority *priority-value*

Syntax Description

priority-value	Specifies the priority level. 0 is the highest priority and 7 the lowest.

Command Default

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.

switchport rate-mode

Each interface belongs to a *port group* and each port group has access to a preallocated subset of the backplane bandwidth. On full bandwidth modules, all interfaces have access to the backplane bandwidth at maximum interface speed. On oversubscribed modules, the total of the maximum interface speeds exceeds the allocated backplane bandwidth of the port group. To configure the port group bandwidth-allocation mode of an interface, use the **switchport rate-mode** command. To remove the configuration, use the **no** form of this command.

switchport rate-mode {**dedicated**|**shared**}
no switchport rate-mode {**dedicated**|**shared**}

Syntax Description

dedicated	Specifies dedicated bandwidth for the interface.
shared	Specifies shared bandwidth for the interface.

Command Default

For oversubscribed modules, the default port group mode is shared. For full bandwidth modules, the only available mode is dedicated.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 3.0(1)	This command was introduced.

Usage Guidelines

Caution This command causes traffic disruption on the specified interface.

The maximum port speed of an interface, combined with the rate mode, determines the amount of shared resources available to the ports in the port group. In the case of dedicated rate mode, the port group resources are reserved even though the bandwidth is not used. For oversubscribed port groups, if an interface is configured for autosensing (**auto**) then bandwidth equal to the maximum supported speed of the interface is reserved, even if the link comes up at a lower speed. If the autosensing maximum speed is configured (for example, **auto max 8000**) then only that much bandwidth is reserved and the remaining possible bandwidth is available for other interfaces in the port group.

Table 3: Default Speed and Buffer Configuration

Switching Module	Speed	Port Mode	Rate Mode	Receive Credits (min/max/default)
DS-X9304-18K9, Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4)	1, 2, or 4 Gbps	Fx	Shared	1/16/16
		Fx	Dedicated	2/250/16
		E-port	Dedicated	2//250/250

Switching Module	Speed	Port Mode	Rate Mode	Receive Credits (min/max/default)
DS-C9222i-K9, Cisco MDS 9222i Switch	1, 2, or 4 Gbps	Fx	Shared	1/16/16
		Fx	Dedicated	2/250/16
		E-port	Dedicated	2//250/250
DS-X9704, Cisco MDS 9000 Family 4-Port 10-Gbps Fibre Channel Switching Module	10 Gbps	NA	Shared	NA
		Fx	Dedicated	2/750/16
		E-port	Dedicated	2/750/750
DS-X9248-48K9, Cisco MDS 9000 4/44-Port Host-Optimized 8-Gbps Fibre Channel Switching Module	1, 2, 4, or 8 Gbps	Fx	Shared	1/32/32
		Fx	Dedicated	2/250/32
		E-port	Dedicated	2/250/125
DS-X9248-96K9, Cisco MDS 9000 48-Port 8-Gbps Fibre Channel Switching Module	1, 2, 4, or 8 Gbps	Fx	Shared	1/32/32
		Fx	Dedicated	2/500/32
		E-port	Dedicated	2/500/250
DS-X9224-96K9, Cisco MDS 9000 24-Port 8-Gbps Fibre Channel Switching Module	1, 2, 4, or 8 Gbps	Fx	Shared	1/32/32
		Fx	Dedicated	2/500/32
		E-port	Dedicated	2/500/500
DS-C9148-K9, Cisco MDS 9148 48-Port Multilayer Fabric Switch	1, 2, 4, or 8 Gbps	NA	Shared	NA
		Fx	Dedicated	1/125/32
		E-port	Dedicated	1/125/32
DS-C9134-K9, Cisco MDS 9134 34-Port Multilayer Fabric Switch	1, 2, or 4 Gbps	NA	Shared	NA
		Fx	Dedicated	1/61/16
		E-port	Dedicated	1/61/16
DS-C9124-K9, Cisco MDS 9124 24-Port Multilayer Fabric Switch	1, 2, or 4 Gbps	NA	Shared	NA
		Fx	Dedicated	1/61/16
		E-port	Dedicated	1/61/16
DS-C9134-K9, Cisco MDS 9134 32-Port Fabric Switch	1, 2, or 4 Gbps	NA	Shared	NA
		Fx	Dedicated	1/61/64
		E-port	Dedicated	2/61/64

Switching Module	Speed	Port Mode	Rate Mode	Receive Credits (min/max/default)
DS-C9124, Cisco MDS 9124 24-Port Fabric Switch	1, 2, or 4 Gbps	Fx	Shared	2/16/16
		Fx	Dedicated	2/250/16
		E-port	Dedicated	2/250/250
DS-C9222i-K9, Cisco MDS 9222i 18-Port Multiservice Modular Switch	1, 2, or 4 Gbps	Fx	Shared	2/16/16
		Fx	Dedicated	2/250/16
		E-port	Dedicated	2/250/250
DS-X9248-256K9, Cisco MDS 9000 48-Port Advanced Fibre Channel Module	1, 2, 4, or 8 Gbps	Fx	Shared	1/125/32
		Fx	Dedicated	2/250/16
DS-X9232-256K9, Cisco MDS 9000 32-Port Advanced Fibre Channel Module	1, 2, 4, or 8 Gbps	Fx	Shared	1/125/32
		Fx	Dedicated	2/250/16

When configuring port modes, observe the following guidelines:

- Auto port mode and E port mode cannot be configured in the shared rate mode.
- The 4-port 10-Gbps module does not support the FL port mode.
- Generation 2 modules do not support the TL port mode.
- Shared to dedicated ports must be configured in the following order: speed, rate mode, port mode, and credit.
- Dedicated to shared ports must be configured in the following order: credit, port mode, rate mode, and speed.

When configuring port channels, observe the following guidelines:

- When an interface is out of service, it cannot be part of a port channel.
- The 24-port module and the 48-port module support making ports out of service. In a shared resource configuration, an out-of-service port reverts to its default values when it comes back into service.
- The maximum number of port channels for Generation 2 modules is 256.
- The number of port channels is independent of the type of supervisor module.
- When using the **force** option to add a port channel to a configuration that uses Generation 2 modules, the force addition can fail for a Generation 2 interface if resources are unavailable.

Examples

The following example reserves shared (default) bandwidth for an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport rate-mode shared
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.
show port-resources	Displays the rate mode of module ports.

switchport speed

To configure the speed of an interface, use the **switchport speed** command. To return to the default speed, use the **no** form of this command.

switchport speed {**1000**|**2000**|**4000**|**8000**|**10000**|**16000**|**auto** [**max** {**2000**|**4000**|**8000**|**16000**}]}
no switchport speed {**1000**|**2000**|**4000**|**8000**|**10000**|**16000**|**auto** [**max** {**2000**|**4000**|**8000**|**16000**}]}

Syntax Description

1000	Configure the link speed to be fixed at 1-Gbps speed.
2000	Configure the link speed to be fixed at 2-Gbps speed.
4000	Configure the link speed to be fixed at 4-Gbps speed.
8000	Configure the link speed to be fixed at 8-Gbps speed.
10000	Configure the link speed to be fixed at 10-Gbps speed.
16000	Configure the link speed to be fixed at 16-Gbps speed.
auto	Configures autosense speed.
max 2000	(Optional) Limits maximum link speed to 2 Gbps.
max 4000	(Optional) Limits maximum link speed to 4 Gbps.
max 8000	(Optional) Limits maximum link speed to 8 Gbps.
max 16000	(Optional) Limits maximum link speed to 16 Gbps.

Command Default

The default speed mode is auto.

The default maximum autosense speed is the maximum port speed.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 3.0(1)	Added the **4000** option to the **speed** keyword.
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures the speed of a Fibre Channel interface to be fixed at 16 Gbps:

```
switch# configure terminal
switch(config)# interface fc 1/1
```

```
switch(config-if)# switchport speed 16000
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport trunk allowed vsan

To configure the list of allowed VSANs on a trunk link, use the **switchport trunk allowed vsan** command. To remove the configuration, use the **no** form of this command.

switchport trunk allowed vsan {**add** *vsan-id*|**all**|*vsan-id* **[no-warning]**}

Syntax Description

add	Configure additional allowed VSANs to the existing list.
vsan-id	Specifies the VSAN ID. The range is 1 to 4093.
all	Adds all VSANs to the allowed VSAN list.

Command Default

All VSANs are allowed.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines

If the allowed VSANs on a trunk are a set of noncontiguous VSANs, use the **switchport trunk allowed vsan** *vsan-id* command first and then use the **switchport trunk allowed vsan add** command to complete the set of desired VSANs. The commands in the configuration are automatically rebuilt in numerical order by NX-OS.

Examples

The following example shows how to limit the VSANs on an interface to VSAN 10 to 20 and 50:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport trunk allowed vsan 10-20
switch(config-if)# switchport trunk allowed vsan add 50
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switchport trunk-max-npiv-limit

To configure the maximum number of logins that are allowed on a trunking interface, use the **switchport trunk-max-npiv-limit** command. To remove the configuration, use the **no** form of this command.

switchport trunk-max-npiv-limit *max-npivs*
no switchport trunk-max-npiv-limit *max-npivs*

Syntax Description

max-npivs	Specifies the maximum NPVI logins per trunk interface. The range is from 1 to 512.

Command Default

None.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 6.2(7)	This command was introduced.

Usage Guidelines

Both **switchport max-npiv-limit** and **switchport trunk-max-npiv-limit** commands can be configured on a port or Port Channel. The current port mode determines the type of configuration used. If the port is nontrunking, the **max-npiv-limit** setting is used. If the port is trunking, the **trunk-max-npiv-limit** setting is used.

If a login limit is reached on a port and it receives a login request, then a syslog message is logged and the login rejected.

Examples

The following example shows how to configure the maximum number of allowed logins on a trunking interface to 500:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport trunk-max-npiv-limit 500
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.
switchport max-npiv-limit	Configures the maximum number of logins that are allowed on a port.

switchport trunk mode

To specify the trunk mode for an interface, use the **switchport trunk mode** command. To remove the configuration, use the **no** form of this command.

switchport trunk mode {**auto**|**off**|**on**}
no switchport trunk mode {**auto**|**off**|**on**}

Syntax Description

auto	Specifies the trunk mode to be auto.
off	Disables trunking mode.
on	Enables trunking mode.

Command Default

The default trunk mode is **on**.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
NX-OS 1.0(2)	This command was introduced.

Usage Guidelines

Caution This command causes traffic disruption on the specified interface.

Note During ISSU, the admin trunk mode is set to **off** for up and operationally non trunking ports to avoid network disruption due to misbehaving peer devices.

By default, trunk mode is enabled on all Fibre Channel interfaces (modes E, F, FL, Fx, ST, and SD) on non-NPV switches. On NPV switches, by default, trunk mode is disabled. You can configure trunk mode as on (enabled), off (disabled), or auto (automatic). The trunk mode configuration at the two ends of an ISL, between two switches, determine the trunking state of the link and the port modes at both ends.

Table 4: Trunk Mode Status Between Switches

Configured Trunk Mode			Resulting State and Port Mode	
Port Type	**Switch 1**	**Switch 2**	**Trunking State**	**Port Mode**
E ports	On	Auto or on	Trunking (EISL)	TE port
	Off	Auto, on, or off	No trunking (ISL)	E port
	Auto	Auto	No trunking (ISL)	E port

Configured Trunk Mode			Resulting State and Port Mode	
Port Type	**Switch 1**	**Switch 2**	**Trunking State**	**Port Mode**
Port Type	**Core Switch**	**NPV Switch**	**Trunking State**	**Link Mode**
F and NP ports	On	Auto or on	Trunking	TF-TNP link
	Auto	On	Trunking	TF-TNP link
	Off	Auto, on, or off	No trunking	F-NP link

Examples

The following example shows how to set the trunk mode to auto on an interface:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# switchport trunk mode auto
```

Related Commands

Command	Description
show interface	Displays interface status and statistics.

switch-wwn

To configure a switch WWN in an autonomous fabric ID (AFID) database, use the **switch-wwn** command in AFID database configuration submode. To disable this feature, use the **no** form of this command.

switch-wwn *wwn-id* {**autonomous-fabric-id** *fabric-id* **vsan-ranges** *vsan-range*|**default-autonomous-fabric-id** *fabric-id* **vsan-ranges** *vsan-range*}
no switch-wwn *wwn-id* {**autonomous-fabric-id** *fabric-id* **vsan-ranges** *vsan-range*|**default-autonomous-fabric-id** *fabric-id***vsan-ranges** *vsan-range*}

Syntax Description

wwn-id	Specifies the port WWN, with the format hh:hh:hh:hh:hh:hh:hh:hh.
autonomous-fabric-id *fabric-id*	Specifies the fabric ID for the IVR topology.
vsan-ranges *vsan-range*	Specifies the IVR VSANs or range of VSANs. The range of values for a VSAN ID is 1 to 4093.
default-autonomous-fabric-id *fabric-id*	Specifies the default fabric ID for the IVR topology.

Command Default

Disabled.

Command Modes

AFID database configuration submode

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

Using the default-autonomous-fabric-id keyword configures the default AFID for all VSANs not explicitly associated with an AFID.

Examples

The following example adds a switch WWN, an AFID, and a range of VSANs to the AFID database:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ivr vsan-topology ?
  activate  Activate VSAN topology database for inter-VSAN routing
  auto      Enable discovery of VSAN topology for inter-VSAN routing
  database  Configure VSAN topology database for inter-VSAN routing
switch(config)# ivr vsan-topology auto
switch(config)# autonomous-fabric-id database
AFID database is used only when VSAN Topology is in AUTO mode
switch(config-afid-db)# ?
autonomous-fabric-id cfg. cmd:
  do          EXEC command
  exit        Exit from this submode
  no          Negate a command or set its defaults
  switch-wwn  Enter Switch WWN of a switch
switch(config-afid-db)# switch ?
  <hh:hh:hh:hh:hh:hh:hh:hh>  Enter a WWN in dotted hex notation
```

```
switch(config-afid-db)# switch 28:1d:00:05:30:00:06:ea ?
  autonomous-fabric-id          Enter Autonomous Fabric ID
  default-autonomous-fabric-id  Enter default Autonomous Fabric ID
switch(config-afid-db)# switch 28:1d:00:05:30:00:06:ea autonomous-fabric-id ?
  <1-64>  Enter an autonomous fabic ID
switch(config-afid-db)# switch 28:1d:00:05:30:00:06:ea autonomous-fabric-id 14 ?
  vsan-ranges  Enter VSANs in this autonomous-fabric-id at this switch
switch(config-afid-db)# switch 28:1d:00:05:30:00:06:ea autonomous-fabric-id 14 v
san-ranges ?
  <1-4093>  Enter upto 5 ranges of VSAN identifiers
switch(config-afid-db)# switch 28:1d:00:05:30:00:06:ea autonomous-fabric-id 14 vsan-ranges
 1-4 ?
  ,     Comma
  <cr>  Carriage Return
switch(config-afid-db)# switch-wwn 28:1d:00:05:30:00:06:ea autonomous-fabric-id 14 vsan-ranges
 1-4
```

The following example adds a switch WWN and the default AFID to the AFID database:

```
switch(config-afid-db)# ?
autonomous-fabric-id cfg. cmd:
  do          EXEC command
  exit        Exit from this submode
  no          Negate a command or set its defaults
  switch-wwn  Enter Switch WWN of a switch
switch(config-afid-db)# switch-wwn ?
  <hh:hh:hh:hh:hh:hh:hh:hh>  Enter a WWN in dotted hex notation
switch(config-afid-db)# switch-wwn 28:1d:00:05:30:00:06:ea ?
  autonomous-fabric-id          Enter Autonomous Fabric ID
  default-autonomous-fabric-id  Enter default Autonomous Fabric ID
switch(config-afid-db)# switch-wwn 28:1d:00:05:30:00:06:ea default-autonomous-fabric-id ?
  <1-64>  Enter a default autonomous fabic ID
switch(config-afid-db)# switch-wwn 28:1d:00:05:30:00:06:ea default-autonomous-fabric-id 16
 ?
  <cr>  Carriage Returnswitch(config-afid-db)# switch-wwn 28:1d:00:05:30:00:06:ea
default-autonomous-fabric-id 16
```

Related Commands

Command	Description
autonomous-fabric-id-database	Enters AFID database configuration submode.
show autonomous-fabric-id-database	Displays the contents of the AFID database.

system cores

To enable copying the core and log files periodically, use the **system cores** command in configuration mode. To revert the switch to factory defaults, use the **no** form of the command.

system cores {**slot0:**|**tftp:**}
no system cores

Syntax Description

slot0:	Selects the destination file system.
tftp:	Selects the destination file system.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Create any required directory before entering this command. If the directory specified by this command does not exist, the switch software logs a syslog message each time a copy cores is attempted.

Examples

The following example enables periodic copying core and log files:

```
switch# config terminal
switch(config)# system cores slot0:coreSample
```

The following example disables periodic copying core and log files:

```
switch(config)# no
 system cores
```

Related Commands

Command	Description
show system cores	Displays the currently configured scheme for copying cores.

system default interface congestion mode

To configure the default interface congestion mode, use the **system default interface congestionmode** command. To disable this feature, use the **no** form of the command.

system default interface congestion mode {**core**|**edge**}
no system default interface congestion mode {**core**|**edge**}

Syntax Description

core	Specifies the core port type.
edge	Specifies the edge port type.

Command Default

None.

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(6)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to configure the default interface congestion mode for the core port type:

```
switch# config terminal
switch(config)# system default interface congestion mode core
switch(config)#
```

The following example shows how to disable the default interface congestion mode for the edge port type:

```
switch# config terminal
switch(config)# no system default interface congestion mode edge
switch(config)#
```

Related Commands

Command	Description
show interface brief	Displays FC port modes.
show system default switchport	Displays default values for switch port attributes.

system default interface congestion timeout

To configure the default timeout value for a congestion timeout, use the **systemdefault interface congestion timeout** command. To disable this feature, use the **no** form of this command.

system default interface congestion timeout *milliseconds* **mode** {**core**|**edge**}
no system default interface congestion timeout *milliseconds* **mode** {**core**|**edge**}

Syntax Description

milliseconds	Number of milliseconds. The range is from 100 to 1000 milliseconds.
mode	Specifies the mode.
core	Specifies the core port type.
edge	Specifies the edge port type.

Command Default

500 milliseconds.

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(6)	This command was introduced.

Usage Guidelines

When you set a smaller timeout on the edge ports such as 100 or 200 milliseconds the congestion on the edge port is reduced by making the packets on that port time out sooner when they see the pause condition.

Note You should use the default configuration for core ports and a value that does not exceed 500 ms (100 to 200 ms preferably) for fabric edge ports.

Examples

The following example shows how to configure the default value for a congestion timeout for the core port type:

```
switch# config terminal
switch(config)# system default interface congestion timeout 100 mode core
switch(config)#
```

The following example shows how to disable the default value for a congestion timeout for the edge port type:

```
switch# config terminal
switch(config)# system default interface congestion timeout 100 mode edge
switch(config)#
```

Related Commands

Command	Description
show interface brief	Displays FC port modes.
show system default switchport	Displays default values for switch port attributes.

system default interface pause mode

To configure the default timeout value for a pause frame, use the **systemdefault interfacepause mode** command. To disable this feature, use the **no** form of this command.

system default interface pause mode {**core**|**edge**}
no system default interface pause mode {**core**|**edge**}

Syntax Description

core	Specifies the core port type.
edge	Specifies the edge port type.

Command Default

None.

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(6)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to configure the default timeout value for a pause frame for the core port type:

```
switch# config terminal
switch(config)# system default interface pause mode core
switch(config)#
```

The following example shows how to disable the timeout default value for a pause frame for the edge port type:

```
switch# config terminal
switch(config)# system default interface pause mode edge
switch(config)#
```

Related Commands

Command	Description
show interface brief	Displays FC port modes.
show system default switchport	Displays default values for switch port attributes.

system default interface pause timeout

To configure the default timeout value for a pause frame, use the **system defaultinterface pause timeout** command. To disable this feature, use the **no** form of the command.

system default interface pause timeout *milliseconds* **mode** {**core**|**edge**}
no system default interface pause timeout *milliseconds* **mode** {**core**|**edge**}

Syntax Description

milliseconds	Number of milliseconds. The range is from 100 to 500 milliseconds.
mode	Specifies the mode.
core	Specifies the core port type.
edge	Specifies the edge port type.

Command Default

500 milliseconds.

Command Modes

Global configuration mode

Command History

Release	Modification
5.2(6)	This command was introduced.

Usage Guidelines

When the port is in the state for the configured period, pause frame timeout can be enabled on that port. All frames that are sent to that port are dropped in the egress. This action frees up the buffer space in the ISL link (which carries traffic for this port) and helps to reduce congestion on other unrelated flows that use the same link.

Examples

The following example shows how to configure the timeout value pause frame for the core port type:

```
switch# config terminal
switch(config)# system default interface pause timeout 100 mode core
switch(config)#
```

The following example shows how to disable the timeout value pause for the edge port type:

```
switch# config terminal
switch(config)# system default interface pause timeout 100 mode edge
switch(config)#
```

Related Commands

Command	Description
show system default switchport	Displays default values for switch port attributes.

system default 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.

Command Default

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
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.

system default zone default-zone permit

To configure default values for a zone, use the **system default zone default-zone permit** command in configuration mode. To revert to the defaults, use the **no** form of the command.

system default zone default-zone permit
no system default zone default-zone permit

Syntax Description

This command has no arguments or keywords.

Command Default

No default values for zones.

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command defines the default values for the default zone for all VSANs. The default values are used when you initially create a VSAN and it becomes active. If you do not want to use the default values, use the **zone default-zone permit vsan** command to define the operational values for the default zone.

The **system default zone default-zone permit** command should only be used in conjunction with VSANs that have not yet been created; it has no effect on existing VSANs.

Note Because VSAN 1 is the default VSAN and is always present, this command has no effect on it.

Examples

The following example sets the default zone to use the default values:

```
switch# config terminal
switch(config)# system default zone default-zone permit
```

The following example restores the default setting:

```
switch(config)# no
 system default zone default-zone permit
```

Related Commands

Command	Description
show system default zone	Displays default values for the default zone.
zone default-zone permit vsan	Defines whether a default zone (nodes not assigned a created zone) permits or denies access to all in the default zone.

system default zone distribute full

To configure default values for distribution to a zone set, use the **system default zone distribute full** command in configuration mode. To revert to the defaults, use the **no** form of the command.

system default zone distribute full
no system default zone distribute full

Syntax Description

This command has no arguments or keywords.

Command Default

Distribution to active zone sets only.

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command distributes the default values for the default zone to all VSANs. The default values are used when you initially create a VSAN and it becomes active. If you do not want to use the default values, use the **zoneset distribute full vsan** command to distribute the operational values for the default zone.

The **system default zone distribute full** command should only be used in conjunction with VSANs that have not yet been created; it has no effect on existing VSANs.

Note Because VSAN 1 is the default VSAN and is always present, this command has no effect on it.

Examples

The following example distributes default values to the full zone set:

```
switch# config terminal
switch(config)# system default zone distribute full
```

The following example distributes default values to the active zone set only:

```
switch(config)# no
 system default zone distribute full
```

Related Commands

Command	Description
show system default zone	Displays default values for the default zone.
zoneset distribute full vsan	Distributes the operational values for the default zone to all zone sets.

system default zone gs

To configure default value for zone generic service permission, use the **system default zone gs** command in the configuration mode. To set the default value for zone generic service permission as none (deny), use the no form of the command.

system default zone gs {**read**|**read-write**}
no system default zone gs {**read**|**read-write**}

Syntax Description

read	Specifies the default zone generic service permission as read.
read-write	Specifies the default zone generic service permission as read-write.

Command Default

read-write.

Command Modes

Configuration mode

Command History

Release	Modification
3. 2(1)	This command was introduced.

Usage Guidelines

Setting write only as the default value for zone generic service permission is not supported.

Examples

The following example shows how to configure the default value for zone generic service permission as read only for new VSANs:

```
switch# config terminal
switch(config)# system default zone gs read
switch(config)#
```

The following example shows how to configure the default value for zone generic service permission as read-write for new VSANs:

```
switch# config terminal
switch(config)# system default zone gs read-write
switch(config)#
```

The following example shows how to configure the default value for zone generic service permission as none (deny) for new VSANs:

```
switch# config terminal
switch(config)# no system default zone gs read-write
switch(config)#
```

Related Commands

Command	Description
show system default zone	Displays the zone specific system default value settings.

system default zone mode enhanced

To configure the zone mode default value as enhanced, use the **system default zone mode enhanced** command in the configuration mode. To configure the zone mode default value as basic, use the no form of the command.

system default zone mode enhanced
no system default zone mode enhanced

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

This command configures the default value of zoning mode as basic or enhanced. The default value of zoning mode is used when a VSAN is newly created. If the VSAN is deleted and recreated, the value of the zoning mode defaults to the value specified by the configuration.

Examples

The following example shows how to configure the zone mode default value as enhanced:

```
switch# config
switch# system default zone mode enhanced
```

The following example shows how to configure the zone mode default value as basic:

```
switch# config
switch# no system default zone mode enhanced
```

Related Commands

Command	Description
show system default zone	Displays the default value of zone mode as basic and enhanced.

system default zone smart-zone

To configure the default values for smart zone, use the system default zone smart-zone command in the configuration mode. To disable this feature, use the no form of the command.

system default zone smart-zone enable
no system default zone smart-zone enable

Syntax Description

enable	Specifies the default smart zone enable or disable.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
5.2(6)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to configure the default values for smart-zone :

```
switch# config
switch(config)# no system default zone smart-zone enable
switch(config)#
```

Related Commands

Command	Description
show system default zone	Displays the default value of zone mode as basic and enhanced.

system delayed-traps enable mode

To configure the system-delayed trap state, use the **system delayed-traps enable** mode command. To disable the system-delayed trap state, use the **no** form of the command.

system delayed-traps enable mode FX
no system delayed-traps enable mode FX

Syntax Description

FX	Enables or disables delayed traps for operationally up FX (F/FX) mode interfaces.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
NX-OS 4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the system-delayed trap state:

```
switch(config)# system delayed-traps enable mode FX
switch(config)#
```

system delayed-traps timer

To configure the system-delayed trap timeout values, use the **system delayed-traps timer** command. To disable the system-delayed trap timeout values, use the **no** form of the command.

system delayed traps-timer *number*
no system delayed traps-timer *number*

Syntax Description

number	Indicates the delayed trap timer in minutes. The range is from 1 to 60.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
NX-OS 4.1(1b)	This command was introduced.

Usage Guidelines

System delayed traps timer is optional. If the user does not provide the timer value, default value of 4 is applied.

Examples

The following example shows how to configure system-delayed trap values:

```
switch(config)# system delayed-traps timer 30
switch(config)#
```

system hap-reset

Command	Description
show system default zone	Displays the default value of zone mode as basic and enhanced.

To configure the HA reset policy, use the **system hap-reset** command in EXEC mode. Use the **no** form of this command to disable this feature.

system hap-reset
system no hap-reset

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can disable the HA policy supervisor reset feature (enabled by default) for debugging and troubleshooting purposes.

Examples

The following example enables the supervisor reset HA policy:

```
switch# system hap-reset
```

system health (configuration mode)

To configure Online Health Management System (OHMS) features for a specified interface or for the entire switch, use the **system health** command. To disable this feature, use the **no** form of the command.

system health [{**failure-action**|**interface** {**fc** *slot/port*|**iscsi** *slot/port*}|**loopback** {**frame-length** { *bytes*|**auto**}|**frequency** *seconds*}}]
no system health [{**failure-action**|**interface** {**fc** *slot/port*|**iscsi** *slot/port*}}]

Note On a Cisco Fabric Switch for HP c-Class BladeSystem and on a Cisco Fabric Switch for IBM BladeCenter, the syntax differs as follows:**interface bay** *port* | **ext** *port* }

Syntax Description

failure-action	(Optional) Prevents the NX-OS software from taking any OHMS action for the entire switch.
interface	(Optional) Configures an interface.
fc *slot*/*port*	(Optional) Specifies the Fibre Channel interface to configure by slot and port number on an MDS 9000 Family switch.
iscsi *slot*/*port*	(Optional) Specifies the iSCSI interface to configure by slot and port number on an MDS 9000 Family switch.
bay *port* | ext *port*	(Optional) Configures the Fibre Channel interface on a port on a Cisco Fabric Switch for HP c-Class BladeSystem or on a Cisco Fabric Switch for IBM BladeCenter. The range is 0 to 48.
loopback	(Optional) Configures the OHMS loopback test.
frame-length *bytes*	(Optional) Specifies the frame-length in bytes ranging from 0 to 128 bytes for the loopback test.
auto	(Optional) Configures the frame-length to auto for the loopback test.
frequency *seconds*	(Optional) Specifies the loopback frequency in seconds ranging from 5 seconds (default) to 255 seconds.

Command Default

Enabled.

Frame-length is auto-size, which could range from 0 to 128.

Command Modes

Configuration mode

Command History

Release	Modification
1.3(4)	This command was introduced.
3.0(1)	Added the **frame-length** and **auto** options to the **loopback** keyword.

Release	Modification
3.1(2)	Added the **interface bay | ext** option.

Usage Guidelines

If you do not configure the loopback frequency value, the default frequency of 5 seconds is used for all modules in the switch.

Note The **no** form of the command is not supported for the **frame-length**, **auto**, and **frequency** options.

Examples

The following example disables OHMS in this switch:

```
switch# config terminal
switch(config)# no system health
System Health is disabled.
```

The following example enables (default) OHMS in this switch:

```
switch(config)# system health
System Health is enabled.
```

The following example enables OHMS in this interface:

```
switch(config)# no system health interface fc8/1
System health for interface fc8/13 is enabled.
```

The following example disables OHMS in this interface:

```
switch(config)# system health interface fc8/1
System health for interface fc8/13 is disabled.
```

The following example configures the loopback frequency to be 50 seconds for any port in the switch:

```
switch(config)# system health loopback frequency 50
The new frequency is set at 50 Seconds.
The following example configures the loopback frame-length to auto:
switch(config)# system health loopback frame-length auto
Loopback frame-length auto-size mode is now enabled.
```

The following example prevents the switch from taking any failure action:

```
switch(config)# system health failure-action
System health global failure action is now enabled.
```

The following example prevents the switch configuration from taking OHMS action (default) in case of a failure:

```
switch(config)# no system health failure-action
System health global failure action now disabled.
```

Related Commands

Command	Description
system health external-health	Explicitly runs an external Online Health Management System (OHMS) loopback test on demand for a specified interface or module.
system health internal-loopback	Explicitly runs an internal OHMS loopback test on demand for a specified interface or module.
system health serdes-loopback	Explicitly runs an internal OHMS Serializer/Deserializer (Serdes) loopback test on demand for a Fibre Channel interface.

system health cf-crc-check

To run the CompactFlash CRC checksum test on demand, use the **system health cf-crc-check** command in EXEC mode.

system health cf-crc-check module *slot*

Syntax Description

module*slot*	Specifies the module slot number.

Command Default

Enabled to automatically run in the background every 7 days.

Command Modes

EXEC mode

Command History

Release	Modification
3.1(3)	This command was introduced.

Usage Guidelines

Run the CompactFlash CRC checksum test on demand to determine if the CompactFlash firmware is corrupted and needs to be updated.

The CRC checksum test can be run on demand on the following modules:

- DS-X9016
- DS-X9032
- DS-X9302-14K9
- DS-X9308-SMIP
- DS-X9304-SMIP
- DS-X9530-SF1-K9

Examples

The following example shows how to run the CRC checksum test on demand:

```
switch# system health cf-crc-check module 4
```

Related Commands

Command	Description
show system health	Displays system health information.
show system health statistics	Displays system health statistics.

system health cf-re-flash

To update the CompactFlash firmware on demand, use the **system health cf-re-flash** command in EXEC mode.

system health cf-re-flash module *slot*

Syntax Description

module*slot*	Specifies the module slot number.

Command Default

Enabled to automatically run in the background every 30 days.

Command Modes

EXEC mode

Command History

Release	Modification
3.1(3)	This command was introduced.

Usage Guidelines

The CRC checksum test and the firmware update can be enabled on the following modules:

- DS-X9016
- DS-X9032
- DS-X9302-14K9
- DS-X9308-SMIP
- DS-X9304-SMIP
- DS-X9530-SF1-K9

Examples

The following example shows how to update firmware on demand:

```
switch# system health cf-re-flash module 4
```

Related Commands

Command	Description
show system health	Displays system health information.
show system health statistics	Displays system health statistics.

system health clear-errors

To clear previous error conditions stored in the Online Health Management System (OHMS) application's memory, use the **system health clear-errors** command.

system health clear-errors interface {**fc slotport**|**iscsi slotport**}
system health clear-errors module *slot*
[{**battery-charger**|**bootflash**|**cache-disk**|**eobc**|**inband**|**loopback**|**mgmt**}]

Note On a Cisco Fabric Switch for HP c-Class BladeSystem and on a Cisco Fabric Switch for IBM BladeCenter, the syntax differs as follows:**interface bay** *port* **| ext** *port* }

Syntax Description

interface	Specifies the interface to be configured.
fc *slot*/*port*	Configures the Fiber Channel interface on a Cisco MDS 9000 Family switch.
iscsi *slot*/*port*	Selects the iSCSI interface to configureon a Cisco MDS 9000 Family switch.
bay *port* **| ext** *port*	(Optional) Configures the Fibre Channel interface on a port on a Cisco Fabric Switch for HP c-Class BladeSystem or on a Cisco Fabric Switch for IBM BladeCenter.
module *slot*	Specifies the required module in the switch,
battery-charger	(Optional) Configures the OHMS battery-charger test on the specified module
bootflash	(Optional) Configures the OHMS bootflash test on the specified module.
cache-disk	(Optional) Configures the OHMS cache-disk test on the specified module.
eobc	(Optional)Configures the OHMS EOBC test on the specified module.
inband	(Optional) Configures the OHMS inband test on the specified module.
loopback	(Optional) Configures the OHMS loopback test on the specified module.
mgmt	(Optional) Configures the OHMS management port test on the specified module.

Command Default

Enabled.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.
3.1(2)	Added the **interface bay | ext** option.

Usage Guidelines

You can clear the error history for Fibre Channel interfaces, iSCSI interfaces, for an entire module, or one particular test for an entire module. The **battery-charger**, the **bootflash**, the **cache-disk**, the **eobc**, the **inband**, the **loopback**, and the **mgmt** test options can be individually specified for a given module.

The management port test cannot be run on a standby supervisor module.

Examples

The following example clears the error history for the specified Fibre Channel interface:

```
switch# system health clear-errors interface fc 3/1
```

The following example clears the error history for the specified module:

```
switch# system health clear-errors interface module 3
```

The following example clears the management port test error history for the specified module:

```
switch# system health clear-errors module 2 mgmt
```

system health external-loopback

To explicitly run an external Online Health Management System (OHMS) loopback test on demand (when requested by the user) for a specified interface or module, use the **system health external-loopback** command.

system health external-loopback {**interface fc** *slot/port*|**source interface fc** *slot/port* **destination fc** *slot/port*} [{**frame-length** *bytes* [**frame-count** *number*]|**frame-count** *number*}] **[force]**

Note On a Cisco Fabric Switch for HP c-Class BladeSystem and on a Cisco Fabric Switch for IBM BladeCenter, the syntax differs as follows:**interface bay** *port* **| ext** *port* }

Syntax Description

interface	Configures an interface.
fc *slot*/*port*	Configures the Fibre Channel interface specified by the slot and port on an MDS 9000 Family switch.
source	Specifies the source Fibre Channel interface.
destination	Specifies the destination Fibre Channel interface.
bay | **ext** port	(Optional) Configures the Fibre Channel interface on a Cisco Fabric Switch for HP c-Class BladeSystem or on a Cisco Fabric Switch for IBM BladeCenter . The range is 0 to 48.
frame-length *bytes*	(Optional) Configures the specified length of the loopback test frame in bytes. The range is 0 to 128 bytes.
frame-count *number*	(Optional) Configures the specified number of frames for the loopback test. The number of frames can range from 1 to 32.
force	(Optional) Directs the software to use the non-interactive loopback mode.

Command Default

The loopback is disabled.

The frame-length is 0. The frame-count is 1.

Command Modes

EXEC mode

Command History

Release	Modification
1.3(4)	This command was introduced.
3.0(1)	Added the **source** and **destination** keywords and the **frame-count** and **frame-length** options.
3.1(2)	Added the **interface bay** | **ext** option.

Usage Guidelines

Use this command to run this test on demand for the external devices connected to a switch that are part of a long haul network.

Examples

The following example displays an external loopback command for a Fibre Channel interface:

```
switch# system health external-loopback interface fc 3/1
This will shut the requested interfaces Do you want to continue (y/n)? [n] y
External loopback test on interface fc3/1 was  successful.
```

The following example displays the effect of the **force** option when implementing a forced loopback:

```
switch# system health external-loopback interface fc 3/1 force
External loopback test on interface fc3/1 was  successful.
```

Related Commands

Command	Description
system health	Configures Online Health Management System (OHMS) features for a specified interface or for the entire switch.
system health internal-loopback	Explicitly runs an internal OHMS loopback test on demand for a specified interface or module.
system health serdes-loopback	Explicitly runs an internal OHMS Serializer/Deserializer (Serdes) loopback test on demand for a Fibre Channel interface.

system health internal-loopback

To explicitly run an internal Online Health Management System (OHMS) loopback test on demand (when requested by the user) for a specified interface or module, use the **system health internal-loopback** command.

system health internal-loopback interface {**fc slot/port**|**iscsi slot**/**port**} [{**frame-length bytes** [**frame-count number**]|**frame-count number**}]

Note On a Cisco Fabric Switch for HP c-Class BladeSystem and on a Cisco Fabric Switch for IBM BladeCenter, the syntax differs as follows:**interface [bay** *port* **| ext** *port]*

Syntax Description

interface	Configures an interface.
fc *slot*/*port*	Configures the Fibre Channel interface specified by the slot and port on an MDS 9000 Family switch.
iscsi *slot*/*port*	Specifies the iSCSI interface to configure by slot and port on an MDS 9000 Family switch.
bay *port* **| ext** *port*	(Optional) Configures the Fibre Channel interface on a Cisco Fabric Switch for HP c-Class BladeSystem or on a Cisco Fabric Switch for IBM BladeCenter . The range is 0 to 48.
frame-length *bytes*	(Optional) Configures the specified length of the loopback test frame in bytes. The range is 0 to 128 bytes.
frame-count *number*	(Optional) Configures the specified number of frames for the loopback test. The number of frames can range from 1 to 32.

Command Default

The loopback is disabled.

The frame-length is 0. The frame-count is 1.

Command Modes

EXEC mode

Command History

Release	Modification
1.3(4)	This command was introduced.
3.0(1)	Added the **frame-count** and **frame-length** options.
3.1(2)	Added the **interface bay | ext** option.

Usage Guidelines

Internal loopback tests send and receive FC2 frames to and from the same ports and provide the round trip time taken in microseconds for the Fibre Channel interface.

Examples

The following example performs the internal loopback test for a Fibre Channel interface:

```
switch# system health internal-loopback interface iscsi 8/1
Internal loopback test on interface iscsi 8/1 was successful.
Round trip time taken is 79 useconds
```

Related Commands

Command	Description
system health	Configures Online Health Management System (OHMS) features for a specified interface or for the entire switch.
system health external-loopback	Explicitly runs an external OHMS loopback test on demand for a specified interface or module.
system health serdes-loopback	Explicitly runs an internal OHMS Serializer/Deserializer (Serdes) loopback test on demand for a Fibre Channel interface.

system health module

To configure Online Health Management System (OHMS) features for a specified module, use the **system health module** command. To disable these features, use the **no** form of this command.

system health module *slot* [{**battery-charger** [{**failure-action**|**frequency** *seconds*}]|**bootflash** [{**failure-action**|**frequency** *seconds*}]|**cache-disk** [{**failure-action**|**frequency** *seconds*}]|**cf-crc-check** [{**failure-action**|**frequency** *frequency*}]|**cf-re-flash** [{**failure-action**|**frequency** *frequency*}]|**eobc** [{**failure-action**|**frequency** *seconds*}]|**failure-action**|**inband** [{**failure-action**|**frequency** *seconds*}]|**loopback** **[failure-action]**|**mgmt** [{**failure-action**|**frequency** *seconds*}]}]
no system health module *slot* [{**battery-charger** [{**failure-action**|**frequency** *seconds*}]|**bootflash** [{**failure-action**|**frequency** *seconds*}]|**cache-disk** [{**failure-action**|**frequency** *seconds*}]|**cf-crc-check** [{**failure-action**|**frequency** *frequency*}]|**cf-re-flash** [{**failure-action**|**frequency** *frequency*}]|**eobc** [{**failure-action**|**frequency** *seconds*}]|**failure-action**|**inband** [{**failure-action**|**frequency** *seconds*}]|**loopback** **[failure-action]**|**mgmt** [{**failure-action**|**frequency** *seconds*}]}]

Syntax Description

slot	The module slot number.
battery-charger	(Optional) Configures the battery-charger test on the specified module.
failure-action	(Optional) Controls the software from taking any action if a CompactFlash failure is determined while running the CRC checksum test.
frequency *seconds*	(Optional) Specifies the frequency in seconds. The range for the **bootflash frequency** option is 10 to 255. The range for the **cf-crc-check frequency** option is 1 to 30. The range for the **cf-re-flash frequency** option is 30 to 90. For all other options, the range is 5 to 255.
bootflash	Configures the bootflash test on the specified module.
cache-disk	Configures the cache-disk test on the specified module.
cf-crc-check	Configures the CRC checksum test.
cf-re-flash	Configures the firmware update.
eobc	Configures the EOBC test on the specified module.
inband	Configures the inband test on the specified module.
loopback	Configures the loopback test on the specified module.
mgmt	Configures the management port test on the specified module.

Command Default

The default for OHMS is enabled.

The CRC Checksum test is enabled to automatically run in the background every 7 days.

The firmware update is enabled to automatically run in the background every 30 days.

The **failure-action** feature is enabled.

Command Modes

Configuration mode

Command History

Release	Modification
1.3(4)	This command was introduced.
3.1(3)	Added the **cf-crc-check** and **cf-reflash** options.

Usage Guidelines

The CRC checksum test and the firmware update can be enabled on the following modules:

- DS-X9016
- DS-X9032
- DS-X9302-14K9
- DS-X9308-SMIP
- DS-X9304-SMIP
- DS-X9530-SF1-K9

If you do not configure the loopback frequency value, the default frequency of 5 seconds is used for all modules in the switch.

Examples

The following example enables the battery-charger test on both batteries in the CSM module. If the switch does not have a CSM, this message is issued:

```
switch# config terminal
switch(config)# system health module 6 battery-charger
battery-charger test is not configured to run on module 6.
```

The following example enables the cache-disk test on both disks in the CSM module. If the switch does not have a CSM, this message is issued:

```
switch(config)# system health module 6 cache-disk
cache-disk test is not configured to run on module 6.
```

The following example enables the bootflash test:

```
switch(config)# system health module 6 bootflash
System health for module 6 Bootflash is already enabled.
```

The following example enables you to prevent the NX-OS software from taking any action if any component fails:

```
switch(config)# system health module 6 bootflash failure-action
System health failure action for module 6 Bootflash test is now enabled.
```

The following example enables an already-enabled bootflash test:

```
switch(config)# system health module 6 bootflash failure-action
System health failure action for module 6 Bootflash test is already enabled.
```

The following example disables the bootflash test configuration:

```
switch(config)# no system health module 6 bootflash failure-action
System health failure action for module 6 Bootflash test is now disabled.
```

The following example sets the new frequency of the bootflash test to 200 seconds:

```
switch(config)# system health module 6 bootflash frequency 200
The new frequency is set at 200 Seconds.
```

The following example enables the EOBC test:

```
switch(config)# system health module 6 eobc
System health for module 6 EOBC is now enabled.
```

The following example enables the inband test:

```
switch(config)# system health module 6 inband
System health for module 6 EOBC is now enabled.
```

The following example enables the loopback test:

```
switch(config)# system health module 6 loopback
System health for module 6 EOBC is now enabled.
```

The following example enables the management test:

```
switch(config)# system health module 6 management
System health for module 6 EOBC is now enabled.
```

The following example shows how to set the CompactFlash CRC test interval:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# system health module 6 cf-crc-check frequency 10
```

The following example shows how to set the CompactFlash CRC test **failure-action** feature:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# system health module 6 cf-crc-check failure-action
```

The following example shows how to set the CompactFlash reflash update interval:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# system health module 6 cf-reflash frequency 10
```

The following example shows how to set the CompactFlash reflash **failure-action** feature:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# system health module # cf-re-flash failure-action
```

Related Commands

Command	Description
show system health	Displays system health information.
show system health statistics	Displays system health statistics.

system health serdes-loopback

To explicitly run an internal Online Health Management System (OHMS) Serializer/Deserializer (Serdes) loopback test on demand (when requested by the user) for a Fibre Channel interface, use the **system health serdes-loopback** command.

system health serdes-loopback interface fc *slot/port* [{**frame-length** *bytes* [**frame-count** *number*]|**frame-count** *number*}] **[force]**

Syntax Description

Note On a Cisco Fabric Switch for HP c-Class BladeSystem and on a Cisco Fabric Switch for IBM BladeCenter, the syntax differs as follows:**interface bay** *port* **| ext** *port* }

interface	Configures an interface.
fc *slot*/*port*	(Optional) Configures the Fiber Channel interface specified by the slot and port on an MDS 9000 Family switch.
bay *port* **| ext** *port*	(Optional) Configures the Fibre Channel interface on a Cisco Fabric Switch for HP c-Class BladeSystem or on a Cisco Fabric Switch for IBM BladeCenter. The range is 0 to 48.
force	Directs the software to use the non-interactive loopback mode.
frame-length *bytes*	(Optional) Configures the specified length of the loopback test frame in bytes. The range is 0 to 128 bytes.
frame-count *number*	(Optional) Configures the specified number of frames for the loopback test. The number of frames can range from 1 to 32.

Command Default

Loopback is disabled.

The frame-length is 0. The frame-count is 1.

Command Modes

EXEC mode

Command History

Release	Modification
3.0(1)	This command was introduced.
3.1(2)	Added the **interface bay | ext** option**.**

Usage Guidelines

None.

Examples

The following example performs a Serdes loopback test within ports for an entire module:

```
switch# system health serdes-loopback interface fc 4/1
```

This will shut the requested interfaces Do you want to continue (y/n)? [n] y

```
Serdes loopback test on interface fc 4/1 was successful.
```

The following example performs a Serdes loopback test within ports for the entire module and overrides the frame count configured on the switch:

```
switch# system health serdes-loopback interface fc 3/1 frame-count 10
This will shut the requested interfaces Do you want to continue (y/n)? [n] y
Serdes loopback test passed for module 3 port 1
```

Related Commands

Command	Description
system health	Configures Online Health Management System (OHMS) features for a specified interface or for the entire switch.
system health external-loopback	Explicitly runs an external OHMS loopback test on demand for a specified interface or module.
system health internal-loopback	Explicitly runs an internal OHMS loopback test on demand for a specified interface or module.

system heartbeat

To enable system heartbeat checks, use the **system heartbeat** command in EXEC mode. Use the **no** form of this command to disable this feature.

system heartbeat
no system heartbeat

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can disable the heartbeat checking feature (enabled by default) for debugging and troubleshooting purposes such as attaching a GDB to a specified process.

Examples

The following example enables the system heartbeat checks:

```
switch# system heartbeat
```

system memlog

To collect system memory statistics, use the **system memlog** command in EXEC mode.

system memlog

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use this command for debugging and troubleshooting purposes.

Examples

The following example enables system memory logging:

```
switch# system memlog
```

system port pacer mode F interface-login-threshold

To enable the pacer mode for F port threshold limit, use the **system port pacer mode F interface -login-threshold** command.

system port pacer mode F interface-login-threshold *port-threshold limit* **concurrent-ports** *port-number*

Syntax Description

mode F	Specifies the F mode.
interface-login-threshold *port-threshold limit*	Specifies the per port threshold limit. The range is from 0 to 256.
concurrent-ports *port-number*	Specifies the maximum number of concurrent port bring up allowed. The range is from 1 to 16. Preferred value is 1.

Command Default

Disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
6.2(7)	This command was introduced.

Usage Guidelines

Note Concurrent-ports port-number needs to be set depending upon customers topology and tune this value onto how many F ports can be brought up simultaneously.

Note Fx or FL or E ports are not supported.

Examples

The following example shows how to enable the pacer mode F for port threshold limit:

```
switch(config)#
system port pacer mode F interface-login-threshold 10 concurrent-ports 1
switch(config)#
```

system startup-config

To release a system startup configuration lock, use the system startup-config**system startup config** command in EXEC mode.

system startup-config unlock *lock-id*

Syntax Description

unlock *lock-id*	Configures the system startup-config unlock ID number. The range is 0 to 65536.

Command Default

Disabled.

Command Modes

EXEC

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

The **system startup-config** command allows you to unlock or release the rr_token lock. To determine the *lock-id, use the* **show system internal sysmgr startup-config locks** command.

Examples

The following example releases the system configuration lock with identifier 1:

```
switch# system ?
  hap-reset       Enables resetting of local or remote sup on ha failures
  health          System health exec commands
  heartbeat       Enables heartbeat
  memlog          Generate memory log in bootflash
  no              Negate a command or set its defaults
  pss             PSS commands
  standby         System standby manual boot
  startup-config  System startup-config commands
  statistics      Changes statistics configuration
  switchover      Switchover now
  watchdog        Enables watchdog
switch# system startup-config ?
  unlock  Unlock startup-config
switch# system startup-config unlock ?
  <0-65536>  Startup-config lock id
switch# system startup-config unlock 1 ?
  <cr>  Carriage Return
switch# system startup-config unlock 1
```

Related Commands

Command	Description
show system	Displays system information.

system statistics reset

To reset the high availability statistics collected by the system, use the **system statistics reset** command in EXEC mode.

system statistics reset

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can disable the system statistics reset feature (enabled by default) for debugging and troubleshooting purposes.

Examples

The following example resets the HA statistics:

```
switch# system statistics reset
```

system switchover (configuration mode)

To enable a switchover for the system, use the **system switchover** command in configuration mode. To revert to the factory default setting, use the **no** form of the command.

system switchover {**ha**|**warm**}
no system switchover

Syntax Description

ha	Specifies an HA switchover.
warm	Specifies a warm switchover.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example enables a HA switchover from an active supervisor module to a standby supervisor module:

```
switch# config terminal
switch(config)# system switchover ha
```

system switchover (EXEC mode)

To specifically initiate a switchover from an active supervisor module to a standby supervisor module, use the**system switchover** command in EXEC mode.

system switchover

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

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.

system timeout congestion-drop

To configure the system timeout values for congestion drop, use the **system timeout congestion-drop** command.

system timeout congestion-drop *number* **logical-type** {**core** | **edge**}|**default logical-type** {**core** | **edge**}

Syntax Description

number	Number in milliseconds. The range is from 200 ms to 500 ms. The congestion timeout value should be in multiples of 10.
default	Specifies the default timeout values for congestion drop.
logical-type	Specifies the logical type for a port.
core	Specifies the core mode.
edge	Specifies the edge mode.

Command Default

The default system timeout congestion-drop value is 500 ms.

Command Modes

Global configuration mode

Command History

Release	Modification
8.1(1)	• **mode** keyword was change to **logical-type** keyword, **E** keyword was changed to **core** keyword, and **F** keyword was changed to **edge** keyword. • The system timeout congestion-drop value range was changed from 100-500 ms to 200-500 ms.
4.2(7a)	This command was introduced.

Usage Guidelines

Each packet received by the MDS is timestamped. This timer determines hold long the MDS holds packets to transmit. If the timer expires then the packet is discarded as a timeout frame.

Examples

The following example shows how to configure the system timeout values for congestion drop core mode:

```
switch# configure terminal
switch(config)# system timeout congestion-drop 210 logical-type core
```

The following example shows how to configure the default timeout values for congestion drop core mode:

```
switch(config)# system timeout congestion-drop default logical-type core
```

Related Commands

Command	Description
system timeout no-credit-drop	Configures the system timeout values for no credit drop.

system timeout no-credit-drop

To configure the system timeout values for no credit drop, use the **system timeout no-credit-drop** command. To disable the system timeout values, use the **no** form of this command.

{**system timeout no-credit-drop** *number* **logical-type edge**|**default logical-type edge**}
{**no system timeout no-credit-drop** *number* **logical-type edge**|**default logical-type edge**}

Syntax Description

number	Number in milliseconds. The range is from 1 to 500 milliseconds.
default	Specifies the default timeout values for no credit drop. The default value is 500 milliseconds.
logical-type	Specifies the logical type for a port.
edge	Specifies the edge mode.

Command Default

By default, frame dropping is disabled and the frame timeout value is 500 ms for all port types.

Command Modes

Global configuration mode

Command History

Release	Modification
8.1(1)	**mode** keyword was change to **logical-type** keyword, and **F** keyword was changed to **edge** keyword.
6.2(9)	Changed the **no-credit-drop** timeout value.
4.2(7a)	This command was introduced.

Usage Guidelines

This timer, when enabled, determines how long an interface is at zero Tx buffer to buffer credits before it starts dropping packets immediately and not waiting for the congestion-drop timeout.

Note **no-credit- drop** timeout value has been changed from 100 to 500 in multiples of 100 milliseconds. Current range changes from 1 to 500 in multiples of 1 milliseconds.

Examples

The following example shows how to configure the system timeout values for no credit drop edge mode:

```
switch(config)# system timeout no-credit-drop 100 logical-type edge
```

The following example shows how to configure the default timeout values for no credit drop edge mode:

```
switch(config)# system timeout no-credit-drop default logical-type edge
```

The following example shows how to disable the system timeout value for no credit drop edge mode:

```
switch(config)# no system timeout no-credit-drop default logical-type edge
```

Related Commands

Command	Description
system timeout congestion-drop	Configures the system timeout values for congestion drop.

system timeout slowport-monitor

To configure the system timeout values for hardware slowport monitoring, use the **system timeout slowport-monitor** command. To remove this feature, use the **no** form of this command.

system timeout slowport-monitor *number* **default mode E/F**
no system timeout slowport-monitor *number* **default mode E/F**

Syntax Description

number	Number in milliseconds. The range is from 1 to 500 milliseconds.
default	Specifies the default timeout value for the hardware slowport monitoring. The default value is 50 milliseconds.
mode	Specifies the Port mode.
E	Specifies the E port mode.
F	Specifies the F port mode.

Command Default

Disabled.

Command Modes

Global configuration mode

Command History

Release	Modification
6.2(9)	This command was introduced.

Usage Guidelines

This timer, when enabled, starts the slowport monitoring of ports and collects the statistics information like average credit delay and the number of times slowport event detected count.

This command is applicable for the platforms that support hardware slowport monitoring (MDS 9710, 9706,9250i,9148S).

Examples

The following example shows how to configure the system timeout values for hardware slowport monitoring:

```
switch(config)# system timeout slowport-monitor 10 mode F
switch(config)#
```

The following example shows how to configure the default timeout values for hardware slowport monitoring:

```
switch(config)# system timeout slowport-monitor default mode F
switch(config)#
```

Related Commands

Command	Description
show process creditmon slowport-monitor-events	Displays the slowport monitor statistics information.

system trace

To configure the system trace level, use the **system trace** command in configuration mode. To disable this feature, use the **no** form of the command.

system trace *bit-mask*
no system trace

Syntax Description

bit-mask	Specifies the bit mask to change the trace level.

Command Default

None.

Command Modes

Configuration mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command is used for debugging purposes.

Examples

The following example shows how to configure the system trace level:

```
switch# config terminal
switch(config)# system trace 0xff
```

system watchdog

To enable watchdog checks, use the **system watchdog** command in EXEC mode. To disable this feature, use the **no** form of the command.

system watchdog
no system watchdog

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If a watchdog is not logged at every 8 seconds by the software, the supervisor module reboots the switch.

You can disable the watchdog checking feature (enabled by default) for debugging and troubleshooting purposes such as attaching a GDB or a kernel GDB (KGDB) to a specified process.

Examples

The following example enables the system watchdog:

```
switch# system watchdog
```

Show Commands

show aaa accounting

To display the accounting configuration, use the **show aaa accounting** command.

show aaa accounting

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays accounting log configuration:

```
switch# show aaa accounting
         default: local
```

Related Commands

Command	Description
aaa accounting default	Configures the default accounting method.

show aaa authentication

To display configured authentication information, use the **show aaa authentication** command.

show aaa authentication [**login** {**error-enable**|}]

Syntax Description

login error-enable	(Optional) Displays the authentication login error message enable configuration.
login **mschap**	(Optional) Displays the authentication login MS-CHAP enable configuration.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(x)	Added the login error-enable option.
3.0(1)	Added the **login mschap** option.

Usage Guidelines

None.

Examples

The following example displays the configured authentication parameters:

```
switch# show aaa authentication
        default: group TacServer local none
        console: local
        iscsi: local
        dhchap: local
```

The following example displays the authentication login error message enable configuration:

```
switch# show aaa authentication login error-enable
disabled
```

The following example displays the authentication login MS-CHAP enable configuration:

```
switch# show aaa authentication login mschap
disabled
```

show aaa authentication login ascii-authentication

To display configured ascii authentication method, use the show aaa authentication login ascii-authentication command.

show aaa authentication login ascii-authentication

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(3a)	enable the password aging command changed from show aaa authentication login password-aging enable to show aaa authentication login ascii-authentication.

Usage Guidelines

None.

Examples

The following example shows how to enable ascii authentication:

```
switch#(config)# aaa authentication login ascii-authentication
switch#(config)#
```

Related Commands

Command	Description
aaa authentication login ascii-authentication	Enables the ascii authentication method.

show aaa authentication login chap enable

To display CHAP authentication for login, use the show aaa authentication login chap enable command.

show aaa authentication login chap enable

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display CHAP authentication for login:

```
switch# show aaa authentication login chap enable
CHAP is enabled
switch#
```

Related Commands

Command	Description
aaa authentication login chap enable	Enables CHAP authentication for login.

show aaa authentication login mschapv2

To display MS-CHAPv2 authentication for login, use the show aaa authentication login mschapv2 command.

show aaa authentication login mschapv2

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display MS-CHAPv2 authentication for login:

```
switch# show aaa authentication login mschapv2
MSCHAP V2 is disabled
switch#
```

Related Commands

Command	Description
aaa authentication login mschapv2 enable	Enables MS-CHAPv2 authentication for login.

show aaa authorization all

To display all authorization information, use the aaa authorization all command.

show aaa authorization all

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display all authorization information:

```
switch# show aaa authorization all
AAA command authorization:
         default authorization for config-commands: local
         default authorization for commands: local
```

show aaa groups

To display configured server groups, use the **show aaa groups** command.

show aaa groups

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to display configured server groups:

```
switch# show aaa groups
radius
TacServer
```

show accounting log

To display the accounting log contents, use the **show accounting log** command.

show accounting log [*size*]

Syntax Description

size	(Optional) Specifies the size of the log to display in bytes. The range is 0 to 250000.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the entire accounting log:

```
switch# show accounting log
2002:stop:snmp_1033151784_171.71.49.83:admin:
Fri Sep 27 18:36:24 2002:start:_1033151784:root
Fri Sep 27 18:36:28 2002:update:::fcc configuration requested
Fri Sep 27 18:36:33 2002:start:snmp_1033151793_171.71.49.83:admin
Fri Sep 27 18:36:33 2002:stop:snmp_1033151793_171.71.49.83:admin:
Fri Sep 27 18:39:28 2002:start:snmp_1033151968_171.71.49.96:admin
Fri Sep 27 18:39:28 2002:stop:snmp_1033151968_171.71.49.96:admin:
Fri Sep 27 18:39:28 2002:start:_1033151968:root
Fri Sep 27 18:39:31 2002:update:::fcc configuration requested
Fri Sep 27 18:39:37 2002:start:snmp_1033151977_171.71.49.96:admin
Fri Sep 27 18:39:37 2002:stop:snmp_1033151977_171.71.49.96:admin:
Fri Sep 27 18:39:37 2002:start:snmp_1033151977_171.71.49.96:admin
Fri Sep 27 18:42:12 2002:start:snmp_1033152132_171.71.49.96:admin
Fri Sep 27 18:42:12 2002:stop:snmp_1033152132_171.71.49.96:admin:
Fri Sep 27 18:42:12 2002:start:snmp_1033152132_171.71.49.96:admin
Fri Sep 27 18:42:40 2002:start:snmp_1033152160_171.71.49.96:admin
...
```

The following example displays 400 bytes of the accounting log:

```
switch# show accounting log 400
Tue Dec  8 22:06:59 1981:start:/dev/pts/2_376697219:admin:
Tue Dec  8 22:07:03 1981:stop:/dev/pts/2_376697219:admin:shell terminated
Tue Dec  8 22:07:13 1981:start:/dev/pts/2_376697233:admin:
Tue Dec  8 22:07:53 1981:stop:/dev/pts/2_376697233:admin:shell terminated
Tue Dec  8 22:08:15 1981:update:/dev/ttyS0_376628597:admin:iSCSI Interface Vsan Enabled
```

Related Commands

Command	Description
clear accounting log	Clears the accounting log.

show arp

To display Address Resolution Protocol (ARP) entries, use the **show arp** command.

show arp

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

This example shows how to display the ARP table:

```
switch# show arp
Protocol Address           Age (min)           Hardware Addr   Type   Interface
Internet  171.1.1.1        0      0006.5bec.699c  ARPA  mgmt0
Internet  172.2.0.1        4    0000.0c07.ac01  ARPA  mgmt0
```

Related Commands

Command	Description
clear arp-cache	Clears the arp-cache table entries.

show autonomous-fabric-id database

To display the contents of the AFID database, use the **show autonomous-fabric-id database** command in EXEC mode.

show autonomous-fabric-id database

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows contents of the AFID database:

```
switch# show autonomous-fabric-id database
SWITCH WWN                      Default-AFID
------------------------------------------------------------
20:00:00:0c:91:90:3e:80            5
Total:   1 entry in default AFID table
SWITCH WWN                      AFID     VSANS
------------------------------------------------------------
20:00:00:0c:91:90:3e:80           10     1,2,5-8
Total: 1 entry in AFID table
```

Related Commands

Command	Description
autonomous-fabric-id (IVR topology database configuration)	Configures an autonomous fabric ID into the Inter-VSAN Routing (IVR) topology database.
autonomous-fabric-id (IVR service group configuration)	Configures an autonomous fabric ID into the IVR service group.
autonomous-fabric-id-database	Configures an autonomous fabric ID (AFID) database.

show banner motd

To display a configured message of the day (MOTD) banner, use the **show banner motd** command.

show banner motd

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

The configured MOTD banner is displayed before the login prompt on the terminal whenever a user logs in to a switch.

Examples

The following example displays the configured banner message:

```
switch# show banner motd
Testing the MOTD Feature
```

The configured message is visible the next time you log in to the switch:

```
 Testing the MOTD Featureswitch login:
```

Related Commands

Command	Description
banner motd	Configures the required banner message.

show boot

To display the boot variables or modules, use the **show boot** command.

show boot [{**module** [{*slotvariable-name*}]|**sup-1**|**sup-2**|**variables**}]

Syntax Description

module	(Optional) Displays the boot variables for modules.
slot	Specifies a module by the slot number.
variable-name	Specifies the variable. Maximum length is 80 characters.
sup-1	(Optional) Displays the upper sup configuration.
sup-2	(Optional) Displays the lower sup configuration.
variables	(Optional) Displays the list of boot variables.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the current contents of the boot variable:

```
switch# show boot
kickstart variable = bootflash:/kickstart-image
system variable = bootflash:/system-image
Module 2
asm-sfn variable = bootflash:/asm-image
```

The following example displays the images on the specified module:

```
switch# show boot module
Module 2
asm-sfn variable = bootflash:/asm-image
```

The following example displays a list of all boot variables:

```
switch# show boot variables
List of boot variables are:
     asm-sfn
  system
     kickstart
```

show boot auto-copy

To display state of the auto-copy feature, use the **show boot auto-copy** command.

show boot auto-copy [list]

Syntax Description

list	(Optional) Displays the list of files to be auto-copied

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows the message that displays on the console when you enable the auto-copy feature:

```
switch(config)# boot auto-copy
 Auto-copy administratively enabled
```

The following example shows the message that displays on the console when you disable the auto-copy feature:

```
switch(config)# boot auto-copy
 Auto-copy administratively disabled
```

The following example displays the current state of the auto-copy feature when it is enabled:

```
switch# show boot auto-copy
Auto-copy feature is enabled
```

The following example displays the current state of the auto-copy feature when it is disabled:

```
switch# show boot auto-copy
Auto-copy feature is disabled
```

The following example displays the ilc1.bin image being copied to the standby supervisor module's bootflash, and once this is successful, the next file will be lasilc1.bin. This command only displays files on the active supervisor module.

```
switch# show boot auto-copy list
File: /bootflash/ilc1.bin
Bootvar: ilce
File:/bootflash/lasilc1.bin
Bootvar: lasilc
```

The following example displays a typical message when the auto-copy option is disabled or if no files are copied:

```
switch# show boot auto-copy list
No file currently being auto-copied
```

show callhome

To display Call Home information configured on a switch, use the **show callhome** command.

show callhome [{**destination-profile** [**profile** {*profile*|**full-txt-destination**|**short-txt-destination**|**XML-destination**}]|**last** {**action status**|**merge status**}|**pending**|**pending-diff**|**script-mapping**|**transport-email**|**user-def-cmds**}]

Syntax Description

destination-profile	(Optional) Displays the Call Home destination profile information.
profile	(Optional) Specifies the destination profile.
profile	Specifies a user-defined destination profile.
full-txt-destination	Specifies the full text destination profile.
short-txt-destination	Specifies the short text destination profile.
XML-destination	Specifies the XML destination profile.
last action status	(Optional) Displays the status of the last CFS commit or discard operation.
last merge status	(Optional) Displays the status of the last CFS merge operation.
pending	(Optional) Displays the status of pending Call Home configuration.
pending-diff	(Optional) Displays the difference between running and pending Call Home configurations.
script-mapping	(Optional) Displays the scripts that are configured for each alert-group.
transport-email	(Optional) Displays the Call Home e-mail transport information.
user-def-cmds	(Optional) Displays the CLI commands configured for each alert group.

Command Default

None

Command Modes

Privilege EXEC(#)

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0(x)	Added **last action status**, **pending**, and **pending-diff** options.
3.0(1)	Added the **user-def-cmds** argument.
7.3(1)DY(1)	Added the **script-mapping** keyword.

Usage Guidelines

Note The **script-mapping** option is only for use by certain customers. Do not configure it if you are not approved by Cisco to use it.

Examples

The following example shows configured Call Home information:

```
switch# show callhome

callhome enabled
Callhome Information:
contact person name:who@where
contact person's email:person@place.com
contact person's phone number:310-408-4000
street addr:1234 Picaboo Street, Any city, Any state, 12345
site id:Site1ManhattanNewYork
customer id:Customer1234
contract id:Andiamo1234
switch priority:0
duplicate message throttling : enabled
periodic inventory : disabled
periodic inventory time-period : 7 days
distribution of callhome configuration data using cfs : disabled
```

The following example shows all destination profile information:

```
switch# show callhome destination-profile

XML destination profile information
maximum message size:250000
email addresses configured:
findout@.cisco.com
Short-txt destination profile information
maximum message size:4000
email addresses configured:
person1@epage.company.com
full-txt destination profile information
maximum message size:250000
email addresses configured:
person2@company2.com
```

The following example shows the full-text destination profile:

```
switch# show callhome destination-profile profile full-txt-destination

full-txt destination profile information
maximum message size:250000
email addresses configured:
person2@company2.com
```

The following example shows the short-text destination profile:

```
switch# show callhome destination-profile profile short-txt-destination
Short-txt destination profile information
maximum message size:4000
email addresses configured:
person2@company2.com
```

The following example shows the XML destination profile:

```
switch# show callhome destination-profile profile XML-destination
XML destination profile information
maximum message size:250000
email addresses configured:
findout@.cisco.com
```

The following example shows email and SMTP information:

```
switch# show callhome transport-email
from email addr:user@company1.com
reply to email addr:pointer@company.com
return receipt email addr:user@company1.com
smtp server:server.company.com
smtp server port:25
```

The following example shows user-defined CLI commands for the alert groups:

```
switch# show callhome user-def-cmds
User configured commands for alert groups :
alert-group test user-def-cmd "show version"
```

Related Commands

Command	Description
alert-group	Customizes a Call Home alert group with user-defined **show** commands.
callhome	Configures Call Home.
callhome test	Sends a dummy test message to the configured destination(s).

show callhome transport

To display the Call Home transport configuration, use the show callhome transport command.

show callhome transport

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 5.2(1)	Changed the command output.
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the Call Home transport when the proxy is not configured :

```
switch# show callhome transport
http vrf:management
from email addr:S1-2@cisco.com
smtp server:171.69.21.28
smtp server port:25
smtp server vrf:management
smtp server priority:0
http proxy server:10.64.65.62
http proxy server port:8080
http proxy status:Enabled
switch#
```

Related Commands

Command	Description
callhome	Configures the Call Home function.

show cdp

To display CDP parameters configured globally or for a specific interface, use the **show cdp** command.

show cdp {**all**|**entry** [{**all**|**name** *cdp-name*}]|**global**|**interface** [{**gigabitethernet** *slot* / *port*|**mgmt 0**}]|**neighbors** [{**detail**|**interface** {**gigabitethernet** *slot* / *port*|**mgmt 0**}}]|**traffic interface** [{**gigabitethernet** *slot* / *port*|**mgmt 0**}]}

Syntax Description

all	Displays all enabled CDP interfaces.
entry	Displays CDP database entries.
all	(Optional) Displays all CDP entries in the database
name *cdp-name*	(Optional) Displays CDP entries that match a specified name. Maximum length is 256 characters.
global	Displays global CDP parameters.
interface	Displays CDP information for neighbors on a specified interface.
gigabitethernet *slot*/*port*	(Optional) Specifies the Gigabit Ethernet interface at the slot number and port number separated by a slash (/).
mgmt 0	(Optional) Specifies the Ethernet management interface.
neighbors	Displays all CDP neighbors.
detail	(Optional) Displays detailed information for all CDP neighbors
interface	Displays CDP information for neighbors on a specified interface.
traffic	Displays CDP traffic statistics for an interface.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is allowed only on the active supervisor module in the Cisco MDS 9500 Series.

Examples

The following example displays all CDP-capable interfaces and parameters:

```
switch# show cdp all
GigabitEthernet4/1 is up
    CDP enabled on interface
```

```
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
GigabitEthernet4/8 is down
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
mgmt0 is up
    CDP enabled on interface
    Sending CDP packets every 100 seconds
    Holdtime is 200 seconds
```

The following example displays all CDP neighbor entries:

```
switch# show cdp entry all
----------------------------------------
Device ID:Switch
System Name:
Interface address(es):
Platform: cisco WS-C2950T-24, Capabilities: Switch IGMP Filtering
Interface: mgmt0, Port ID (outgoing port): FastEthernet0/24
Holdtime: 152 sec

Version:
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(19)EA1c, RELEASE SOFTWARE
 (fc2)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Mon 02-Feb-04 23:29 by yenanh

Advertisement Version: 2
Native VLAN: 1
Duplex: full
```

The following example displays the specified CDP neighbor:

```
switch# show cdp entry name 0
----------------------------------------
Device ID:0
Entry address(es):
    IP Address: 209.165.200.226
Platform: DS-X9530-SF1-K9, Capabilities: Host
Interface: GigabitEthernet4/1, Port ID (outgoing port): GigabitEthernet4/1
Holdtime: 144 sec
Version:
1.1(0.144)
Advertisement Version: 2
Duplex: full
```

The following example displays global CDP parameters:

```
switch# show cdp global
Global CDP information:
    CDP enabled globally
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled
```

The following example displays CDP parameters for the management interface:

```
switch# show cdp interface mgmt 0
mgmt0 is up
    CDP enabled on interface
```

```
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
```

The following example displays CDP parameters for the Gigabit Ethernet interface:

```
switch# show cdp interface gigabitethernet 4/1
GigabitEthernet4/1 is up
    CDP enabled on interface
    Sending CDP packets every 80 seconds
    Holdtime is 200 seconds
```

The following example displays CDP neighbors (brief):

```
switch# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID        Local Intrfce   Hldtme  Capability  Platform      Port ID
0                Gig4/1          135     H           DS-X9530-SF1- Gig4/1
069038732(Kiowa2 mgmt0           132     T S         WS-C5500      8/11
069038747(Kiowa3 mgmt0           156     T S         WS-C5500      6/20
069038747(Kiowa3 mgmt0           158     T S         WS-C5500      5/22
```

The following example displays CDP neighbors (detail):

```
switch# show CDP neighbor detail
----------------------------------------
Device ID:Switch
System Name:
Interface address(es):
Platform: cisco WS-C2950T-24, Capabilities: Switch IGMP Filtering
Interface: mgmt0, Port ID (outgoing port): FastEthernet0/24
Holdtime: 137 sec

Version:
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(19)EA1c, RELEASE SOFTWARE
 (fc2)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Mon 02-Feb-04 23:29 by yenanh

Advertisement Version: 2
Native VLAN: 1
Duplex: full
```

The following example displays the specified CDP neighbor (detail):

```
switch# show CDP neighbors interface gigabitethernet 4/1 detail
----------------------------------------
Device ID:0
Entry address(es):
    IP Address: 209.165.200.226
Platform: DS-X9530-SF1-K9, Capabilities: Host
Interface: GigabitEthernet4/1, Port ID (outgoing port): GigabitEthernet4/1
Holdtime: 144 sec
Version:
1.1(0.144)
Advertisement Version: 2
Duplex: full
```

The following example displays CDP traffic statistics for the management interface:

```
switch# show cdp traffic interface mgmt 0
```

```
----------------------------------------
Traffic statistics for mgmt0
Input Statistics:
    Total Packets: 1148
    Valid CDP Packets: 1148
        CDP v1 Packets: 1148
        CDP v2 Packets: 0
    Invalid CDP Packets: 0
        Unsupported Version: 0
        Checksum Errors: 0
        Malformed Packets: 0
Output Statistics:
    Total Packets: 2329
        CDP v1 Packets: 1164
        CDP v2 Packets: 1165
    Send Errors: 0
```

The following example displays CDP traffic statistics for the Gigabit Ethernet interface:

```
switch# show cdp traffic interface gigabitethernet 4/1
----------------------------------------
Traffic statistics for GigabitEthernet4/1
Input Statistics:
    Total Packets: 674
    Valid CDP Packets: 674
        CDP v1 Packets: 0
        CDP v2 Packets: 674
    Invalid CDP Packets: 0
        Unsupported Version: 0
        Checksum Errors: 0
        Malformed Packets: 0
Output Statistics:
    Total Packets: 674
        CDP v1 Packets: 0
        CDP v2 Packets: 674
    Send Errors: 0
```

show cfs

To display Cisco Fabric Services (CFS) information, use the **show cfs** command.

show cfs {**application** [**name** *app-name*]|**lock** [**name** *app-name*]|**merge status** [**name** *app-name*]|**peers** [**name** *app-name*]|**status** [**name** *app-name*]}

Syntax Description

application	Displays locally registered applications.
name *app-name*	(Optional) Specifies a local application information by name. Maximum length is 64 characters.
lock	Displays the state of application logical or physical locks.
merge status	(Optional) Displays CFS merge information.
peers	Displays logical or physical CFS peers.
status	Displays if CFS distribution is enabled or disabled. Enabled is the default configuration.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(1b)	This command was introduced.
2.1(1a)	• Added **status** keyword. • Replaced vsan with fctimer for the fctimer application in the Application field in the command output.
3.0(1)	Modified the **show cfs application** example with output that shows which applications support CFS distribution over IP and Fibre Channel and those that support only CFS distribution over Fibre Channel.

Usage Guidelines

None.

Note As soon as the customer encounters the syslog " %VSHD_4_VSHD_ROLE_DATABASE_OUT_OF _SYNC", Role configuration database is found to be different between the switches during merge. Role configuration database is recommended to be identical among all switches in the fabric. Edit the configuration on one of the switches to obtain the desire role configuration database and then commit it. For more information, Refer to the System Messages Guide.

Examples

The following example shows how to display CFS physical peer information for all applications:

```
switch# show cfs peers
Physical Fabric
-------------------------------------------------
 Switch WWN               IP Address
-------------------------------------------------
 20:00:00:05:30:00:61:de 209.165.200.226 [Local]
 20:00:00:0d:ec:08:66:c0 209.165.200.226
 20:00:00:05:30:00:f1:e2 209.165.200.226
 20:00:00:05:30:00:eb:46 209.165.200.226
 20:00:00:05:30:00:cb:56 209.165.200.227
20:00:00:05:30:00:5b:5e 209.165.200.228
 20:00:00:05:30:00:34:9e 209.165.200.229
Total number of entries = 7
```

The following example shows how to display CFS information for all applications on the switch:

```
switch# show cfs application
-----------------------------------------------
 Application    Enabled   Scope
-----------------------------------------------
ntp            No        Physical-all
fscm           Yes       Physical-fc
role           No        Physical-all
rscn           No        Logical
radius         No        Physical-all
fctimer        No        Physical-fc
syslogd        No        Physical-all
callhome       No        Physical-all
fcdomain       Yes       Logical
device-alias   Yes       Physical-fc
Total number of entries = 10
```

Note The **show cfs application** command displays only those applications that are registered with CFS. Conditional services that use CFS do not appear in the output unless those services are running.

The following example shows how to display CFS information for the device alias application:

```
switch# show cfs application name device-alias
 Enabled        : Yes
 Timeout        : 5s
 Merge Capable  : Yes
 Scope          : Physical
```

The following example shows how to display CFS merge operation information for the device alias application:

```
switch# show cfs merge status device-alias
Physical  Merge Status: Success
 Local Fabric
------------------------------------------------------------
 Switch WWN               IP Address
------------------------------------------------------------
 20:00:00:05:30:00:34:9e 209.165.200.226 [Merge Master]
 20:00:00:05:30:00:5b:5e 209.165.200.227
 20:00:00:05:30:00:61:de 209.165.200.228
 20:00:00:05:30:00:cb:56 209.165.200.229
 20:00:00:05:30:00:eb:46 209.165.200.230
 20:00:00:05:30:00:f1:e2 209.165.200.231
```

The following example shows whether or not CFS distribution is enabled:

```
switch# show cfs status

Fabric distribution Enabled
switch#
```

show cfs regions

To display the list of distribution-enabled applications with peers in a region, use the show cfs region command.

show cfs regions [{**brief [region-id]**|**name** [**name app-name**]|**region [region-id]**}]

Syntax Description

brief *region-id*	(Optional) Displays all configured regions and applications without peers.
name name *app-name*	(Optional) Displays all peers and region information for a given application.
region *region-id*	(Optional) Displays all configured applications with peers.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows all the region information with peers:

```
switch# show cfs regions
Region-ID  : 1
Application: callhome
Scope      : Physical-all
--------------------------------------------------------------------------
 Switch WWN              IP Address
--------------------------------------------------------------------------
 20:00:00:0d:ec:04:99:c0 209.165.200.226 [Local]
                         switch-
 20:00:00:0d:ec:04:99:c1 209.165.200.226
                         switch-2.cisco.com
 20:00:00:0d:ec:04:99:c2 209.165.200.226
                         switch-3.cisco.com
Total number of entries = 3
Region-ID  : 1
Application: ntp
Scope      : Physical-all
--------------------------------------------------------------------------
 Switch WWN              IP Address
--------------------------------------------------------------------------
 20:00:00:0d:ec:06:55:c0 209.165.200.226 [Local]
                         switch-1
Total number of entries = 1
```

The following example shows the list of applications without peers in a region:

```
switch# show cfs regions brief
--------------------------------------
```

```
 Region         Application   Enabled
--------------------------------------
   1            callhome      yes
   1            ntp           yes
```

The following example shows the peer and region information for a given application in a region:

```
switch# show cfs regions name callhome
Region-ID  : 1
Application: callhome
Scope      : Physical-all
--------------------------------------------------------------------------------
 Switch WWN              IP Address
--------------------------------------------------------------------------------
 20:00:00:0d:ec:06:55:c0 209.165.200.226 [Local]
                         switch 1
Total number of entries = 1
```

Related Commands

Command	Description
cfs regions	Creates a region that restricts the scope of application distribution to a selected switch.

show cfs static peers

To display all the configured static peers with status, use the show cfs static peers command.

show cfs static peers

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the CFS static peers:

```
-------------------------------------------------------------------------------
 IP address                      WWN name                 Status
-------------------------------------------------------------------------------
 1.2.3.4              00:00:00:00:00:00:00:00          Un Reachable
 1.2.3.5              00:00:00:00:00:00:00:00          Un Reachable
 10.64.66.47          20:00:00:0d:ec:06:55:c0          Reachable
 10.64.66.56          20:00:08:00:88:04:99:80          Local
Total number of entries = 4
```

Related Commands

Command	Description
cfs static peers	Displays configured static peers with status.

show cfs status

To display the Cisco Fabric Services (CFS) status, use the show cfs region command.

show cfs status

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the CFS status:

```
switch# show cfs status
Distribution: Enabled
Distribution over IP: Enabled (static)
IPv4 multicast address : 239.255.70.83
IPv6 multicast address : ff15::efff:4563
```

Related Commands

Command	Description
cfs enable	Starts CFS.

show cimserver

To display the Common Information Model (CIM) configurations and settings, use the **show cimserver** command.

show cimserver [{**certificateName**|**HttpsStatus**|**HttpStatus**|**status**}]

Syntax Description

certificateName	(Optional) Displays the installed Secure Socket Layer (SSL) certificate.
HttpsStatus	(Optional) Displays the HTTPS (secure) protocol settings for the CIM server.
HttpStatus	(Optional) Displays the HTTP (non-secure) protocol for the CIM server.
status	(Optional) Displays the CIM server status.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
5.2(1)	This command was deprecated.

Usage Guidelines

None.

Examples

The following example displays CIM server certificate files:

```
switch# show cimserver certificateName
cimserver certificate file name is servcert.pem
```

The following example displays the CIM server configuration:

```
switch# show cimserver
 cimserver is enabled
 cimserver Http is not enabled
 cimserver Https is enabled
 cimserver certificate file name is servcert.pem
```

The following example displays the CIM server HTTPS status:

```
switch# show cimserver httpsstatus
 cimserver Https is enabled
```

The following example displays the CIM server HTTP status:

```
switch# show cimserver httpstatus
 cimserver Http is not enabled
```

show cimserver indications

To display cimserver indications such as filters, recipients, and subscriptions, use the show cimserver indication command.

show cimserver indication

Syntax Description

This command has no arguments or keywords:

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
3.3(1a)	This command was introduced.
5.2(1)	This command was deprecated.

Usage Guidelines

None.

Examples

The following example displays the cimserver indications:

```
switch# show cimserver indication
Filter:           root/cimv2:Feb 7, 2008 2:32:11 PM
Query:            "SELECT * FROM CISCO_LinkUp"
Query Language:   WQL
----------------------------------------
Handler:           root/cimv2:CIM_ListenerDestinationCIMXML.Thu Feb 07 14:32:44 IST
20081202374964083
Destination:       http://10.77.91.110:59901
PersistenceType:   Transient
----------------------------------------
Namespace:         root/cimv2
Filter:            root/cimv2:Feb 7, 2008 2:32:11 PM
Handler:           root/cimv2:CIM_ListenerDestinationCIMXML.Thu Feb 07 14:32:44 IST
20081202374964083
Query:             "SELECT * FROM CISCO_LinkUp"
Destination:       http://10.77.91.110:59901
SubscriptionState: Enabled
The following example displays the cimserver's indication filters:
switch# show cimserver indication filters
Filter:           root/cimv2:Feb 7, 2008 2:32:11 PM
Query:            "SELECT * FROM CISCO_LinkUp"
Query Language:   WQL
The following example displays the cimserver's indication recipient:
switch# show cimserver indication recipients
Handler:           root/cimv2:CIM_ListenerDestinationCIMXML.Thu Feb 07 14:32:44 IST
20081202374964083
Destination:       http://10.77.91.110:59901
PersistenceType:   Transient
The following example displays the subscriptions on cimserver:
switch# show cimserver indication subscriptions
Namespace:         root/cimv2
```

```
Filter:            root/cimv2:Feb 7, 2008 2:32:11 PM
Handler:           root/cimv2:CIM_ListenerDestinationCIMXML.Thu Feb 07 14:32:44 IST
20081202374964083
Query:             "SELECT * FROM CISCO_LinkUp"
Destination:       http://10.77.91.110:59901
SubscriptionState: Enabled
```

show cimserver logs

To display the cimserver logs, use the show cimserver logs command.

show cimserver logs

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
3.3(1a)	This command was introduced.
5.2(1)	This command was deprecated.

Usage Guidelines

None.

Examples

The following example displays the cimserver logs:

```
switch# show cimserver logs
02/07/2008-16:38:14 INFO    cimserver: Sent response to: localhost
02/07/2008-16:38:26 INFO    cimserver: Received request from: 10.77.91.110
02/07/2008-16:38:27 INFO    cimserver: Sent response to: 10.77.91.110
```

Related Commands

Command	Description
cimserver loglevel	Enters cimsever log level filters.

show cimserver status

To display the cimserver status, use the show cimserver status command.

show cimserver status

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
3.3(1a)	This command was introduced.
5.2(1)	This command was deprecated.

Usage Guidelines

None.

Examples

The following example displays the cimserver status:

```
switch# show cimserver status
cimserver is enabled
```

Related Commands

Command	Description
cimserver enable	Starts the cimserver.

show cli alias

To display configured aliases on a switch, use the **show cli alias** command.

show cli alias [**name** *name*]

Syntax Description

name *name*	(Optional) Specifies an alias name. The maximum size of the name is 31 characters.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The **show cli alias** command shows the default alias and other user-defined aliases. The default alias is **alias**, which means **show cli alias**.

Examples

The following example displays CLI aliases:

```
switch# show cli alias
CLI alias commands
==================
alias  :show cli alias
env    :show environment
clock  :show clock
```

The following example displays a specific alias by name:

```
switch# show cli alias name qos
qos :show qos
```

Related Commands

Command	Description
cli alias name	Defines a command alias name.

show cli variables

To display user-defined session and persistent CLI variables, use the **show cli variables** command.

show cli variables

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The **show CLI variables** command shows all available CLI variables, including user-defined session CLI variables, user-defined persistent CLI variables, and system-defined CLI variables. There is no distinction between the types of CLI variables in the output.

Examples

The following example displays CLI variables:

```
switch# show cli variables
VSH Variable List
-----------------
TIMESTAMP="2005-10-24-21.29.33"
testinterface="fc 1/1"
```

Note The TIMESTAMP variable shown in the output in the preceding example is a predefined variable supported by Cisco MDS NX-OS. For more information about the TIMESTAMP variable, refer to the *Cisco MDS 9000 Family CLI Configuration Guide* .

Related Commands

Command	Description
cli var name	Defines a CLI session variable.
cli var name (configuration)	Defines a CLI persistent variable.

show clock

To display the system date and time and verify the time zone configuration, use the **show clock** command.

show clock

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the system date, time, and time zone configuration:

```
switch# show clock
Fri Mar 14 01:31:48 UTC 2003
```

show cloud discovery

To display discovery information about the cloud, use the **show cloud discovery** command.

show cloud discovery {**config**|**stats**|**status**}

Syntax Description

config	Displays global discovery configuration information.
stats	Displays discovery statistics information.
status	Displays discovery status information.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.
3.2(2c)	This command was deprecated.

Usage Guidelines

None.

Examples

The following example shows information about a cloud:

```
switch# show cloud discovery config
Auto discovery: Enabled
```

The following example shows statistics about a cloud:

```
switch# show cloud discovery stats
Global statistics
    Number of Auto Discovery                      = 4
    Number of Manual (demand) Discovery                     = 0
    Number of cloud discovery (ping) messages sent = 17
    Number of cloud discovery (ping) success       = 1
```

Related Commands

Command	Description
cloud discover	Initiates manual, on-demand cloud discovery.
cloud discovery	Configures cloud discovery.
cloud-discovery	Enables discovery of cloud memberships.
show cloud membership	Displays information about members of a cloud.

show cloud membership

To display membership information about the cloud, use the **show cloud membership** command.

show cloud membership [{**all**|**interface** {**gigabitethernet** *slot/port*|**port-channel** *number*}|**unresolved**}]

Syntax Description

all	(Optional) Displays all clouds and cloud members.
interface	(Optional) Displays all members of a cloud containing a specified interface.
gigabitethernet *slot/port*	Specifies a Gigabit Ethernet interface by slot and port number. The range is 1 to 6.
port-channel *number*	Specifies a PortChannel interface. The range is 1 to 128.
unresolved	(Optional) Displays unresolved members of the cloud.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.
3.2(2c)	This command was deprecated.

Usage Guidelines

None.

Examples

The following example displays the members of clouds:

```
switch# show cloud membershp
Undiscovered Cloud
    port-channel 1[20:00:00:05:30:00:a7:9e] IP Addr fe80::205:30ff:fe00:a412
    port-channel 1.250[20:00:00:05:30:00:a7:9e] IP Addr 3000:2::1
    port-channel 1.250[20:00:00:05:30:00:a7:9e] IP Addr fe80::205:30ff:fe00:a412
  #members=3
Cloud 2
    port-channel 1[20:00:00:05:30:00:a7:9e] IP Addr 3000:1::1
  #members=1
Cloud 3
    GigabitEthernet1/1[20:00:00:05:30:00:a7:9e] IP Addr 10.10.10.1
  #members=1
Cloud 4
    GigabitEthernet1/2[20:00:00:05:30:00:a7:9e] IP Addr 10.10.60.1
  #members=1
```

Related Commands

Command	Description
cloud discover	Initiates manual, on-demand cloud discovery.

Command	Description
cloud discovery	Configures cloud discovery.
cloud-discovery enable	Enables discovery of cloud memberships.
show cloud discovery	Displays discovery information about a cloud.

show copyright

To display the NX-OS software copyright statement, use the **show copyright** command in EXEC mode.

show copyright

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(2)	This command was introduced.
NX-OS 4.1(1b)	Changed the command output from SAN-OS to NX-OS.

Usage Guidelines

Use the **show copyright** command to verify the copyright statement of the current NX-OS image.

Examples

The following example displays copyright information for NX-OS software:

```
switch# show copyright
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2008, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch#
```

show cores

To display all the cores presently available for uploading from the active supervisor, use the **show cores** command.

show cores

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

In the following example, an FSPF core was generated on the active supervisor (slot 5), an FCC core on the standby supervisor (slot 6) and acltcam and FIB on module (slot 8):

```
switch# show cores
Module-num     Process-name       PID     Core-create-time
----------     ------------       ---     ----------------
5               fspf             1524     Jan 9 03:11
6               fcc               919     Jan 9 03:09
8               acltcam           285     Jan 9 03:09
8               fib               283     Jan 9 03:08
```

show crypto ca certificates

To display configured trust point certificates, use the **show crypto ca certificates** command.

show crypto ca certificates *trustpoint-label*

Syntax Description

trustpoint-label	Specifies the name of the trust point. The maximum size is 64 characters.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command displays the important fields in the identity certificate, if present, followed by those in the CA certificate (or each CA certificate if it is a chain, starting from the lowest to the self-signed root certificate), or the trust point. If the trust point name is not specified, all trust point certificate details are displayed.

Examples

The following example displays configured trust point certificates:

```
switch# show crypto ca certificates
Trustpoint: admin-ca
certificate:
subject= /CN=switch160
issuer= /C=US/O=cisco/CN=Aparna CA2
serial=6CDB2D9E000100000006
notBefore=Jun  9 10:51:45 2005 GMT
notAfter=May  3 23:10:36 2006 GMT
MD5 Fingerprint=0A:22:DC:A3:07:2A:9F:9A:C2:2C:BA:96:EC:D8:0A:95
purposes: sslserver sslclient ike
CA certificate 0:
subject= /C=US/O=cisco/CN=Aparna CA2
issuer= /emailAddress=amandke@cisco.com/C=IN/ST=Maharashtra/L=Pune/O=cisco/OU=ne
tstorage/CN=Aparna CA1
serial=14A3A877000000000005
notBefore=May  5 18:43:36 2005 GMT
notAfter=May  3 23:10:36 2006 GMT
MD5 Fingerprint=32:50:26:9B:16:B1:40:A5:D0:09:53:0A:98:6C:14:CC
purposes: sslserver sslclient ike
CA certificate 1:
subject= /emailAddress=amandke@cisco.com/C=IN/ST=Maharashtra/L=Pune/O=cisco/OU=n
etstorage/CN=Aparna CA1
issuer= /emailAddress=amandke@cisco.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/OU
=netstorage/CN=Aparna CA
serial=611B09A1000000000002
notBefore=May  3 23:00:36 2005 GMT
notAfter=May  3 23:10:36 2006 GMT
MD5 Fingerprint=65:CE:DA:75:0A:AD:B2:ED:69:93:EF:5B:58:D4:E7:AD
purposes: sslserver sslclient ike
CA certificate 2:
subject= /emailAddress=amandke@cisco.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/O
```

```
U=netstorage/CN=Aparna CA
issuer= /emailAddress=amandke@cisco.com/C=IN/ST=Karnataka/L=Bangalore/O=Cisco/OU
=netstorage/CN=Aparna CA
serial=0560D289ACB419944F4912258CAD197A
notBefore=May  3 22:46:37 2005 GMT
notAfter=May  3 22:55:17 2007 GMT
MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
purposes: sslserver sslclient ike
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the certificate of the CA.
show ca trustpoints	Displays trust point configurations.

show crypto ca crl

To display configured certificate revocation lists (CRLs), use the **show crypto ca crl** command.

show crypto ca crl trustpoint-label

Syntax Description

trustpoint-label	Specifies the name of the trust point. The maximum size is 64 characters.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command lists serial numbers of revoked certificates in the CRL of the specified trust point.

Examples

The following example displays a configured CRL:

```
switch# show crypto ca crl admin-ca
Trustpoint: admin-ca
CRL:
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: /emailAddress=rviyyoka@cisco.com/C=IN/ST=Kar/L=Bangalore/O=Cisco
 Systems/OU=1/CN=cisco-blr
        Last Update: Sep 22 07:05:23 2005 GMT
        Next Update: Sep 29 19:25:23 2005 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
            keyid:CF:72:E1:FE:14:60:14:6E:B0:FA:8D:87:18:6B:E8:5F:70:69:05:3F
            1.3.6.1.4.1.311.21.1:
                ...
Revoked Certificates:
    Serial Number: 1E0AE838000000000002
        Revocation Date: Mar 15 09:12:36 2005 GMT
    Serial Number: 1E0AE9AB000000000003
        Revocation Date: Mar 15 09:12:45 2005 GMT
    Serial Number: 1E721E50000000000004
        Revocation Date: Apr  5 11:04:20 2005 GMT
    Serial Number: 3D26E445000000000005
        Revocation Date: Apr  5 11:04:16 2005 GMT
    Serial Number: 3D28F8DF000000000006
        Revocation Date: Apr  5 11:04:12 2005 GMT
    Serial Number: 3D2C6EF3000000000007
        Revocation Date: Apr  5 11:04:09 2005 GMT
    Serial Number: 3D4D7DDC000000000008
        Revocation Date: Apr  5 11:04:05 2005 GMT
    Serial Number: 5BF1FE87000000000009
        Revocation Date: Apr  5 11:04:01 2005 GMT
    Serial Number: 5BF22FB300000000000A
```

```
    Revocation Date: Apr  5 11:03:45 2005 GMT
Serial Number: 5BFA4A4900000000000B
    Revocation Date: Apr  5 11:03:42 2005 GMT
Serial Number: 5C0BC225000000000000C
    Revocation Date: Apr  5 11:03:39 2005 GMT
Serial Number: 5C0DA95E000000000000D
    Revocation Date: Apr  5 11:03:35 2005 GMT
Serial Number: 5C137769000000000000E
    Revocation Date: Apr  5 11:03:31 2005 GMT
Serial Number: 4864FD5A000000000000F
    Revocation Date: Apr  5 11:03:28 2005 GMT
Serial Number: 48642E2E000000000010
    Revocation Date: Apr  5 11:03:24 2005 GMT
Serial Number: 486D4230000000000011
    Revocation Date: Apr  5 11:03:20 2005 GMT
Serial Number: 7FCB75B9000000000012
    Revocation Date: Apr  5 10:39:12 2005 GMT
Serial Number: 1A7519000000000013
    Revocation Date: Apr  5 10:38:52 2005 GMT
Serial Number: 20F1B0000000000014
    Revocation Date: Apr  5 10:38:38 2005 GMT
Serial Number: 436E43A90000000000023
    Revocation Date: Sep  9 09:01:23 2005 GMT
    CRL entry extensions:
        X509v3 CRL Reason Code:
        Cessation Of Operation
Serial Number: 152D3C5E000000000047
    Revocation Date: Sep 22 07:12:41 2005 GMT
Serial Number: 1533AD7F000000000048
    Revocation Date: Sep 22 07:13:11 2005 GMT
Serial Number: 1F9EB8EA00000000006D
    Revocation Date: Jul 19 09:58:45 2005 GMT
    CRL entry extensions:
        X509v3 CRL Reason Code:
        Cessation Of Operation
Serial Number: 1FCA9DC600000000006E
    Revocation Date: Jul 19 10:17:34 2005 GMT
    CRL entry extensions:
        X509v3 CRL Reason Code:
        Cessation Of Operation
Serial Number: 2F1B5E2E000000000072
    Revocation Date: Jul 22 09:41:21 2005 GMT
    CRL entry extensions:
        X509v3 CRL Reason Code:
        Cessation Of Operation
Signature Algorithm: sha1WithRSAEncryption
    4e:3b:4e:7a:55:6b:f2:ec:72:29:70:16:2a:fd:d9:9a:9b:12:
    f9:cd:dd:20:cc:e0:89:30:3b:4f:00:4b:88:03:2d:80:4e:22:
    9f:46:a5:41:25:f4:a5:26:b7:b6:db:27:a9:64:67:b9:c0:88:
    30:37:cf:74:57:7a:45:5f:5e:d0
```

Related Commands

Command	Description
crypto ca crl request	Configures a CRL or overwrites the existing one for the trust point CA.

show crypto ca remote-certstore

To display configured remote certstores, use the show crypto ca remote-certstore command.

show crypto ca remote certstore

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command Default

None.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Note In the current 5.0 release only ssh-client will use remote certstore. Other applications like ike, callhome will continue using local certstore irrespective of the configurations.

Examples

The following example shows how to display configured remote certstores:

```
switch# show crypto ca remote-certstore
Remote Certstore:LDAP
CRL Timer : 10 Hours
LDAP Server group : Ldap1
switch#
```

Related Commands

Command	Description
crypto certificatemap mapname	Specifies the certificate map that will be used for filtering the certificate request.

show crypto ca trustpoints

To display trust point configurations, use the **show crypto ca trustpoints** command.

show crypto ca trustpoints

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays configured trust points:

```
switch# show crypto ca trustpoints
trustpoint: CAname; key:
revokation methods:  crl
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the certificate of the CA.
crypto ca trustpoint	Declares the trust point certificate authority that the switch should trust.
show crypto ca certificates	Displays configured trust point certificates.

show crypto certificatemap

To display certificatemap filters, use the show crypto certificatemap command.

show crypto certificatemap

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command Default

None.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display certificatemap filters:

```
switch# show crypto certificatemap
Map Name: map1
Subject name: /DCBU
Altname Email: koukumar@cisco.com
Altname UPN:
switch#
```

Related Commands

Command	Description
crypto certificatemap mapname	Specifies the certificate map that will be used for filtering the certificate request.

show crypto global domain ipsec

To display global IPsec crypto map set information, use the **show crypto global domain ipsec** command.

show crypto global domain ipsec [{**interface gigabitethernet** *slot*/*port*|**security-association lifetime**}]

Syntax Description

interface gigabitethernet *slot/port*	(Optional) Displays crypto IPsec domain information for the specified Gigabit Ethernet interface slot and port.
security-association lifetime	(Optional) Displays crypto IPsec domain security association lifetime parameters.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(x)	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 display crypto global domain IPsec statistics:

```
switch# show crypto global domain ipsec
IPSec global statistics:
        Number of crypto map sets: 2
```

The following example shows how to display crypto global domain IPsec statistics for an interface:

```
switch# show crypto global domain ipsec interface gigabitethernet 1/2
IPSec interface statistics:
        IKE transaction stats: 0 num
        Inbound SA stats: 0 num, 512 max
        Outbound SA stats: 0 num, 512 max
```

The following example shows how to display crypto global domain IPsec security association lifetime parameters:

```
switch# show crypto global domain ipsec security-association lifetime
Security Association Lifetime: 4500 megabytes/3600 seconds
```

Related Commands

Command	Description
crypto global domain ipsec security-association lifetime	Configures global attributes for IPsec.
crypto ipsec enable	Enables IPsec.

show crypto ike domain ipsec

To display IKE protocol information, use the **show crypto ike domain ipsec** command.

show crypto ike domain ipsec [{**initiator** [**address** *ip-address*]|**keepalive**|**key** [**address** *ip-address*]|**policy** [*policy-number*]|**sa**}]

Syntax Description

initiator	(Optional) Displays initiator configuration information.
address *ip-address*	Specifies the initiator peer IP address.
keepalive	(Optional) Displays keepalive for the IKE protocol in seconds
key	(Optional) Displays pre-shared authentication keys.
policy *policy-number*	Displays IKE configuration policies for IPsec. The range is 1 to 255.
sa	(Optional) Displays IKE Security Associations for IPsec.

Command Default

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, the IKE protocol must be enabled using the **crypto ike enable** command.

Examples

The following example shows how to display IKE keepalive value configuration information:

```
switch# show crypto ike domain ipsec keepalive
keepalive 3600
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.

show crypto key mypubkey rsa

To display any RSA public key configurations, use the **show crypto key mypubkey rsa** command.

show crypto key mypubkey rsa

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays RSA public key configurations:

```
switch# show crypto key mupubkey rsa
key label: myrsa
key size: 512
exportable: yes
```

Related Commands

Command	Description
crypto ca enroll	Requests certificates for the switch's RSA key pair.
crypto key generate rsa	Generates an RSA key pair.
rsakeypair	Configures trust point RSA key pair details

show crypto map domain ipsec

To map configuration information for IPsec, use the **show crypto map domain ipsec** command.

`show crypto map domain ipsec [{interface gigabitethernet` *slot* `/` *port*`|tag` *tag-name*`}]`

Syntax Description

interface gigabitethernet *slot*/*port*	(Optional) Displays IPsec map information for a specific Gigabit Ethernet interface.
tag *tag-name*	(Optional) Displays IPsec map information for a specific tag name. The maximum length is 63 characters.

Command Default

Displays all IPsec map information.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(x)	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 display IPsec crypto map information:

```
switch# show crypto map domain ipsec
Crypto Map "cm10" 1 ipsec
        Peer = 10.10.10.4
        IP ACL = aclmds10
            permit ip 10.10.10.1 255.255.255.255 10.10.10.4 255.255.255.255
        Transform-sets: 3des-md5, 3des-sha, des-md5, des-sha,
        Security Association Lifetime: 450 gigabytes/3600 seconds
        PFS (Y/N): N
Crypto Map "cm10" 2 ipsec
        Peer = Auto Peer
        IP ACL = acl10
            permit ip 10.10.10.0 255.255.255.0 10.10.10.0 255.255.255.0
        Transform-sets: 3des-md5, 3des-sha, des-md5, des-sha,
        Security Association Lifetime: 450 gigabytes/3600 seconds
        PFS (Y/N): N
Crypto Map "cm11" 1 ipsec
        Peer = 10.10.11.2
        IP ACL = aclany
            permit ip any any
        Transform-sets: 3des-md5, 3des-sha, des-md5, des-sha,
        Security Association Lifetime: 450 gigabytes/3600 seconds
        PFS (Y/N): N
Crypto Map "cm50" 1 ipsec
        Peer = 10.10.50.2
        IP ACL = aclany
            permit ip any any
        Transform-sets: 3des-md5,
```

```
        Security Association Lifetime: 450 gigabytes/3600 seconds
        PFS (Y/N): N
Interface using crypto map set cm50:
    GigabitEthernet1/2.1
Crypto Map "cm51" 1 ipsec
        Peer = 10.10.51.2
        IP ACL = aclany
            permit ip any any
        Transform-sets: 3des-md5,
        Security Association Lifetime: 450 gigabytes/3600 seconds
        PFS (Y/N): N
Interface using crypto map set cm51:
    GigabitEthernet1/2.2
Crypto Map "cm60" 1 ipsec
        Peer = 10.10.60.2
        IP ACL = acl60
            permit ip 10.10.60.0 255.255.255.0 10.10.60.0 255.255.255.0
        Transform-sets: 3des-md5,
        Security Association Lifetime: 450 gigabytes/3600 seconds
        PFS (Y/N): N
Interface using crypto map set cm60:
    GigabitEthernet1/2
Crypto Map "cm100" 1 ipsec
        Peer = 10.10.100.221
        IP ACL = aclmds100
            permit ip 10.10.100.231 255.255.255.255 10.10.100.221 255.255.255.255
        Transform-sets: 3des-md5, 3des-sha, des-md5, des-sha,
        Security Association Lifetime: 450 gigabytes/3600 seconds
        PFS (Y/N): N
Crypto Map "cm100" 2 ipsec
        Peer = Auto Peer
        IP ACL = acl100
            permit ip 10.10.100.0 255.255.255.0 10.10.100.0 255.255.255.0
        Transform-sets: 3des-md5, 3des-sha, des-md5, des-sha,
        Security Association Lifetime: 450 gigabytes/3600 seconds
        PFS (Y/N): N
```

Related Commands

Command	Description
crypto ipsec enable	Enables IPsec.
crypto map domain ipsec	Enters IPsec map configuration mode.

show crypto sad domain ipsec

To display IPsec security association database information, use the **show crypto sad domain ipsec** command.

show crypto sad domain ipsec [**interface gigabitethernet** *slot* / *port* [{**inbound**|**outbound**} **sa-index** *index*]]

Syntax Description

interface gigabitethernet *slot*/*port*	(Optional) Displays IPsec security association information for a specific Gigabit Ethernet interface.
inbound	(Optional) Specifies the inbound association.
outbound	(Optional) Specifies the outbound association.
sa-index *index*	(Optional) Specifies the security association index. The range is 0 to 2147483647.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(x)	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 display IPsec security association information:

```
switch# show crypto sad domain ipsec
interface: GigabitEthernet4/1
    Crypto map tag: cm10, local addr. 10.10.10.1
    protected network:
    local ident (addr/mask): (10.10.10.0/255.255.255.0)
    remote ident (addr/mask): (10.10.10.4/255.255.255.255)
    current_peer: 10.10.10.4
      local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.4
      mode: tunnel, crypto algo: esp-3des, auth algo: esp-md5-hmac
    current outbound spi: 0x30e000f (51249167), index: 0
      lifetimes in seconds:: 120
      lifetimes in bytes:: 423624704
    current inbound spi: 0x30e0000 (51249152), index: 0
      lifetimes in seconds:: 120
      lifetimes in bytes:: 423624704
```

Related Commands

Command	Description
crypto ipsec enable	Enables IPsec.

show crypto spd domain ipsec

To display the security policy database (SPD), use the **show crypto spd domain ipsec** command.

`show crypto spd domain ipsec [interface gigabitethernet` *slot* `/` *port* `[policy` *number*`]]`

Syntax Description

interface gigabitethernet *slot*/*port*	(Optional) Displays SPD information for a specific Gigabit Ethernet interface.
policy *number*	(Optional) Specifies a SPD policy number.

Command Default

Displays all SPD information.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(x)	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 display the SPD:

```
switch# show crypto spd domain ipsec
Policy Database for interface: GigabitEthernet1/1, direction: Both
#   0:      deny  udp any port eq 500 any
#   1:      deny  udp any any port eq 500
#   2:      permit ip any any
#  63:      deny  ip any any
Policy Database for interface: GigabitEthernet1/2, direction: Both
#   0:      deny  udp any port eq 500 any
#   1:      deny  udp any any port eq 500
#   3:      permit ip 10.10.50.1 255.255.255.255 10.10.50.2 255.255.255.255
#   4:      permit ip 10.10.51.1 255.255.255.255 10.10.51.2 255.255.255.255
#  63:      deny  ip any any
```

Related Commands

Command	Description
crypto ipsec enable	Enables IPsec.

show crypto ssh-auth-map

To display mapping filters applied for SSH authentication, use the show crypto ssh-auth-map command.

show crypto ssh-auth-map

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command Default

None.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display mapping filters applied for SSH authentication:

```
switch# show crypto ssh-auth-map
Issuer Name: /DCBU
Map1: map1
Map2: map2
switch#
```

Related Commands

Command	Description
crypto certificatemap mapname	Specifies the certificate map that will be used for filtering the certificate request.

show crypto transform-set domain ipsec

To display transform set information for IPsec, use the **show crypto transform-set domain ipsec** command.

show crypto transform-set domain ipsec [*set-name*]

Syntax Description

set-name	(Optional) Specifies the transform set name. Maximum length is 63 characters.

Command Default

Displays information for all transform sets.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(x)	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 display information for all IPsec transform sets:

```
switch# show crypto transform-set domain ipsec
Transform set: ipsec_default_transform_set {esp-aes-256-ctr esp-aes-xcbc-mac}
    will negotiate {tunnel}
```

Related Commands

Command	Description
crypto ipsec enable	Enables IPsec.
crypto transform-set domain ipsec	Configures IPsec transform set information.

show debug

To display all Cisco SME related debug commands configured on the switch, use the show debug command.

show debug {**cluster** {**bypass**|**sap sap bypass**}|**sme bypass**}

Syntax Description

cluster	Displays all the debugging flags.
bypass	Displays the bypass flags.
sap sap	Displays all debugging flags of SAP. Specifies the SAP in the range from 1 to 65535.
sme	Displays all the debugging flags of Cisco SME.
bypass	Displays all the bypass flags of Cisco SME.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(2c)	This command was introduced.
NX-OS 4.1(1c)	Added the syntax description.

Usage Guidelines

None.

Examples

The following example shows all debug commands configured on the switch:

```
switch# show debug
ILC helper:
 ILC_HELPER errors debugging is on
 ILC_HELPER info debugging is on
```

Related Commands

Commands	Description
debug sme	Debugs Cisco SME features.

show debug logfile

To display the debug messages that are saved in the debug log file, use the **show debug logfile** command.

show debug logfile filename

Syntax Description

filename	Specifies the debug log file name. Maximum length is 80 characters.

Command Default

None.

Command Modes

EXEC mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.0(2).

Usage Guidelines

None.

Examples

The following example displays the debug messages in the specified debug log file.

```
switch# show debug logfile SampleFile
2004 Jun 28 00:14:17 snmpd[2463]: header_fspfLinkEntry : Sending GETNEXT request
 for fspfLsrTable for vsanIndex  =0,fspfLsrDomainId = 0, fspfLsrType = 0
2004 Jun 28 00:14:17 snmpd[2463]: header_fspfLinkEntry : Sending GETNEXT request
 for fspfLsrTable for vsanIndex  =0,fspfLsrDomainId = 0, fspfLsrType = 0
2004 Jun 28 00:14:17 snmpd[2463]: header_fspfLinkEntry : Recd rsp for GETNEXT fo
r entry (vsanIndex=1,fspfLsrDomainId = 10, fspfLsrType=0, fspfLinkIndex = 1,fspf
LinkNbrDomainId = 84, fspfLinkPortIndex = 67331,fspfLinkNbrPortIndex = 66064, fs
pfLinkType = 1,fspfLinkCost = 500
2004 Jun 28 00:14:17 snmpd[2463]: header_fspfLinkEntry : Sending GETNEXT request
 for fspfLsrTable for vsanIndex  =1,fspfLsrDomainId = 209, fspfLsrType = 0
2004 Jun 28 00:14:17 snmpd[2463]: header_fspfLinkEntry : Sending GETNEXT request
 for fspfLsrTable for vsanIndex  =16777216,fspfLsrDomainId = 3506438144, fspfLsr
Type = 0
2004 Jun 28 00:14:17 snmpd[2463]: header_fspfLinkEntry : Sending GETNEXT request
 for fspfLsrTable for vsanIndex  =33554432,fspfLsrDomainId = 4009754624, fspfLsr
Type = 16777216
```

show debug npv

To display the N Port Virtualization (NPV) debug commands configured on the switch, use the show debug npv command.

show debug npv

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows all NPV debug commands configured on the switch:

```
switch# show debug npv
N_port Virtualizer:
 FC Receive Packets debugging is on
 FC Transmit Packets debugging is on
 FC Receive Packet header debugging is on
 FC Transmit Packet header debugging is on
 MTS Receive Packets debugging is on
 MTS Transmit Packets debugging is on
 MTS Receive Packet header/payload debugging is on
 MTS Transmit Packet header/payload debugging is on
 High Availability debugging is on
 FSM Transitions debugging is on
 Error debugging is on
 Warning debugging is on
 Trace debugging is on
 Trace Detail debugging is on
 Demux debugging is on
 Dequeue debugging is on
 Packets debugging is on
 Database debugging is on
 Timers debugging is on
 External Interface FSM Events debugging is on
 External Interface FSM Errors debugging is on
 External Interface FSM Trace debugging is on
 FLOGI FSM Events debugging is on
 FLOGI FSM Errors debugging is on
 FLOGI FSM Trace debugging is on
 Server Interface FSM Events debugging is on
 Server Interface FSM Errors debugging is on
 Server Interface FSM Trace debugging is on
 Events debugging is on
```

Related Commands

Command	Description
debug npv	Enables debugging NPV configurations.

show debug sme

To display all Cisco SME related debug commands configured on the switch, use the show debug command.

show debug {**cluster** {**bypass**|**sap sap**}|**sme bypass**}

Syntax Description

cluster	Displays all the debugging flags.
bypass	Displays the bypass flags.
sap sap	Displays all debugging flags of SAP. Specifies the SAP in the range from 1 to 65535.
sme	Displays all the debugging flags of Cisco SME.
bypass	Displays all the bypass flags of Cisco SME.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows all debug commands configured on the switch:

```
switch# show debug
ILC helper:
 ILC_HELPER errors debugging is on
 ILC_HELPER info debugging is on
```

Related Commands

Commands	Description
debug sme	Debugs Cisco SME features.

show device-alias

To display the device name information, use the **show device-alias** command.

show device-alias {**database** [{**pending**|**pending-diff**}]|**name** *device-name* **[pending]**|**pwwn** *pwwn-id* **[pending]**|**session** {**rejected**|**status**}|**statistics**|**status**}

Syntax Description

database	Displays the entire device name database.
pending	(Optional) Displays the pending device name database information.
pending-diff	(Optional) Displays pending differences in the device name database information.
name *device-name*	Displays device name database information for a specific device name.
pwwn *pwwn-id*	Displays device name database information for a specific pWWN. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
session	Displays the session information.
rejected	Display the rejected command list.
status	Displays the device-alias session status.
statistics	Displays device name database statistics.
status	Displays the device name database status.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(9)	Added the rejected keyword to the syntax description.
2.0(x)	This command was introduced.

Usage Guidelines

To make use of fcaliases as device names instead of using the cryptic device name, add only one member per fcalias.

The device-alias configuration best practice has been described in the configuration guide.

Examples

The following example shows the set of rejected device-alias commands in a session:

```
switch(config-device-alias-db)# show device-alias session rejected
To avoid command rejections, within a device alias session
Do not reuse:
a) a device alias name while configuring a rename command
b) a PWWN while configuring an add or delete command
```

```
c) a device alias name already renamed while configuring add command
Rejected commands must be committed in a separate device alias session
which may cause traffic interruption for those devices. Plan accordingly.
Refer to this command in the NX-OS Command Reference Guide
for more information about device alias configuration best practices


Rejected Command List
---------------------
device-alias name Dev1 pwwn 01:01:01:01:02:02:02:02
device-alias name Dev20 pwwn 01:01:01:01:02:02:02:02
switch(config-device-alias-db)#
```

The following examples shows the device-alias session status:

```
switch(config)# show device-alias session status
Last Action Time Stamp     : Tue Jul  1 01:54:21 2014
Last Action                : Commit
Last Action Result         : Success
Last Action Failure Reason : none
switch(config)#
```

The following example shows how to display the contents of the device alias database:

```
switch# show device-alias database
device-alias name efg pwwn 21:00:00:20:37:9c:48:e5
device-alias name fred pwwn 10:00:00:00:c9:2d:5a:de
device-alias name myalias pwwn 21:21:21:21:21:21:21:21
device-alias name test pwwn 21:00:00:20:37:6f:db:bb
device-alias name test2 pwwn 21:00:00:20:37:a6:be:35
Total number of entries = 5
```

The following example shows how to display all global fcaliases and all VSAN dependent fcaliases:

```
switch# show device-alias name efg
device-alias name efg pwwn 21:00:00:20:37:9c:48:e5
```

The following example shows how to display all global fcaliases and all VSAN dependent fcaliases:

```
switch# show device-alias statistics
        Device Alias Statistics
========================================
Lock requests sent: 1
Database update requests sent: 1
Unlock requests sent: 1
Lock requests received: 0
Database update requests received: 0
Unlock requests received: 0
Lock rejects sent: 0
Database update rejects sent: 0
Unlock rejects sent: 0
Lock rejects received: 0
Database update rejects received: 0
Unlock rejects received: 0
Merge requests received: 5
Merge request rejects sent: 0
Merge responses received: 0
Merge response rejects sent: 0
Activation requests received: 5
Activation request rejects sent: 0
Activation requests sent: 0
```

```
Activation request rejects received: 0
v_226# pwwn 21:00:00:20:37:6f:dc:0e
```

Related Commands

Command	Description
device-alias name	Configures device alias names.
device-alias database	Configures device alias information.
device-alias distribute	Enables device alias CFS distribution.

show device-alias status

To view the current device alias mode setting, use the device-alias status command.

show device-alias status

Syntax Description

This command has no arguments or keywords.

Command Default

Basic mode.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the device alias status:

```
switch# show device-alias status
Fabric Distribution: Enabled
Database:- Device Aliases 0 Mode: Basic
Locked By:- User "admin" SWWN 20:00:00:0d:ec:30:90:40
Pending Database:- Device Aliases 0 Mode: Basic
```

Related Commands

Command	Description
device-alias commit	Commits changes to the active device alias database.
device-alias database	Configures and activates the device alias database.

show diagnostic bootup level

To display the diagnostic bootup level information (bypass or complete) that is currently in place on the device, use the show diagnostic bootup level command.

show diagnostic bootup level

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the diagnostic bootup level information (bypass or complete) that is currently in place on the device:

```
switch# show diagnostic bootup level
Current bootup diagnostic level: complete
switch#
```

Related Commands

Commands	Description
debug sme	Debugs Cisco SME features.

show diagnostic content module

To display information about diagnostic test content for a module, use the show diagnostic content module command.

show diagnostic content module {**module-number**|**all**}

Syntax Description

module-number	Displays the module number. The range is from 1 to 10.
all	Displays all module ID.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display information about diagnostic test content for a module:

```
switch# show diagnostic content module 1
Module 1: 2/4/8/10/16 Gbps Advanced FC Module
Diagnostics test suite attributes:
B/C/* - Bypass bootup level test / Complete bootup level test
 / NA
P/*   - Per port test / NA
M/S/* - Only applicable to active / standby unit / NA
D/N/* - Disruptive test / Non-disruptive test / NA
H/O/* - Always enabled monitoring test / Conditionally enable
d test / NA
F/*   - Fixed monitoring interval test / NA
X/*   - Not a health monitoring test / NA
E/*   - Sup to line card test / NA
L/*   - Exclusively run this test / NA
T/*   - Not an ondemand test / NA
A/I/* - Monitoring is active / Monitoring is inactive / NA
switch#
```

Related Commands

Commands	Description
debug sme	Debugs Cisco SME features.

show diagnostic description module

To display the diagnostic test description for a module, use the show diagnostic description module command.

show diagnostic description module module-number test [{**test-id test-name**|**all**}]

Syntax Description

module-number	Displays the module number. The range is from 1 to 10.
test	Displays the diagnostic test selection.
test-id	Displays the diagnostic test ID.
test-name	Displays the test name.
all	Displays all test ID.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the diagnostic test description for a module:

```
switch# show diagnostic description module 1 test all
ASICRegisterCheck :
        A health monitoring test,enabled by default that chec
ks read/write
        access to scratch registers on ASICs on the module.
PrimaryBootROM :
        A health monitoring test that verifies the primary Bo
otROM
        state.
SecondaryBootROM :
        A health monitoring test that verifies the secondary
BootROM
        state.
EOBCPortLoopback :
switch#
```

Related Commands

Commands	Description
debug sme	Debugs Cisco SME features.

show diagnostic events

To display the diagnostic events by error and information event type, use the show diagnostic events command.

show diagnostic events [{**error**|**info**}]

Syntax Description

error	Displays the error event type.
info	Displays the information event type.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the diagnostic events by error event type:

```
switch# show diagnostic events error
switch#
```

Related Commands

Commands	Description
debug sme	Debugs Cisco SME features.

show diagnostic ondemand setting

To display the information about on demand diagnostic settings, use the show diagnostic ondemand setting command.

show diagnostic ondemand setting

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the information about on demand diagnostic settings:

```
switch# show diagnostic ondemand setting
Test iterations = 1
        Action on test failure = continue until test failure
limit reaches 1
switch#
switch#
```

Related Commands

Commands	Description
debug sme	Debugs Cisco SME features.

show diagnostic result module

To display the information about the diagnostic test result for a module, use the show diagnostic result module command.

show diagnostic result module module-number all [{**detail**|**statistics**|**test**}]

Syntax Description

module-number	Displays the module number. The range is from 1 to 10.
detail	(Optional) Displays the detailed result.
statistics	Displays the statistics result.
test	Displays the diagnostic test selection.
all	Displays all test ID.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the detailed information about the diagnostic test result for a module:

```
switch# show diagnostic result module 1 detail
Current bootup diagnostic level: complete
Module 1: 2/4/8/10/16 Gbps Advanced FC Module
  Diagnostic level at card bootup: complete
        Test results: (. = Pass, F = Fail, I = Incomplete,
        U = Untested, A = Abort, E = Error disabled)

        ----------------------------------------------------
-----------------
        1) ASICRegisterCheck .
                Error code ------------------> DIAG TEST SUCC
ESS
                Total run count -------------> 23
                Last test execution time ----> Fri Jun 26 21:
25:33 2009
                First test failure time ------>  n/a
                Last test failure time ------>  n/a
--More--
switch#
```

Related Commands

Commands	Description
debug sme	Debugs Cisco SME features.

show diagnostic simulation module

To display the information about a simulated diagnostic result for a module, use the show diagnostic simulation module command.

show diagnostic simulation module module-number

Syntax Description

module-number	Displays the module number. The range is from 1 to 10.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the information about a simulated diagnostic result for a module:

```
switch# show diagnostic simulation module 1
Card(1): 2/4/8/10/16 Gbps Advanced FC Module
_____________________________________________________
    -NA-
switch#
```

Related Commands

Commands	Description
debug sme	Debugs Cisco SME features.

show diagnostic status module

To display test status for a module, use the show diagnostic status module command.

show diagnostic status module module-number

Syntax Description

module-number	Displays the module number. The range is from 1 to 10.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to displays test status for a module:

```
switch# show diagnostic status module 1
<BU>-Bootup Diagnostics, <HM>-Health Monitori
ng Diagnostics
                <OD>-OnDemand Diagnostics, <SCH>-Scheduled Di
agnostics
==============================================
Card:(1) 2/4/8/10/16 Gbps Advanced FC Module
==============================================
Current running test                Run by
    -NA-                            -NA-
Currently Enqueued Test             Run by
    -NA-                            -NA-
indapex-03#
switch#
switch#
```

Related Commands

Commands	Description
debug sme	Debugs Cisco SME features.

show diagnostic status module

To display the test status for all tests on a module, use the show diagnostic status module command.

show diagnostic status module module-number

Syntax Description

module-number	Displays the module number. The range is from 1 to 10.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the test status for all tests on a module:

```
switch# show diagnostic status module 1
<BU>-Bootup Diagnostics, <HM>-Health Monitori
ng Diagnostics
                <OD>-OnDemand Diagnostics, <SCH>-Scheduled Di
agnostics
==============================================
Card:(1) 2/4/8/10/16 Gbps Advanced FC Module
==============================================
Current running test               Run by
    -NA-                           -NA-
Currently Enqueued Test            Run by
    -NA-                           -NA-
switch#
```

Related Commands

Commands	Description
debug sme	Debugs Cisco SME features.

show dmm discovery-log

To display SCSI device discovery logs, use the **show dmm discovery-log** command in EXEC mode.

show dmm discovery-log {**all**|**error**}

Syntax Description

all	Displays all entries in the device discovery SCSI log.
error	Displays error entries in the device discovery SCSI log.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

You must connect to an SSM on your switch to execute DMM **show** commands. Use the **show module** command to determine the slot number of an SSM on your switch. Use the **attach module** command to connect to the SSM.

Examples

The following example displays error entries:

```
switch# attach module 3
Attaching to module 3 ...
To exit type 'exit', to abort type '$.'
Bad terminal type: "ansi". Will assume vt100.
module-3# show dmm discovery-log error
005 State: 3
CDB: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Sts:0x02 SnsKey:0x02 AscAscq:0x0403
Time:    5(ms)
LogIndex:26 HostPWWN:2c:fc:00:05:30:01:9e:88  TargetPWWN:50:06:01:62:30:60:36:64
OPC: 0x00 Lun:0x0000000000000006 State: 3
CDB: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Sts:0x02 SnsKey:0x02 AscAscq:0x0403
Time:    4(ms)
```

Related Commands

Command	Description
dmm module	Enables DMM configuration on a module.
show dmm srvr-vt-login	Enables the DMM feature.

show dmm fp-port

To display front panel ports on a line card, use the **show dmm fp-port** command in EXEC mode.

show dmm fp-port

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

You must connect to an SSM on your switch to execute DMM **show** commands. Use the **show module** command to determine the slot number of an SSM on your switch. Use the **attach module** *slot* command to connect to the SSM.

Examples

The following example displays front panel ports:

```
switch# attach module 3
Attaching to module 3 ...
To exit type 'exit', to abort type '$.'
Bad terminal type: "ansi". Will assume vt100.
module-3# show dmm fp-port
Cisco DMM Front Panel Port Map
--------------------------------------------------------------------
 Port     Index     Mirage Id    DPP Id
--------------------------------------------------------------------
  1           0           1          2
  2           1           1          2
  3           2           1          2
  4           3           1          2
  5           4           2          3
  6           5           2          3
  7           6           2          3
  8           7           2          3
  9           8           3          6
 10           9           3          6
 11          10           3          6
 12          11           3          6
 13          12           4          7
 14          13           4          7
 15          14           4          7
 16          15           4          7
 17          16           1          1
 18          17           1          1
 19          18           1          1
 20          19           1          1
 21          20           2          4
 22          21           2          4
 23          22           2          4
```

```
24              23              2               4
25              24              3               5
26              25              3               5
27              26              3               5
28              27              3               5
29              28              4               8
30              29              4               8
31              30              4               8
32              31              4               8
```

Related Commands

Command	Description
dmm module	Enables DMM configuration on a module.
show dmm srvr-vt-login	Enables the DMM feature.

show dmm ip-peer

To display information about the IP peers the DMM interface is connected to, use the **show dmm ip-peer** command in EXEC mode.

show dmm ip-peer

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

You must connect to an SSM on your switch to execute DMM **show** commands. Use the **show module** command to determine the slot number of an SSM on your switch. Use the **attach module** *slot* command to connect to the SSM.

Examples

The following example displays DMM IP peer information:

```
switch# attach module 3
Attaching to module 3 ...
To exit type 'exit', to abort type '$.'
Bad terminal type: "ansi". Will assume vt100.
module-3# show dmm ip-peer
                  Cisco DMM IP Peer Table
------------------------------------------------------------------------
 No      Type              SD   IP Address      TCP State
------------------------------------------------------------------------
  1      CONFIG_STATION    23    10.100.2.1      DOWN
  2      PEER_SSM          22    10.100.1.20     UP
  3      CONFIG_STATION    19    10.100.2.1      DOWN
```

show dmm job

To display DMM job information, use the **show dmm job** command in EXEC mode.

show dmm job *job-id* {**detail**|**job-fsm-eventlog**|**job-infra-fsm-eventlog**|**lun_tokens token** *tok-pwwn*|**session**|[**session_id** *sess-id*] **[session-event-log]**|**storage** [**tgt-pwwn** *tgt-pwwn*] **vi-pwwn** *vi-pwwn* [{**lun-event-log** *lun-id*|**tgt-event-log**}]}

Syntax Description

job-id	Specifies the job ID. The range is 0 to 18446744073709551615.
detail	Displays detailed job information.
job-fsm-eventlog	Displays the Job FSM Event Log.
job-infra-fsm-eventlog	Displays the Job Infra FSM Event Log.
lun_tokens	Displays a list of job LUN tokens.
token *tok-pwwn*	Specifies the storage port world-wide name.
session	Displays job session information.
sess-id	(Optional) Specifies the job session. The range is 0 to 2147483647255.
session-event-log	(Optional) Displays the Session FSM Event Log.
storage	Displays the storage ports discovered by DMM.
tgt-pwwn *tgt-pwwn*	(Optional) Specifies the storage port world-wide name. The format is hh:hh:hh:hh:hh:hh:hh:hh, where h is a hexadecimal number.
vi-pwwn *vi-pwwn*	(Optional) Specifies the Virtual Initiator port world-wide name. The format is hh:hh:hh:hh:hh:hh:hh:hh, where h is a hexadecimal number.
lun-event-log *lun-id*	(Optional) Displays the Virtual Initiator and Target LUN FSM event log and specifies the LUN ID.
tgt-event-log	(Optional) Displays the Virtual Initiator and Target FSM Event Log.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(2)	Removed the session-id keyword from the syntax description. Changed the command output.
3.2(1)	This command was introduced.

Usage Guidelines

You must connect to an SSM on your switch to execute DMM **show** commands. Use the **show module** command to determine the slot number of an SSM on your switch. Use the **attach module** *slot* command to connect to the SSM.

Examples

The following example shows how to display a summary of the jobs:

```
switch# show dmm job
================================================================================

                      Data Mobility Manager Job Information
================================================================================

 Num Job Identifier     Name                    Type  Mode  Method DMM GUI IP Peer SSM
DPP Session  Status    Est. Time of Completion
================================================================================

  1         1         CLI_JOB_0x1               SRVR  ONL  METHOD-2 127.0.0.1  NOT_APPL
      1         IN_PROGRESS      Wed Jun 30 07:10:16 1971
Number of Jobs :1
switch#
```

Related Commands

Command	Description
dmm module	Enables DMM configuration on a module.
show dmm srvr-vt-login	Enables the DMM feature.

show dmm module

To display DMM module information use the show dmm module command.

show dmm module module-id vi-list

Syntax Description

module-id	Specifies the module ID. The range is 1 to 13.
vi-list	Displays the VI list.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(1b)	Added the vi-list to syntax description and the command output.
3.2(1)	This command was introduced.

Usage Guidelines

The show dmm module command displays the list of VIs assigned to each data movement engine. A storage based data migration job uses one of these VIs. Use the command to choose the VI and then use the **dmm module job set-vi** command to specify the VI.

Examples

The following example shows how to display a summary of all the jobs:

```
switch# show dmm module 4 vi-list
================================================================================
DPP-Id   VI-pWWN                  VI-nWWN                 Outstanding jobs
================================================================================
1        24:53:00:05:30:00:64:22  24:52:00:05:30:00:64:22  0
2        20:0d:00:05:30:00:64:22  2c:c4:00:05:30:00:64:21  0
3        20:0f:00:05:30:00:64:22  20:0e:00:05:30:00:64:22  0
4        24:55:00:05:30:00:64:22  24:54:00:05:30:00:64:22  0
5        24:57:00:05:30:00:64:22  24:56:00:05:30:00:64:22  0
6        20:11:00:05:30:00:64:22  20:10:00:05:30:00:64:22  0
7        24:51:00:05:30:00:64:22  24:50:00:05:30:00:64:22  0
8        24:59:00:05:30:00:64:22  24:58:00:05:30:00:64:22  0
```

Related Commands

Command	Description
dmm module	Enables DMM configuration on a module.
dmm module job set-vi	Specifies the VI for the storage based job.
show dmm srvr-vt-login	Enables the DMM feature.

show dmm srvr-vt-login

To display server virtual target login information, use the **show dmm srvr-vt-login** command in EXEC mode.

show dmm srvr-vt-login [**job-id** *job-id*] **server-pwwn** *srvr-pwwn* **vt-pwwn** *vt-pwwn* {**fc_rdrt-fsm-eventlog**|**login-fsm-eventlog**}

Syntax Description

job-id *job-id*	(Optional) Specifies the job ID. The range is 0 to 18446744073709551615.
server-pwwn *srvr-pwwn*	Specifies the server port world-wide name. The format is hh:hh:hh:hh:hh:hh:hh:hh, where h is a hexadecimal number.
vt-pwwn *vt-pwwn*	Specifies the VT port worldwide name. The format is hh:hh:hh:hh:hh:hh:hh:hh, where h is a hexadecimal number.
fc_rdrt-fsm-eventlog	Displays the server VT FC-Redirect FSM event log.
login-fsm-eventlog	Displays the server VT FSM event log.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

You must connect to an SSM on your switch to execute DMM **show** commands. Use the **show module** command to determine the slot number of an SSM on your switch. Use the **attach module** command to connect to the SSM.

Examples

The following example shows how to display the server VT login summary:

```
switch# show dmm srvr-vt-login
================================================================================================
           Data Mobility Manager Server VT Login Information
================================================================================================
  Id  Job Id    VSAN Srvr pWWN                Srvr FCID VT pWWN                   VT FCID
      State (FC Redirect/Login)
================================================================================================
  1   1187978941    1  21:32:00:0d:ec:02:2d:82   0x660000  21:36:00:0d:ec:02:2d:82   0x660003
    (READY/WAITING_PLOGI)
  2   1187978941    1  21:32:00:0d:ec:02:2d:82   0x660000  21:34:00:0d:ec:02:2d:82   0x66000a
    (READY/WAITING_PLOGI)
Number of Logins :2
```

The following example shows how to display the event log for a specified VT:

```
switch# show dmm srvr-vt-login  job-id 1187978941 server-pwwn 21:32:00:0d:ec:02:2d:82 vt-pwwn
 21:36:00:0d:ec:02:2d:82 login-fsm-e
```

```
==========================================================================================
Server/VT Login FSM Event Log -> Job Id : 1187978941 Server : 21:32:00:0d:ec:02:2d:82  VT
: 21:36:00:0d:ec:02:2d:82
==========================================================================================
Log Entry: 1 time: Fri Aug 24 11:09:19 2007
    Curr state: DMM_SRVR_VT_LOGIN_S_NULL
    Triggered event: DMM_SRVR_VT_LOGIN_E_START_ACTION
Log Entry: 2 time: Fri Aug 24 11:09:19 2007
    Curr state: DMM_SRVR_VT_LOGIN_S_WAITING_PLOGI
    Triggered event: DMM_SRVR_VT_LOGIN_E_LOGIN_DONE_OK
```

Related Commands

Command	Description
dmm module	Enables DMM configuration on a module.
show dmm srvr-vt-login	Displays the DMM feature.

show dmm vt

To display virtual target information, use the **show dmm vt** command in EXEC mode.

show dmm vt vt-job-id *job-id* **pwwn** *vt-pwwn* **vt-fsm-eventlog**

Syntax Description

vt-job-id *job-id*	Specifies the virtual target job ID. The range is 0 to 18446744073709551615.
pwwn *vt-pwwn*	Specifies the virtual target port worldwide name. The format is hh:hh:hh:hh:hh:hh:hh:hh, where h is a hexadecimal number.
vt-fsm-eventlog	Displays the virtual target (VT) Finite State Machine (FSM) event log.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

You must connect to an SSM on your switch to execute DMM **show** commands. Use the **show module** command to determine the slot number of an SSM on your switch. Use the **attach module** *slot* command to connect to the SSM.

Examples

The following example shows how to display the virtual target information:

```
switch# attach module 3
Attaching to module 3 ...
To exit type 'exit', to abort type '$.'
Bad terminal type: "ansi". Will assume vt100.
module-3# show dmm vt
================================================================================
                      Data Mobility Manager VT Information
================================================================================
  Id Job Id      VT pWWN                    VSAN FCID       IF-IDX      PORT    STATE
================================================================================
  1  1177009472  2f:00:00:05:30:01:9e:88    3    0xee00a0   0x1110000   0x10    VT_UP
  2  1177009472  2c:fe:00:05:30:01:9e:88    3    0xee00a1   0x1110000   0x10    VT_UP
Number of VTs :2
```

Related Commands

Command	Description
dmm module	Enables DMM configuration on a module.
show dmm srvr-vt-login	Displays the DMM feature.

show dpvm

To display dynamic port VSAN membership (DPVM) information, use the **show dpvm** command.

show dpvm {**database** [**active**]|**pending**|**pending-diff**|**ports** [**vsan** *vsan-id*]|**status**}

Syntax Description

database	Displays both the configured and active DPVM databases.
active	Displays only the active DPVM database.
pending	Displays pending DPVM operations.
pending-diff	Displays differences between the pending DPVM operations and the active DPVM database.
ports	Displays DPVM information for the ports.
vsan *vsan-id*	Specifies a VSAN ID. The range is from 0 to 4093.
status	Displays DPVM status information.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, DPVM must be enabled using the **dpvm enable** command.

Examples

The following example shows how to display DPVM database information:

```
switch# show dpvm database
pwwn 00:00:00:00:00:00:00:01 vsan 1
pwwn 00:00:00:00:00:00:00:02 vsan 1
[Total 2 entries]
```

Related Commands

Command	Description
dpvm database	Configures the DPVM database.

show dpvm merge statistics

To display the DPVM merge statistics, use the show dpvm merge statistics command.

show dpvm merge statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the DPVM merge statistics:

```
switch# show dpvm merge statistics
DPVM merge statistics:
======================
 Merge request received     : 0
 Merge response sent        : 0
 Merge response received    : 0
 Activate request sent      : 0
 Activate response received : 0
 Application response sent  : 0
 Merge success received     : 0
 Merge failure received     : 0
switch#
```

Related Commands

Command	Description
clear dpvm merge statistics	Clears the DPVM merge statistics.

show dpvm merge status

To display the DPVM merge status, use the dpvm merge status command.

show dpvm merge status

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(1b)	Enhanced the command output.

Usage Guidelines

None.

Examples

The following example shows how to display the conflict in DPVM database:

```
switch# show dpvm merge status
Last Merge Time Stamp     : Fri Aug  8 15:46:36 2008
Last Merge State          : Fail
Last Merge Result         : Fail
Last Merge Failure Reason : DPVM DB conflict found during merge [cfs_status: 76] Last Merge
 Failure Details     : DPVM merge failed due to database conflict
Local Switch WWN          : 20:00:00:0d:ec:24:e5:00
Remote Switch WWN         : 20:00:00:0d:ec:09:d5:c0

------------------------------------------------------------------------------
        Conflicting DPVM member(s)                    Loc VSAN   Rem VSAN
------------------------------------------------------------------------------
dev-alias dpvm_dev_alias_1 [21:00:00:04:cf:cf:45:ba]    1313       1414
dev-alias dpvm_dev_alias_2 [21:00:00:04:cf:cf:45:bb]    1313       1414
dev-alias dpvm_dev_alias_3 [21:00:00:04:cf:cf:45:bc]    1313       1414
[Total 3 conflict(s)]
switch#
```

show environment

To display all environment-related switch information (status of chassis clock, chassis fan modules, power supply modules, power supply redundancy mode and power usage summary, module temperature thresholds and alarm status, use the **show environment** command.

show environment [{**clock**|**fan**|**power**|**temperature**}]

Syntax Description

clock	(Optional) Displays status of chassis clock modules.
fan	(Optional) Displays status of chassis fan modules.
power	(Optional) Displays status of power supply modules, power supply. redundancy mode and power usage summary.
temperature	(Optional) Displays module temperature thresholds and alarm status of temperature sensors.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the power capacity and power distribution of the system:

```
switch(config)# show environment power Power Supply
Voltage: 42 Volts
-------------------------------------------------------
PS  Model                Power       Power     Status
                         (Watts)     (Amp)
-------------------------------------------------------
1   DS-CAC-3000W         2771.16     65.98     Ok
2   ------------            0.00      0.00     Fail/Shut
Mod Model                Power     Power       Power     Power       Status
                         Requested Requested   Allocated Allocated
                         (Watts)   (Amp)       (Watts)   (Amp)
--- -------------------  -------   ----------  --------- ----------  ----------
1    DS-X9248-256K9       136.50    3.25       136.50    3.25        Powered-Up
2    DS-X9248-96K9        298.20    7.10       298.20    7.10        Powered-Up
3    DS-X9304-18K9        199.50    4.75       199.50    4.75        Powered-Up
4    DS-X9232-256K9       130.20    3.10       130.20    3.10        Powered-Up
5    DS-X9530-SF2AK9      126.00    3.00       126.00    3.00        Powered-Up
6    DS-X9530-SF2AK9      126.00    3.00       126.00    3.00        Powered-Up
7    DS-X9248-256K9       136.50    3.25       136.50    3.25        Powered-Up
8    DS-X9232-256K9       130.20    3.10       130.20    3.10        Powered-Up
9    DS-X9232-256K9       130.20    3.10       130.20    3.10        Powered-Up
fan1 DS-9SLOT-FAN         210.00    5.00       210.00    5.00        Powered-Up
Power Usage Summary:
```

```
--------------------
Power Supply redundancy mode:                 Redundant
Power Supply redundancy operational mode:     Redundant
Total Power Capacity                             2771.16 W
Power reserved for Supervisor(s)                  252.00 W
Power reserved for Fan Module(s)                  210.00 W
Power currently used by Modules                  1161.30 W
                                                 -------------
Total Power Available                             1147.86 W
                                                 -------------
switch9509(config)#
```

The following example displays the status and alarm states of the clock, fan, power supply and temperature sensors:

```
switch# show environment
Power Supply:
Voltage: 42 Volts
-----------------------------------------------------
PS  Model                Power       Power     Status
                         (Watts)     (Amp)
-----------------------------------------------------
1   DS-CAC-3000W         2771.16     65.98     Ok
2   ------------            0.00      0.00     Fail/Shut
Mod Model                Power     Power       Power     Power       Status
                         Requested Requested   Allocated Allocated
                         (Watts)   (Amp)       (Watts)   (Amp)
--- -------------------  -------   ----------  --------- ----------  ----------
1    DS-X9248-256K9       136.50    3.25       136.50    3.25        Powered-Up
2    DS-X9248-96K9        298.20    7.10       298.20    7.10        Powered-Up
3    DS-X9304-18K9        199.50    4.75       199.50    4.75        Powered-Up
4    DS-X9232-256K9       130.20    3.10       130.20    3.10        Powered-Up
5    DS-X9530-SF2AK9      126.00    3.00       126.00    3.00        Powered-Up
6    DS-X9530-SF2AK9      126.00    3.00       126.00    3.00        Powered-Up
7    DS-X9248-256K9       136.50    3.25       136.50    3.25        Powered-Up
8    DS-X9232-256K9       130.20    3.10       130.20    3.10        Powered-Up
9    DS-X9232-256K9       130.20    3.10       130.20    3.10        Powered-Up
fan1 DS-9SLOT-FAN         210.00    5.00       210.00    5.00        Powered-Up
Power Usage Summary:
--------------------
Power Supply redundancy mode:                 Redundant
Power Supply redundancy operational mode:     Redundant
Total Power Capacity                             2771.16 W
Power reserved for Supervisor(s)                  252.00 W
Power reserved for Fan Module(s)                  210.00 W
Power currently used by Modules                  1161.30 W
                                                 -------------
Total Power Available                             1147.86 W
                                                 -------------
Clock:
------------------------------------------------------------
Clock           Model                Hw         Status
------------------------------------------------------------
A               DS-C9509-CL          1.0        Ok/Active
B               DS-C9509-CL          1.0        Ok/Standby
Fan:
-----------------------------------------------------
Fan             Model                Hw         Status
-----------------------------------------------------
ChassisFan1     DS-9SLOT-FAN         2.0        Ok
Fan_in_PS1      --                   --         Ok
Fan_in_PS2      --                   --         Failure
Fan Air Filter : NotSupported
```

```
Temperature:
--------------------------------------------------------------------------
Module   Sensor        MajorThresh   MinorThres   CurTemp     Status
                       (Celsius)     (Celsius)    (Celsius)
--------------------------------------------------------------------------
1        Outlet1         80              70          47          Ok
1        Outlet2         80              70          45          Ok
1        Intake1         65              50          34          Ok
1        IOSlice0        105             95          54          Ok
1        IOSlice1        105             95          57          Ok
2        Outlet1         80              70          42          Ok
2        Outlet2         80              70          47          Ok
2        Intake1         65              50          31          Ok
3        Outlet1         75              60          38          Ok
3        Outlet2         75              65          38          Ok
3        Intake1         65              50          30          Ok
4        Outlet1         80              70          41          Ok
4        Outlet2         80              70          40          Ok
4        Intake1         65              50          33          Ok
4        IOSlice0        105             95          46          Ok
4        IOSlice1        105             95          47          Ok
5        Outlet1         75              60          36          Ok
5        Outlet2         75              60          39          Ok
5        Intake1         65              50          32          Ok
6        Outlet1         75              60          36          Ok
6        Outlet2         75              60          40          Ok
6        Intake1         65              50          33          Ok
7        Outlet1         80              70          44          Ok
7        Outlet2         80              70          44          Ok
7        Intake1         65              50          37          Ok
7        IOSlice0        105             95          47          Ok
7        IOSlice1        105             95          49          Ok
8        Outlet1         80              70          45          Ok
8        Outlet2         80              70          45          Ok
8        Intake1         65              50          36          Ok
8        IOSlice0        105             95          49          Ok
8        IOSlice1        105             95          51          Ok
9        Outlet1         80              70          45          Ok
9        Outlet2         80              70          45          Ok
9        Intake1         65              50          40          Ok
9        IOSlice0        105             95          48          Ok
9        IOSlice1        105             95          49          Ok
switch(config)#
```

Related Commands

Command	Description
show hardware	Displays all hardware components on a system.

show event manager environment

To display the name and value of Embedded Event Manager (EEM) environment variables, use the show event manager environment command.

show event manager environment {**variable-name**|**all**}

Syntax Description

variable-name	Displays information about the specified environment variable.
all	Displays information about all environment variables.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows all the EEM environment variables:

```
switch# show event manager environment all
switch#
```

Related Commands

Command	Description
event manager environment	Displays an EEM environment variable.

show event manager policy

To display the registered Embedded Event Manager (EEM) policies, use the show event manager policy command.

show event manager policy [detail] [{**policy-name**|**inactive**}]

Syntax Description

detail	(Optional) Displays details of all policies.
policy-name	(Optional) Specifies a policy-name policy to display.
inactive	(Optional) Displays only those policies that are inactive.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the EEM policies:

```
switch# show event manager policy
```

switch

Related Commands

Command	Description
event manager applet	Displays an applet with the Emedded Event manager.

show fabric switch information vsan

To display the switch name, switch model, running version and memory details, use the **show fabric switch information vsan command**.

show fabric switch information [**vsan vsan-id**]

Syntax Description

vsan-id	(Optional) Specifies the VSAN range. The range is from 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(9)	Added a note.
6.2(7)	This command was introduced.

Usage Guidelines

None.

Note In scenarios where the show fabric switch information command output has few missing parameters like switchname, model, version, etc. Please re-execute this command after few seconds.

Note Without the VSAN option this command will displays the information about switches in all the VSANs.

Note SUP memory is not displayed for switches that are running versions prior to 6.2(7) release.

Examples

The following example displays the switch name, switch model, running version and memory details of all switches in the fabric in the given VSAN:

```
switch# show fabric switch information vsan 320
VSAN 320:
--------------------------------------------------------------------------------
Switch Name Model Version Sup Memory
--------------------------------------------------------------------------------
sw3-gd99-9148s DS-C9148S48PK9 6.2(9) 4 GB
minishan-scale DS-C9148S48PK9 6.2(9) 4 GB
mdsng-sca DS-C9710 6.2(9) 8 GB
```

x

show fabric-binding

To display configured fabric binding information, use the **show fabric-binding** command in EXEC mode.

show fabric-binding {**database [active]** [**vsan** *vsan-id*]|**efmd statistics** [**vsan** *vsan-id*]|**statistics** [**vsan** *vsan-id*]|**status** [**vsan** *vsan-id*]|**violations** [**last** *number*]}

database	Displays configured database information.
active	Displays the active database configuration information.
vsan *vsan-id*	(Optional) Specifies the FICON-enabled VSAN ID. The range is 1 to 4093.
efmd statistics	Displays Exchange Fabric Membership Data (EFMD) statistics.
statistics	Displays fabric binding statistics.
status	Displays fabric binding status.
violations	Displays violations in the fabric binding configuration.
last *number*	(Optional) Specifies recent violations. The range is 1 to 100.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays configured fabric binding database information:

```
switch# show fabric-binding database
-------------------------------------------------
Vsan   Logging-in Switch WWN     Domain-id
-------------------------------------------------
1      21:00:05:30:23:11:11:11   0x66(102)
1      21:00:05:30:23:1a:11:03    0x19(25)
1      20:00:00:05:30:00:2a:1e   0xea(234)
4      21:00:05:30:23:11:11:11   0x66(102)
4      21:00:05:30:23:1a:11:03    0x19(25)
61     21:00:05:30:23:1a:11:03    0x19(25)
61     21:00:05:30:23:11:11:11   0x66(102)
[Total 7 entries]
```

The following example displays active fabric binding information:

```
switch# show fabric-binding database active
-------------------------------------------------
```

```
Vsan   Logging-in Switch WWN     Domain-id
-------------------------------------------------
1      21:00:05:30:23:11:11:11   0x66(102)
1      21:00:05:30:23:1a:11:03    0x19(25)
1      20:00:00:05:30:00:2a:1e   0xea(234)
61     21:00:05:30:23:1a:11:03    0x19(25)
61     21:00:05:30:23:11:11:11   0x66(102)
61     20:00:00:05:30:00:2a:1e   0xef(239)
```

The following example displays active VSAN-specific fabric binding information:

```
switch# show fabric-binding database active vsan 61
-------------------------------------------------
Vsan   Logging-in Switch WWN     Domain-id
-------------------------------------------------
61     21:00:05:30:23:1a:11:03    0x19(25)
61     21:00:05:30:23:11:11:11   0x66(102)
61     20:00:00:05:30:00:2a:1e   0xef(239)
[Total 3 entries]
```

The following example displays configured VSAN-specific fabric binding information:

```
switch# show fabric-binding database vsan 4
-------------------------------------------------
Vsan   Logging-in Switch WWN     Domain-id
-------------------------------------------------
4      21:00:05:30:23:11:11:11   0x66(102)
4      21:00:05:30:23:1a:11:03    0x19(25)
[Total 2 entries]
```

The following example displays fabric binding statistics:

```
switch# show fabric-binding statistics
Statistics For VSAN: 1
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 4
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 61
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 345
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 346
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted  : 0
Total Logins denied     : 0
```

```
Statistics For VSAN: 347
------------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 348
------------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 789
------------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 790
------------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0
Total Logins permitted  : 0
Total Logins denied     : 0
```

The following example displays fabric binding status for each VSAN:

```
switch# show fabric-binding status
VSAN 1 :Activated database
VSAN 4 :No Active database
VSAN 61 :Activated database
VSAN 345 :No Active database
VSAN 346 :No Active database
VSAN 347 :No Active database
VSAN 348 :No Active database
VSAN 789 :No Active database
VSAN 790 :No Active database
```

The following example displays EFMD statistics:

```
switch# show fabric-binding efmd statistics
EFMD Protocol Statistics for VSAN 1
---------------------------------------
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0
EFMD Protocol Statistics for VSAN 4
---------------------------------------
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0
EFMD Protocol Statistics for VSAN 61
---------------------------------------
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0
```

The following example displays EFMD statistics for a specified VSAN:

```
switch# show fabric-binding efmd statistics vsan 4
EFMD Protocol Statistics for VSAN 4
---------------------------------------
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0
```

The following example displays fabric binding violations:

```
switch# show fabric-binding violations
-------------------------------------------------------------------------------
VSAN Switch WWN [domain] Last-Time [Repeat count] Reason
-------------------------------------------------------------------------------
3 20:00:00:05:30:00:4a:1e [*] Nov 25 05:44:58 2003 [2] sWWN not found
3 20:00:00:05:30:00:4a:1e [0xeb] Nov 25 05:46:14 2003 [2] Domain mismatch
4 20:00:00:05:30:00:4a:1e [*] Nov 25 05:46:25 2003 [1] Database mismatch
```

show fc2

To display FC2 information, use the **show fc2** command.

show fc2 {**bind**|**classf**|**exchange**|**exchresp**|**flogi**|**nport**|**plogi**|**plogi_pwwn**|**port [brief]**|**socket**|**sockexch**|**socknotify**|**socknport**|**vsan**}

Syntax Description

bind	Displays FC2 socket bindings.
classf	Displays FC2 classf sessions.
exchange	Displays FC2 active exchanges.
exchresp	Displays FC2 active responder exchanges.
flogi	Displays FC2 FLOGI table.
nport	Displays FC2 local N ports.
plogi	Displays FC2 PLOGI sessions.
plogi_pwwn	Displays FC2 PLOGI pWWN entries.
port brief	Displays FC2 physical port table.
socket	Displays FC2 active sockets.
sockexch	Displays FC2 active exchanges for each socket.
socknotify	Displays FC2 local N port PLOGI/LOGO notifications for each socket.
socknport	Displays FC2 local N ports per each socket.
vsan	Displays FC2 VSAN table.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays FC2 active socket information:

```
switch# show fc2 socket
SOCKET   REFCNT PROTOCOL      PID   RCVBUF  RMEM_USED     QLEN    NOTSK
b2a64b20        2        0     1421    65535          0        0        0
```

```
b2a647e0        3        0     1418   262142          0        0        0
b2a644a0        3        0     1417    65535          0        0        0
b2a64160        3        0     1417   262142          0        0        0
b294b180        3        0     1411    65535          0        0        0
b294ae40        3        0     1411    65535          0        0        0
b294a7c0        3        0     1410    65535          0        0        0
b294a480        2        7     1410    65535          0        0        0
b294a140        3        0     1409   262142          0        0        0
b278bb20        3        0     1409   262142          0        0        0
b278b4a0        3        0     1407    65535          0        0        0
b278b160        3        0     1407   256000          0        0        0
b278ae20        3        0     1407    65535          0        0        0
b1435b00        3        0     1408    65535          0        0        0
b1434e00        3        0     1406    65535          0        0        0
b1434ac0        3        0     1406   131072          0        0        0
b1434780        3        0     1406    65535          0        0        0
b1434440        2        0     1405   131072          0        0        0
b1434100        3        0     1405   262142          0        0 b1434440
b22e2420        2        0     1372    65535          0        0        0
...
```

The following example displays FC2 socket binding information:

```
switch# show fc2 bind
  SOCKET RULE   SINDEX   VSAN     D_ID     MASK TYPE  SUBTYPE M_VALUES
b23ba0c0   16  6081000      1        0        0    0 00:00:00 00:00:00:00:00:00:00:00
b2a647e0    7 ffffffff  65535   fffffd   ffffff   22 03:01:00 14:15:16:00:00:00:00:00
b294b180    7 ffffffff  65535   fffffd   ffffff    1 02:01:00 61:62:00:00:00:00:00:00
b294ae40    7 ffffffff  65535   fffc00   ffff00   22 01:01:00 1b:00:00:00:00:00:00:00
b294a7c0    7 ffffffff  65535   fffffd   ffffff    1 01:01:00 10:00:00:00:00:00:00:00
...
```

The following example displays FC2 local N port information:

```
switch# show fc2 nport
REF   VSAN   D_ID   MASK   FL   ST  IFINDEX   CF   TC 2-SO   IC   RC   RS   CS
 EE 3-SO   IC   RC   RS   CS   EE
  1  65535 fffffd ffffff    3    0 ffffffff c800 0128 8000 0000 0000 2112 0064 0
008 8000 0000 0000 2112 0064 0000
  6  65535 fffc00 ffff00  18b    0 ffffffff c800 0128 8000 0000 0000 2112 0064 0
008 8000 0000 0000 2112 0064 0000
  2  65535 fffffa ffffff    3    0 ffffffff c800 0128 8000 0000 0000 2112 0064 0
008 8000 0000 0000 2112 0064 0000
  1  65535 fffffc ffffff    3    0 ffffffff c800 0128 8000 0000 0000 2112 0064 0
008 8000 0000 0000 2112 0064 0000
...
```

The following example displays FC2 PLOGI session information:

```
switch# show fc2 plogi
HIX  ADDRESS   VSAN   S_ID   D_ID  IFINDEX   FL  STATE   CF   TC 2-SO   IC   RC
  RS   CS   EE 3-SO   IC   RC   RS   CS   EE EECNT TCCNT 2CNT 3CNT REFCNT
2157 af364064      1 fffc6c 123400 ffffffff 0000      0 0000 0001 8000 0000 2000
 0256 0001 0001 8000 0000 2000 0256 0001 0000     0     0    0    0      1
```

The following example displays FC2 physical port information:

```
switch# show fc2 port
 IX ST MODE EMUL   TXPKTS   TXDROP    TXERR   RXPKTS   RXDROP  R_A_TOV  E_D_TOV
F-SO   RC   RS   CS   EE 2-SO   RS 3-SO   RS
  0  D    1    0        0        0        0        0        0    10000     2000
8000 0000 2112 0001 0001 8000 0256 8000 0256
```

```
  1  D    1    0        0        0        0        0        0    10000     2000
8000 0000 2112 0001 0001 8000 0256 8000 0256
  2  D    1    0        0        0        0        0        0    10000     2000
8000 0000 2112 0001 0001 8000 0256 8000 0256
  3  D    1    0        0        0        0        0        0    10000     2000
8000 0000 2112 0001 0001 8000 0256 8000 0256
  4  D    1    0        0        0        0        0        0    10000     2000
8000 0000 2112 0001 0001 8000 0256 8000 0256
...
```

The following example displays FC2 local N port PLOGI notifications for each socket:

```
switch# show fc2 socknotify
  SOCKET  ADDRESS REF   VSAN   D_ID   MASK   FL   ST  IFINDEX
b2a64160 b27f01e4   6  65535 fffc00 ffff00  18b    0 ffffffff
b294a7c0 b27f01e4   6  65535 fffc00 ffff00  18b    0 ffffffff
af8a3a60 b27f01e4   6  65535 fffc00 ffff00  18b    0 ffffffff
```

The following example displays FC2 local N ports for each socket:

```
switch# show fc2 socknport
  SOCKET  ADDRESS REF   VSAN   D_ID   MASK   FL   ST  IFINDEX
b2a64160 b27f01e4   6  65535 fffc00 ffff00  18b    0 ffffffff
b294b180 b27f0294   1  65535 fffffd ffffff    3    0 ffffffff
b294a7c0 b27f01e4   6  65535 fffc00 ffff00  18b    0 ffffffff
b278ae20 b27f0134   2  65535 fffffa ffffff    3    0 ffffffff
b1434e00 b27f0134   2  65535 fffffa ffffff    3    0 ffffffff
b1434780 b27f0084   1  65535 fffffc ffffff    3    0 ffffffff
af8a3a60 b27f01e4   6  65535 fffc00 ffff00  18b    0 ffffffff
```

The following example displays FC2 VSAN table:

```
switch# show fc2 vsan

  VSAN     X_ID  E_D_TOV  R_A_TOV                      WWN
     1        4     2000    10000  20:01:00:05:30:00:58:1f
     2        1     2000    10000  20:02:00:05:30:00:58:1f
     3        1     2000    10000  20:03:00:05:30:00:58:1f
     4        1     2000    10000  20:04:00:05:30:00:58:1f
     5        1     2000    10000  20:05:00:05:30:00:58:1f
     6        1     2000    10000  20:06:00:05:30:00:58:1f
     7        1     2000    10000  20:07:00:05:30:00:58:1f
     8        1     2000    10000  20:08:00:05:30:00:58:1f
     9        1     2000    10000  20:09:00:05:30:00:58:1f
    10        1     2000    10000  20:0a:00:05:30:00:58:1f
    11        1     2000    10000  20:0b:00:05:30:00:58:1f
    12        1     2000    10000  20:0c:00:05:30:00:58:1f
    13        1     2000    10000  20:0d:00:05:30:00:58:1f
    14        1     2000    10000  20:0e:00:05:30:00:58:1f
    15        1     2000    10000  20:0f:00:05:30:00:58:1f
    16        1     2000    10000  20:10:00:05:30:00:58:1f
    17        1     2000    10000  20:11:00:05:30:00:58:1f
    18        1     2000    10000  20:12:00:05:30:00:58:1f
....
```

show fcalias

To display the member name information in a Fibre Channel alias (fcalias), use the **show fcalias** command.

show fcalias [**name fcalias-name**] **[pending]** [**vsan** *vsan-id*]

Syntax Description

name *fcalias-name*	(Optional) Displays fcalias information for a specific name. The maximum length is 64.
pending	(Optional) Displays pending fcalias information.
vsan *vsan-id*	(Optional) Displays fcalias information for a VSAN. The range is 1 to 4093.

Command Default

Displays a list of all global fcaliases and all VSAN dependent fcaliases.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0(x)	Added the pending keyword.

Usage Guidelines

To make use of fcaliases as device names instead of using the cryptic device name, add only one member per fcalias.

Examples

The following example displays fcalias configuration information:

```
switch# show fcalias vsan 1
fcalias name Alias2 vsan 1
fcalias name Alias1 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:9c:48:e5
```

Related Commands

Command	Description
fcalias name	Configures fcalias names.

show fcanalyzer

To display the list of hosts configured for a remote capture, use the **show fcanalyzer** command.

show fcanalyzer

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The default keyword shown with the ActiveClient entry specifies that the default port is used to connect to the client.

Examples

The following example displays configured hosts:

```
switch# show fcanalyzer

PassiveClient = 10.21.0.3
PassiveClient = 10.21.0.3
ActiveClient = 10.21.0.3, DEFAULT
```

show fcc

To view FCC settings, use the **show fcc** commands.

show fcc [**statistics interface** {**fc** *slot* / *port*|**fcip** *fcip-id*|**iscsi** *slot* / *port*}]

Syntax Description

statistics interface	(optional) Displays FCC statistics for a specified interface.
fc *slot*/*port*	(optional) Specifies a Fibre Channel interface.
fcip *fcip-id*	(optional) Specifies an FCIP interface. The range is 1 to 255.
iscsi *slot*/*port*	(optional) Specifies an iSCSI interface.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays FCC information:

```
switch# show fcc
fcc is disabled
fcc is applied to frames with priority up to 4
```

show fcdomain

To display the Fibre Channel domain (fcdomain) information, use the show fcdomain command.

show fcdomain [{**address-allocation [cache]**|**allowed**|**domain-list**|**fcid persistent [unused]**|**pending** [**vsan vsan-id**]|**pending-diff** [**vsan vsan-id**]|**session-status** [**vsan vsan-id**]|**statistics** [{**interface** {**fc** *slot / port* [**vsan vsan-id**]|**fcip** *fcip-id* [**vsan vsan-id**]|**iscsi** *slot / port*}|**port-channel** [**vsan vsan-id**]}]|**status**|**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

address-allocation	(Optional) Displays statistics for the FC ID allocation.
cache	(Optional) Reassigns the FC IDs for a device (disk or host) that exited and reentered the fabric for the principal switch. In the cache content, VSAN refers to the VSAN that contains the device, WWN refers to the device that owned the FC IDs, and mask refers to a single or entire area of FC IDs.
allowed	Displays a list of allowed domain IDs.
domain-list	Displays a list of domain IDs granted by the principal switch.
fcid persistent	Displays persistent FC IDs (across reboot).
unused pending	Displays the pending configuration.
vsan vsan-id	Specifies a VSAN ID. The range is 1 to 4093.
pending-diff	Displays the difference between the running configuration and the pending configuration.
session-status	Displays the last action performed by FC domain.
statistics	Displays the statistics of FC domain.
interface	Specifies an interface.
fc *slot*/*port*	Specifies a Fibre Channel interface on a Cisco MDS 9000 Family Switch.
bay *port* | **ext** *port*	(Optional) Specifies a Fibre Channel interface on a Cisco MDS 9124 Fabric Switch, a Cisco Fabric Switch for HP c-Class BladeSystem, and a Cisco Fabric Switch for IBM BladeCenter.
fcip *fcip-id*	Specifies an FCIP interface. The range is 1 to 255.
iscsi *slot*/*port*	Specifies an iSCSI interface.
port-channel	Specifies a PortChannel interface. The range is 1 to 128.
status	Displays all VSAN-independent information in FC domain.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(3)	Added the Optimized mode: Disabled, in the command output.
1.0(2)	This command was introduced.
2.1(1a)	The domain-list display was modified to include a virtual IVR description.
3.0(1)	Added the **pending**, **pending-diff**, s**ession-status**, and **status** options.

Usage Guidelines

Entering the **show fcdomain** with no arguments displays all VSANs. The VSANs should be active or you will get an error.

Examples

The following example displays the fcdomain information for VSAN 1:

```
switch# show fcdomain vsan 1
The local switch is a Subordinated Switch.
Local switch run time information:
        State: Stable
        Local switch WWN:    20:01:00:05:30:00:51:1f
        Running fabric name: 10:00:00:60:69:22:32:91
        Running priority: 128
        Current domain ID: 0x64(100) ß verify domain id
Local switch configuration information:
        State: Enabled
        Auto-reconfiguration: Disabled
        Contiguous-allocation: Disabled
        Configured fabric name: 41:6e:64:69:61:6d:6f:21
  Optimize Mode: Disabled
        Configured priority: 128
        Configured domain ID: 0x64(100) (preferred)
Principal switch run time information:
        Running priority: 2
Interface               Role          RCF-reject
----------------    -------------    ------------
fc2/1               Downstream       Disabled
fc2/2               Downstream       Disabled
fc2/7               Upstream         Disabled
----------------    -------------    ------------
```

The following example displays the fcdomain domain-list information for VSAN 76:

```
switch# show fcdomain domain-list vsan 76
Number of domains: 3
Domain ID              WWN
---------    -----------------------
0xc8(200)    20:01:00:05:30:00:47:df [Principal]
 0x63(99)    20:01:00:0d:ec:08:60:c1 [Local]
 0x61(97)    50:00:53:0f:ff:f0:10:06 [Virtual (IVR)]
```

Table 5: show fcdomain Field Descriptions, on page 1276 describes the significant fields shown in the **show fcdomain domain-list** command output.

Table 5: show fcdomain Field Descriptions

Field	Description
Domain ID	Lists the domain IDs corresponding to the WWN.
WWN	Indicates the WWN of the switch (physical or virtual) that requested the corresponding domain ID.
Principal	Indicates which row of the display lists the WWN and domain ID of the principal switch in the VSAN.
Local	Indicates which row of the display lists the WWN and domain ID of the local switch (the switch where you entered the **show fcdomain domain-list** command).
Virtual (IVR)	Indicates which row of the display lists the WWN of the virtual switch used by the Inter-VSAN Routing (IVR) manager to obtain the domain ID.

The following example displays the allowed domain ID lists:

```
switch# show fcdomain
 allowed vsan 1
Assigned or unallowed domain IDs: 1-96,100,111-239.
[Interoperability Mode 1] allowed domain IDs: 97-127.
[User] configured allowed domain IDs: 50-110.
```

The following example shows the status of CFS distribution for allowed domain ID lists:

```
switch# show fcdomain status
CFS distribution is enabled
```

The following example displays pending configuration changes:

```
switch# show fcdomain pending vsan 10
Pending Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 1-9,24,100,231-239.
[User] configured allowed domain IDs: 10-230.
```

The following example displays the differences between the pending configuration and the current configuration:

```
switch# show fcdomain pending-diff vsan 10
Current Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 24,100.
[User] configured allowed domain IDs: 1-239.
Pending Configured Allowed Domains
---------------------------------
VSAN 10
Assigned or unallowed domain IDs: 1-9,24,100,231-239.
[User] configured allowed domain IDs: 10-230.
```

The following example displays the status of the distribution session:

```
switch# show fcdomain session-status vsan 1
```

```
Last Action: Distribution Enable
Result: Success
```

Related Commands

Command	Description
fcdomain	Configures the Fibre Channel domain feature.

show fcdroplatency

To display the configured Fibre Channel latency parameters, use the **show fcdroplatency** command.

show fcdroplatency [{**network**|**switch**}]

Syntax Description

network	(Optional) Network latency in milliseconds.
switch	(Optional) Switch latency in milliseconds.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the configured Fibre Channel latency parameters:

```
switch# show
fcdroplatency
switch latency value:4000 milliseconds
network latency value:5000 milliseconds
```

show fcflow stats

To display the configured Fibre Channel flow (fcflow) information, use the **show fcflow stats** command.

show fcflow stats [{**aggregated**|**usage**}] **module** *slot* [**index** *flow-index*]

Syntax Description

aggregated	(optional) Displays aggregated fcflow statistics.
usage	(optional) Displays flow index usage.
module slot	Displays fcflow statistics for a module in the specified slot.
index *flow-index*	(optional) Specifies an fcflow index.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays aggregated fcflow details for the specified module:

```
switch# show fcflow stats aggregated module 2
```

Idx VSAN # frames # bytes ---- ---- -------- ------- 0000 4 387,653 674,235,875 0001 6 34,402 2,896,628

The following example displays fcflow details for the specified module:

```
switch# show fcflow stats module 2
```

Idx VSAN D ID S ID mask # frames # bytes ---- ---- ----------- ----------- ----- -------- ------- 0000 4 032.001.002 007.081.012 ff.ff.ff 387,653 674,235,875 0001 6 004.002.001 019.002.004 ff.00.00 34,402 2,896,628

The following example displays fcflow index usage for the specified module:

```
switch# show fcflow stats usage module 2
2 flows configured
configured flow : 3,7
```

show fcfwd

To display the configured fcfwd tables and statistics, use the **show fcfwd** command.

show fcfwd {**idxmap** [{**interface-toport**|**port-to-interface**|**statistics**}]|**pcmap** **[interface]**|**sfib** [{**multicast**|**statistics**|**unicast**}]|**spanmap** [{**rx**|**tx**}]}

Syntax Description

idxmap	Displays the FC forward index tables.
interface-to-port	(Optional) Displays the interface index to port index table.
port-to-interface	(Optional) Displays the port index to interface index table.
statistics	(Optional) Displays index table statistics.
pcmap	Displays the FC forward PortChannel table.
interface	(Optional) Displays PortChannel tables for an interface.
sfib	Displays software forwarding tables.
multicast	(Optional) Displays multicast software forwarding tables.
statistics	(Optional) Displays software forwarding statistics.
unicast	(Optional) Displays unicast software forwarding tables.
spanmap	Displays SPAN map tables.
rx	(Optional) Displays SPAN map tables in the ingress -rx direction.
tx	(Optional) Displays SPAN map tables in the egress -tx direction.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays fcfwd SPAN map receive information:

```
switch# show fcfwd spanmap rx
SPAN source information: size [c8]
dir source               vsan   bit   drop_thresh destination
```

show fcid-allocation

Use the **show fcid allocation** command to display the Fibre Channel area list of company IDs.

show fcid-allocation area company-id [company-id]

Syntax Description

area	Selects the auto area list of company IDs.
company-id	Selects company ID list.
company-id	(Optional) Selects the individual company ID (also known as Organizational Unit Identifier, or OUI) to display.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0	New command

Examples

The following example shows the Fibre Channel area company list of company IDs:

```
switch# show fcid-allocation area company-id
Fcid area allocation company id info:
    00:50:2E
    00:50:8B
    00:60:B0
    00:A0:B8
    00:E0:69
    00:E0:8B
    00:32:23 +
Total company ids: 7
+ - Additional user configured company ids.
* - Explicitly deleted company ids from default list.
switch#
```

Table 6: show fcid-allocation area company Field Descriptions, on page 1281 describes the significant fields shown in the display.

Table 6: show fcid-allocation area company Field Descriptions

Field	Description
+	Indicates a company ID added to the default list.
–	Indicates a company ID deleted from the default list.

show fcip

To display FCIP profile information, use the show fcip command.

show fcip {**host-map** *fcip-id*|**profile** [{*profile-id*|**all**}]|**summary**|**tape-session** {**summary**|**tunnel** *tunnel-id* {**host-end**|**target-end**}}|**target-map** *fcip-id*|**wa-login-list** *tunnel-id*}

Syntax Description

host-map *fcip-id*	Displays the information for a specified map. The range is 1 to 255.
profile	Displays the information for a profile.
profile-id	(Optional) Specifies the profile ID. The range is 1 to 255.
all	(Optional) Specifies all profile IDs.
summary	Displays summary information.
tape-session	Displays tape session information.
tunnel *tunnel-id*	Displays information for a specified FCIP tunnel ID. The range is 1 to 255.
host-end	Displays information for the host end.
target-end	Displays information for the target end.
target-map *fcip-id*	Displays information for a specified target map. The range is 1 to 255.
wa-login-list *tunnel-id*	Displays the write acceleration login list for a specified FCIP tunnel ID. The range is 1 to 255.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(5)	Added the command output for FCIP Profiles for Cisco MDS 9250i Multiservice Fabric Switch.
1.1(1)	This command was introduced.
2.0(x)	Added the host-map , summary , and target-map keywords.
3.0(1)	Added the **tape-session**, **tunnel**, **host-end**, **target-end**, and **wa-login-list** keywords.

Usage Guidelines

None.

Examples

The following example displays FCIP Profiles for SSN-16/18+4

```
switch# show fcip profile
```

```
-------------------------------------------------------------------------------
ProfileId Ipaddr TcpPort
-------------------------------------------------------------------------------
1 10.10.100.150 3225
2 10.10.100.150 3226
40 40.1.1.2 3225
100 100.1.1.2 3225
200 200.1.1.2 3225
```

The following example displays FCIP Profiles for Cisco MDS 9250i Multiservice Fabric Switch:

```
switch# show fcip profile
-------------------------------------------------------------------------------
ProfileId Ipaddr TcpPort
-------------------------------------------------------------------------------
1 20.1.1.1 3225
2 20.1.1.1 2000
3 20.1.1.1 3000
4 20.1.1.1 4000
5 20.1.1.1 5000
6 20.1.1.1 6000
7 30.1.1.1 3225
8 31.1.1.1 3225
9 32.1.1.1 3225
10 33.1.1.1 3225
11 34.1.1.1 3225
12 35.1.1.1 3225
```

The following example displays all FCIP profiles:

```
switch# show fcip profile all
-----------------------------------------------------
ProfileId       Ipaddr          TcpPort
-----------------------------------------------------
1               41.1.1.2        3225
2               10.10.100.154   3225
3               43.1.1.2        3225
4               44.1.1.100      3225
6               46.1.1.2        3225
7               47.1.1.2        3225
```

The following example displays information for a specified FCIP profile for SSN-16/18+4:

```
switch# show fcip profile 7
FCIP Profile 7
    Internet Address is 47.1.1.2 (interface GigabitEthernet4/7)
    Listen Port is 3225
    TCP parameters
        SACK is disabled
        PMTU discovery is enabled, reset timeout is 3600 sec
        Keep alive is 60 sec
        Minimum retransmission timeout is 300 ms
        Maximum number of re-transmissions is 4
        Send buffer size is 0 KB
        Maximum allowed bandwidth is 1000000 kbps
        Minimum available bandwidth is 15000 kbps
        Estimated round trip time is 1000 usec
```

The following example displays information for the Specified FCIP Profile Information for Cisco MDS 9250i Multiservice Fabric Switch:

```
switch# show fcip profile 1
```

```
FCIP Profile 1
Internet Address is 20.1.1.1 (interface IPStorage1/1)
Tunnels Using this Profile: fcip1
Listen Port is 3225
TCP parameters
SACK is enabled
PMTU discovery is enabled, reset timeout is 3600 sec
Keep alive is 60 sec
Minimum retransmission timeout is 200 ms
Maximum number of re-transmissions is 4
Send buffer size is 16384 KB
Maximum allowed bandwidth is 5000000 kbps
Minimum available bandwidth is 4000000 kbps
Configured round trip time is 1000 usec
Congestion window monitoring is enabled, burst size is 50 KB
Auto jitter detection is enabled
```

The following example displays the FCIP Summary information (SSN-16/18+4):

```
switch# show fcip summary
--------------------------------------------------------------------------------
Tun prof Eth-if peer-ip Status T W T Enc Comp Bandwidth rtt
E A A max/min (us)
--------------------------------------------------------------------------------
10 91 GE4/1 3.3.3.2 UP N N N N N 1000M/1000M 2000
11 11 GE3/1.601 30.1.1.2 DOWN N N N N N 1000M/500M 1000
12 12 GE3/1.602 30.1.2.2 DOWN N N N N N 1000M/500M 1000
13 0 0.0.0.0 DOWN N N N N N
14 0 0.0.0.0 DOWN N N N N N
15 0 0.0.0.0 DOWN N N N N N
16 0 0.0.0.0 DOWN N N N N N
17 0 0.0.0.0 DOWN N N N N N
18 0 0.0.0.0 DOWN N N N N N
19 0 0.0.0.0 DOWN N N N N N
20 92 GE4/2 3.3.3.1 UP N N N N N 1000M/1000M 2000
21 21 GE3/2.601 30.1.1.1 DOWN N N N N N 1000M/500M 1000
22 22 GE3/2.602 30.1.2.1 DOWN N N N N N 1000M/500M 1000
```

The following example displays the FCIP Summary (Cisco MDS 9250i Multiservice Fabric Switch):

```
switch# show fcip summary
--------------------------------------------------------------------------------
Tun prof IPS-if peer-ip Status T W T Enc Comp Bandwidth rtt
E A A max/min (us)
--------------------------------------------------------------------------------
1 1 IPS1/1 20.1.1.2 TRNK Y N N N A 5000M/4000M 1000
2 2 IPS1/1 20.1.1.2 TRNK Y N N N A 1000M/800M 1000
3 3 IPS1/1 20.1.1.2 DOWN N N N N N 1000M/800M 1000
4 4 IPS1/1 20.1.1.2 DOWN N N N N N 1000M/800M 1000
5 5 IPS1/1 20.1.1.2 DOWN N N N N N 1000M/800M 1000
6 6 IPS1/1 20.1.1.2 DOWN N N N N N 1000M/800M 1000
7 7 IPS1/2.1 30.1.1.2 TRNK Y N N N M2 1000M/800M 1000
8 8 IPS1/2.2 31.1.1.2 TRNK Y N N N M2 1000M/800M 1000
9 9 IPS1/2.3 32.1.1.2 DOWN N N N N N 1000M/800M 1000
10 10 IPS1/2.4 33.1.1.2 DOWN N N N N N 1000M/800M 1000
11 11 IPS1/2.5 34.1.1.2 DOWN N N N N N 1000M/800M 1000
12 12 IPS1/2.6 35.1.1.2 DOWN N N N N N 1000M/800M 1000
```

Table 7: show fcip summary Field Descriptions, on page 1285 describes the significant fields shown in the previous display.

Table 7: show fcip summary Field Descriptions

Field	Description
Tun	Tunnel number for the row. For example, a number 1 indicates tunnel fcip1 and a number 2 indicates fcip2.
prof	Tunnel profile.
Eth-if	Ethernet interface to which this tunnel is bound.
peer-ip	IP address of the tunnel peer port on the far end of the tunnel.
Status	State of the tunnel (UP or DOWN).
TE	Tunnel operating in TE mode (**Y**es or **N**o).
WA	Write acceleration enabled (**Y**es or **N**o).
TA	Tape acceleration enabled (**Y**es or **N**o).
Enc	Encryption enabled (**Y**es or **N**o).
Bandwidth max/min	Maximum and minimum bandwidth configured in the profile to which this tunnel is bound.
rtt (us)	Round trip time (RTT) in microseconds.

Related Commands

Command	Description
fcip enable	Configures FCIP parameters.

show fcip counters

To display FCIP tunnel statistics, use the **show fcip counters** command in privileged EXEC mode. This command also displays the statistics for all TCP connections present in an FCIP tunnel.

show fcip counters

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
1.1(1)	This command was introduced.
6.2(11c)	This command was modified to display statistics for all TCP connections in an FCIP tunnel.

Usage Guidelines

None.

Examples

The following example shows statistics for an FCIP tunnel with 4 data and 1 control TCP connections:

```
switch# show fcip counters
fcip5
    TCP Connection Information
      5 Active TCP connections
        30 Attempts for active connections, 1 close of connections
        Path MTU 2500 bytes
        Current retransmission timeout is 200 ms
        Current Send Buffer Size: 66648 KB, Requested Send Buffer Size: 65536 KB
        CWM Burst Size: 50 KB
        Measured RTT : 500000 us Min RTT: 7640 us Max RTT: 0 us
        Round trip time: Smoothed 8 ms, Variance: 4 Jitter: 150 us
 CONN<0>
    Data connection: Local 10.10.9.1:65433, Remote 10.10.9.2:5000
    TCP Parameters
      Advertized window: Current: 1112 KB, Maximum: 24580 KB, Scale: 6
      Peer receive window: Current: 4095 KB, Maximum: 4095 KB, Scale: 6
      Congestion window: Current: 873 KB, Slow start threshold: 1840 KB
    TCP Connection Rate
      Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
      Input Frames: 0/sec, Output Frames: 0/sec
 CONN<1>
    Data connection: Local 10.10.9.1:65431, Remote 10.10.9.2:5000
    TCP Parameters
      Advertized window: Current: 1116 KB, Maximum: 24580 KB, Scale: 6
      Peer receive window: Current: 4095 KB, Maximum: 4095 KB, Scale: 6
      Congestion window: Current: 876 KB, Slow start threshold: 1842 KB
    TCP Connection Rate
      Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
      Input Frames: 0/sec, Output Frames: 0/sec
 CONN<2>
    Data connection: Local 10.10.9.1:65429, Remote 10.10.9.2:5000
```

```
    TCP Parameters
      Advertized window: Current: 1117 KB, Maximum: 24580 KB, Scale: 6
      Peer receive window: Current: 4095 KB, Maximum: 4095 KB, Scale: 6
      Congestion window: Current: 877 KB, Slow start threshold: 1842 KB
    TCP Connection Rate
      Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
      Input Frames: 0/sec, Output Frames: 0/sec
CONN<3>
    Data connection: Local 10.10.9.1:65427, Remote 10.10.9.2:5000
    TCP Parameters
      Advertized window: Current: 1118 KB, Maximum: 24580 KB, Scale: 6
      Peer receive window: Current: 4095 KB, Maximum: 4095 KB, Scale: 6
      Congestion window: Current: 878 KB, Slow start threshold: 1843 KB
    TCP Connection Rate
      Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
      Input Frames: 0/sec, Output Frames: 0/sec
CONN<4>
    Control connection: Local 10.10.9.1:65425, Remote 10.10.9.2:5000
    TCP Parameters
      Advertized window: Current: 1107 KB, Maximum: 24580 KB, Scale: 6
      Peer receive window: Current: 4089 KB, Maximum: 4089 KB, Scale: 6
      Congestion window: Current: 50 KB, Slow start threshold: 2070 KB
    TCP Connection Rate
      Input Bytes: 0.00 MB/sec, Output Bytes: 0.00 MB/sec
      Input Frames: 0/sec, Output Frames: 0/sec
    5 minutes input rate 120 bits/sec, 15 bytes/sec, 0 frames/sec
    5 minutes output rate 160 bits/sec, 20 bytes/sec, 0 frames/sec
      1060823 frames input, 2307076112 bytes
         4675 Class F frames input, 448880 bytes
         1056148 Class 2/3 frames input, 2306627232 bytes
         0 Reass frames
         0 Error frames timestamp error 0
      2788188 frames output, 6079611624 bytes
         4691 Class F frames output, 454176 bytes
         2783497 Class 2/3 frames output, 6079157448 bytes
0 Error frames
```

Related Commands

Command	Description
show fcip	Displays FCIP profile information.
show ips stats	Displays IP storage statistics.

show fc-management

To display the Fibre Channel Common Transport (FC-CT) management security information, use the show fc-management command.

{**show fc-management database**|**status**}

Syntax Description

database	Displays the FC-CT management security database.
status	Displays the management security information.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(9)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to display the FC-CT management security database:

```
switch(config)# show fc-management database
Fc-Management Security Database
---------------------------------------------------------------
VSAN       PWWN              FC-CT Permissions per FC services
---------------------------------------------------------------
1    01:01:01:01:01:01:01:01   Zone(RW), Unzoned-NS(RW), FCS(RW), FDMI(RW)
---------------------------------------------------------------
Total 1 entries
switch(config)#
```

The following example shows how to display the management security information**:**

```
switch(config)# show fc-management status
Mgmt Security Enabled
switch(config)#
```

Related Commands

Command	Description
fc-management database	Configures the FC-CT management security database.

show fcns database

To display the results of the discovery, or to display the name server database for a specified VSAN or for all VSANs, use the **show fcns database** command.

show fcns database {**detail** [**vsan vsan-id**]|**domain domain-id [detail]** [**vsan vsan-range**]|**fcid fcid-id [detail] vsan vsan-range**|**local [detail]** [**vsan vsan-range**]|**vsan vsan-id**}

Syntax Description

detail	Displays all objects in each entry.
vsan vsan-id	(Optional) Displays entries for a specified VSAN ID. The range is 1 to 4093.
domain domain-id	Displays entries in a domain.
vsan vsan-range	Displays the VSAN range. The range is 1 to 4093.
fcid fcid-id	Displays entry for the given port.
local	Displays local entries.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.2(1)	Changed the command output for show fcns database and show fcns database detail. (Two attributes are added to the command output Connected Interface :fc3/4 Switch Name (IP address) :rbadri-vegas11 (10.64.66.50)
NX-OS 4.1(3)	Changed the command output for show fcns database detail.
1.2(2)	This command was introduced.

Usage Guidelines

The discovery can take several minutes to complete, especially if the fabric is large or if several devices are slow to respond.

Virtual enclosure ports can be viewed using the **show fcns database** command.

Examples

The following example displays the contents of the FCNS database:

```
switch# show fcns database
VSAN 1:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x460100    N     10:00:00:00:c9:32:89:e6 (Emulex)        scsi-fcp:init
0x460200    N     21:00:00:e0:8b:09:4e:d3 (Qlogic)        scsi-fcp:init
0x460300    N     21:01:00:e0:8b:29:4e:d3 (Qlogic)        scsi-fcp:init
0x460423    NL    21:00:00:04:cf:cf:45:ba (Seagate)       scsi-fcp
```

```
Total number of entries = 4
VSAN 2:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x8e0000    N     21:01:00:e0:8b:2e:85:8a (Qlogic)        scsi-fcp:init
0x9509b5    N     50:00:53:00:00:6b:30:02 (Cisco)         scsi-fcp:init sdv
Total number of entries = 2
```

The following example displays the detailed contents of the FCNS database:

```
switch# show fcns database detail
------------------------
VSAN:1     FCID:0x460100
------------------------
port-wwn (vendor)                  :10:00:00:00:c9:32:89:e6 (Emulex)
node-wwn                                :20:00:00:00:c9:32:89:e6
class                                   :2,3
node-ip-addr                           :0.0.0.0
ipa                                     :ff ff ff ff ff ff ff ff
fc4-types:fc4_features        :scsi-fcp:init
symbolic-port-name                   :
symbolic-node-name                  :Emulex LP9002 FV3.90A7 DV8.0.16.34
port-type                                 :N
port-ip-addr                            :0.0.0.0
fabric-port-wwn                       :20:85:00:05:30:00:4a:de
hard-addr                                :0x000000
permanent-port-wwn (vendor) :10:00:00:00:c9:32:89:e6 (Emulex)
Connected Interface            :fc3/5
Switch Name (IP address)      :rbadri-vegas11 (10.64.66.50)
------------------------
VSAN:1     FCID:0x460200
------------------------
port-wwn (vendor)             :21:00:00:e0:8b:09:4e:d3 (Qlogic)
node-wwn                      :20:00:00:e0:8b:09:4e:d3
class                          :3
node-ip-addr                  :0.0.0.0
ipa                            :ff ff ff ff ff ff ff ff
fc4-types:fc4_features        :scsi-fcp:init
symbolic-port-name             :
symbolic-node-name               :
port-type                                 :N
port-ip-addr                            :0.0.0.0
fabric-port-wwn                       :20:84:00:05:30:00:4a:de
hard-addr                                :0x000000
permanent-port-wwn (vendor) :21:00:00:e0:8b:09:4e:d3 (Qlogic)
Connected Interface            :fc3/4
Switch Name (IP address)      :rbadri-vegas11 (10.64.66.50)
------------------------
VSAN:1     FCID:0x460300
------------------------
port-wwn (vendor)             :21:01:00:e0:8b:29:4e:d3 (Qlogic)
node-wwn                      :20:01:00:e0:8b:29:4e:d3
class                          :3
node-ip-addr                  :0.0.0.0
ipa                            :ff ff ff ff ff ff ff ff
fc4-types:fc4_features        :scsi-fcp:init
symbolic-port-name            :
symbolic-node-name            :
port-type                      :N
port-ip-addr                   :0.0.0.0
fabric-port-wwn               :20:8d:00:05:30:00:4a:de
hard-addr                      :0x000000
permanent-port-wwn (vendor) :21:01:00:e0:8b:29:4e:d3 (Qlogic)
```

```
Connected Interface              :fc3/13
Switch Name (IP address)       :rbadri-vegas11 (10.64.66.50)
------------------------
VSAN:1     FCID:0x460423
------------------------
port-wwn (vendor)             :21:00:00:04:cf:cf:45:ba (Seagate)
node-wwn                      :20:00:00:04:cf:cf:45:ba
class                          :3
node-ip-addr                  :0.0.0.0
ipa                            :ff ff ff ff ff ff ff ff
fc4-types:fc4_features        :scsi-fcp
symbolic-port-name            :
symbolic-node-name            :
port-type                      :NL
port-ip-addr                   :0.0.0.0
fabric-port-wwn               :20:81:00:05:30:00:4a:de
hard-addr                      :0x000000
permanent-port-wwn (vendor) :00:00:00:00:00:00:00:00
Connected Interface                 :fc3/1
Switch Name (IP address)       :rbadri-vegas11 (10.64.66.50)
Total number of entries = 4
==============================================================
```

The following example shows how to display the output for the virtual devices.

```
------------------------
VSAN:2     FCID:0x9509b5
------------------------
port-wwn (vendor)               :50:00:53:00:00:6b:30:02 (Cisco)
node-wwn                            :50:00:53:00:00:6b:30:02
class                                 :-
node-ip-addr                        :0.0.0.0
ipa                                   :ff ff ff ff ff ff ff ff
fc4-types:fc4_features         :scsi-fcp:init sdv
symbolic-port-name                :
symbolic-node-name               :
port-type                                 :N
port-ip-addr                              :0.0.0.0
fabric-port-wwn                       :20:0e:00:0d:ec:25:ef:00
hard-addr                        :0x000000
permanent-port-wwn (vendor) :00:00:00:00:00:00:00:00
Connected Interface               :Virtual Device
Switch Name (IP address)     :Not Available
Total number of entries = 2
```

The following example shows how to display the output for a non-cisco switches:

```
switch# show fcns database detail
------------------------
VSAN:1     FCID:0x6600e2
------------------------
port-wwn (vendor)                 :21:00:00:0c:50:02:c6:f7 (Seagate)
node-wwn                               :20:00:00:0c:50:02:c6:f7
class                                        :3
node-ip-addr                           :0.0.0.0
ipa                                          :ff ff ff ff ff ff ff ff
fc4-types:fc4_features            :scsi-fcp
symbolic-port-name               :
symbolic-node-name              :
port-type                       :NL
port-ip-addr                    :0.0.0.0
fabric-port-wwn                :20:02:00:0d:ec:11:d4:82
hard-addr                                 :0x000000
```

```
permanent-port-wwn (vendor) :00:00:00:00:00:00:00:00
Connected to                           :fc1/2
Switch Name (IP address)        :rbadri-paradise1 (10.64.66.58)
------------------------
VSAN:1     FCID:0x6b0f23
------------------------
port-wwn (vendor)                    :21:00:00:04:cf:cf:45:50 (Seagate)
node-wwn                                 :20:00:00:04:cf:cf:45:50
class                                          :3
node-ip-addr                             :0.0.0.0
ipa                                             :ff ff ff ff ff ff ff ff
fc4-types:fc4_features              :scsi-fcp
symbolic-port-name                 :SEAGATE ST336753FC      0005
symbolic-node-name                :
port-type                                    :NL
port-ip-addr                              :0.0.0.0
fabric-port-wwn                        :20:0f:00:60:69:80:62:4a
hard-addr                          :0x000000
permanent-port-wwn (vendor) :00:00:00:00:00:00:00:00
Connected to                            :Non-Cisco Switch
Switch Name (IP address)     :bs11 (10.64.66.57)
```

Related Commands

Command	Description
asm mgmt-vsan	Displays the CPP interface configuration for a specified interface.

show fcns statistics

To display the statistical information for a specified VSAN or for all VSANs, use the **show fcns statistics** command.

show fcns statistics [detail] [vsan vsan-id]

Syntax Description

detail	(Optional) Displays detailed statistics.
vsan vsan-id	(Optional) Displays statistics for the specified VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays statistical information for a specified VSAN:

```
switch# show fcns statistics

registration requests received = 27
deregistration requests received = 0
queries received = 57
queries sent = 10
reject responses sent = 14
RSCNs received = 0
RSCNs sent = 0
switch#
```

show fc-redirect active-configs

To display all active configurations on a switch, use the show fc-redirect active-configs command.

show fc-redirect active-configs

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

This command is used to verify that there are no active configurations running on the switch during the following operations:

- Downgrading from 3.2.1 image (supporting FC-Redirect) to an older image where FC-Redirect is not supported.
- Decommissioning a local switch.

Note Active configuration implies configurations created by applications running on the current switch or applications created on remote switches for hosts or targets connected to the local switch.

Examples

The following example displays the active configurations running on the switch:

```
switch# show fc-redirect active-configs
Config#1
==========
Appl UUID       = 0x00D8 (ISAPI CFGD Service)
SSM Slot        = 2
SSM Switch WWN  = 20:00:00:05:30:00:90:9e (LOCAL)
Vt PWWN         = 2f:ea:00:05:30:00:71:64
Tgt PWWN        = 21:00:00:20:37:38:63:9e (LOCAL)
Local Host PWWN = 21:00:00:e0:8B:0d:12:c6
Config#2
==========
Appl UUID       = 0x00D8 (ISAPI CFGD Service)
SSM Slot        = 2
SSM Switch WWN  = 20:00:00:05:30:00:90:9e (LOCAL)
Vt PWWN         = 2f:ea:00:05:30:00:71:65
Tgt PWWN        = 21:00:00:20:37:18:67:2c
Local Host PWWN = 21:00:00:e0:8B:0d:12:c6
Config#3
==========
Appl UUID       = 0x00D8 (ISAPI CFGD Service)
SSM Slot        = 2
SSM Switch WWN  = 20:00:00:0d:EC:20:13:00 (REMOTE)
```

```
Vt PWWN         = 2f:ea:00:05:30:00:71:66
Tgt PWWN        = 21:00:00:20:37:18:64:92
Local Host PWWN = 21:00:00:e0:8B:0d:12:c6
```

Related Commands

Command	Description
clear fc-redirect config vt	Clears the active configurations on the local switch.

show fc-redirect configs

To display all the current configuration mode on a switch, use the show fc-redirect configs command.

show fc-redirect configs

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
3.2(1)	This command was introduced.
3.3(1a)	Added the configuration mode information to the command output.

Usage Guidelines

None.

Examples

The following example displays the current configuration mode on a switch :

```
switch# show fc-redirect configs
Configuration Mode    = MODE_V1
Config#1
==========
Appl UUID          = 0x00D8 (ISAPI CFGD Service)
SSM Slot           = 2
SSM Switch WWN     = 20:00:00:05:30:00:90:9e (LOCAL)
Vt PWWN            = 2f:ea:00:05:30:00:71:61
Tgt PWWN           = 21:00:00:20:37:38:89:86
Host  1: Host PWWN = 21:00:00:e0:8b:0d:12:c6
         VI   PWWN = 2f:ec:00:05:30:00:71:61
Config#2
==========
Appl UUID          = 0x00D8 (ISAPI CFGD Service)
SSM Slot           = 2
SSM Switch WWN     = 20:00:00:05:30:00:90:9e (LOCAL)
Vt PWWN            = 2f:ea:00:05:30:00:71:62
Tgt PWWN           = 21:00:00:20:37:38:a9:0a
Host  1: Host PWWN = 21:00:00:e0:8b:0d:12:c7
         VI   PWWN = 2f:ec:00:05:30:00:71:62
```

Related Commands

Command	Description
show fc-redirect active-configs	Displays all active configurations on a switch.

show fc-redirect peer-switches

To display all the peer switches in the fabric running FC-Redirect, use the show fc-redirect peer-switches command.

show fc-redirect peer-switches

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
3.2(1)	This command was introduced.
3.3(1a)	Added the FC-Redirect version of the switch and configuration mode to the command output.

Usage Guidelines

This command is used to verify the fabric state and is used for troubleshooting.

Note To find the switch IP address for the list of switch WWNs, use the show cfs peers command.

Examples

The following example displays the peer switches in the fabric running FC-Redirect:

```
switch# show fc-redirect peer-switches
------------------------------------------------------------------
 num  Switch WWN                  State  FCR-Ver Cfg-Mode
------------------------------------------------------------------
   1  20:00:00:0d:EC:20:13:00     UP      2       V2
```

Table 8: Show FC-Redirect Peer Switch States, on page 1297 lists the output for the show fc-redirect peer-switches command states.

Table 8: Show FC-Redirect Peer Switch States

State	Description
Up	The peer switch is fully synchronized with the local switch.
Down	The communication with the peer switch is not available.
Syncing	The local switch is synchronizing its configuration with the peer switch.
Error	Connection with peer switch is not available.

Related Commands

Command	Description
show fc-redirect active-configs	Displays all active configurations on a switch.

show fcroute

To view specific information about existing Fibre Channel and FSPF configurations, Use the **show fcroute** command.

show fcroute {**distance**|**label [label] vsan vsan-id**|**multicast** [{**fc-id vsan vsan-id**|**vsan vsan-id**}]|**summary** [**vsan vsan-id**]|**unicast** [{**[host] fc-id fc-mask vsan vsan-id**|**vsan vsan-id**}]}

Syntax Description

distance	Displays FC route preference.
label label	Displays label routes.
vsan vsan-id	Specifies the ID of the VSAN (from 1 to 4093).
multicast	Displays FC multicast routes.
fc-id	Specifies the Fibre Channel ID.
summary	Displays the FC routes summary.
unicast	Displays FC unicast routes.
vsan vsan-id	Specifies the ID of the VSAN (from 1 to 4093).

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

When the number of routes are displayed in the command output, both visible and hidden routes are included in the total number of routes.

Examples

The following example displays administrative distance:

```
switch# show fcroute distance
        Route
UUID    Distance        Name
----    --------        ----
10      20              RIB
22      40              FCDOMAIN
39      80              RIB-CONFIG
12      100             FSPF
17      120             FLOGI
21      140             TLPM
```

```
14      180             MCAST
64      200             RIB-TEST
```

The following example displays multicast routing information:

```
switch# show fcroute multicast
VSAN FC ID    # Interfaces
---- -------- ------------
1    0xffffff 0
2    0xffffff 1
3    0xffffff 1
4    0xffffff 0
5    0xffffff 0
6    0xffffff 0
7    0xffffff 0
8    0xffffff 0
9    0xffffff 0
10   0xffffff 0
```

The following example displays FCID information for a specified VSAN:

```
switch# show fcroute multicast vsan 3
VSAN FC ID    # Interfaces
---- -------- ------------
3    0xffffff 1
```

The following example displays FCID and interface information for a specified VSAN:

```
switch# show fcroute multicast 0xffffff vsan 2
VSAN FC ID    # Interfaces
---- -------- ------------
2    0xffffff 1
  fc1/1
```

The following example displays unicast routing information:

```
switch# show fcroute unicast
D:direct R:remote P:permanent V:volatile A:active N:non-active
                                                  # Next
Protocol VSAN    FC ID/Mask     RCtl/Mask Flags Hops   Cost
-------- ---- -------- -------- ---- ---- ----- ------ ----
static   1    0x010101 0xffffff 0x00 0x00 D P A 1      10
static   2    0x111211 0xffffff 0x00 0x00 R P A 1      10
fspf     2    0x730000 0xff0000 0x00 0x00 D P A 4      500
fspf     3    0x610000 0xff0000 0x00 0x00 D P A 4      500
static   4    0x040101 0xffffff 0x00 0x00 R P A 1      103
static   4    0x040102 0xffffff 0x00 0x00 R P A 1      103
static   4    0x040103 0xffffff 0x00 0x00 R P A 1      103
static   4    0x040104 0xffffff 0x00 0x00 R P A 1      103
static   4    0x111211 0xffffff 0x00 0x00 D P A 1      10
```

The following example displays unicast routing information for a specified VSAN:

```
switch# show fcroute unicast vsan 4
D:direct R:remote P:permanent V:volatile A:active N:non-active
                                                  # Next
Protocol VSAN    FC ID/Mask     RCtl/Mask Flags Hops   Cost
-------- ---- -------- -------- ---- ---- ----- ------ ----
static   4    0x040101 0xffffff 0x00 0x00 R P A 1      103
static   4    0x040102 0xffffff 0x00 0x00 R P A 1      103
static   4    0x040103 0xffffff 0x00 0x00 R P A 1      103
```

```
static   4    0x040104 0xffffff 0x00 0x00 R P A 1      103
static   4    0x111211 0xffffff 0x00 0x00 D P A 1      10
```

The following example displays unicast routing information for a specified FCID:

```
switch# show fcroute unicast 0x040101 0xffffff vsan 4
D:direct R:remote P:permanent V:volatile A:active N:non-active
                                                  # Next
Protocol VSAN    FC ID/Mask     RCtl/Mask Flags Hops   Cost
-------- ---- -------- -------- ---- ---- ----- ------ ----
static   4    0x040101 0xffffff 0x00 0x00 R P A 1      103
  fc1/2 Domain 0xa6(166)
```

The following example displays route database information:

```
switch# show fcroute summary
FC route database created Tue Oct 29 01:24:23 2002
VSAN    Ucast   Mcast   Label   Last Modified Time
----    -----   -----   -----   ------------------
1       2       1       0       Tue Oct 29 18:07:02 2002
2       3       1       0       Tue Oct 29 18:33:24 2002
3       2       1       0       Tue Oct 29 18:10:07 2002
4       6       1       0       Tue Oct 29 18:31:16 2002
5       1       1       0       Tue Oct 29 01:34:39 2002
6       1       1       0       Tue Oct 29 01:34:39 2002
7       1       1       0       Tue Oct 29 01:34:39 2002
8       1       1       0       Tue Oct 29 01:34:39 2002
9       1       1       0       Tue Oct 29 01:34:39 2002
10      1       1       0       Tue Oct 29 01:34:39 2002
Total   19      10      0
```

The following example displays route database information for a specified VSAN:

```
switch# show fcroute summary
vsan 4
FC route database created Tue Oct 29 01:24:23 2002
VSAN    Ucast   Mcast   Label   Last Modified Time
----    -----   -----   -----   ------------------
4       6       1       0       Tue Oct 29 18:31:16 2002
Total   6       1       0
```

show fcroute-map

To display the preferred path route map configuration and status, use the **show fcroute-map** command.

show *fcroute-map* [*vsan vsan-id route-map-identifier*]

Syntax Description

vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
route-map-identifier	Specifies the route map identifier. The range is 1 to 65535.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(3)	This command was introduced.

Usage Guidelines

Use this command to display the preferred path route map configuration and status before and after activation.

Examples

The following example displays the fcroute map output before preferred path route map activation.

```
switch# show fcroute-map
Fcroute Map: Vsan 2 Route ID: 12 [Status: Pending]
Match Criteria
==============
Source FCID Source FCID Mask Dest FCID     Dest FCID Mask    Status
----------- ---------------- --------- -------------- --------------
0x123456    0xffffff         0x567890      0xffffff          Pending
Set Criteria
============
Preference select strict: Yes (Operational: Yes)
Preference Level Interface IVR Nexthop Vsan Status
---------------- --------------- ------------------
   1              fc8/1 --                  Pending
   5              fc8/2 3                   Pending
```

The following example displays the fcroute map output after preferred path route map activation.

```
switch# show fcroute-map
Fcroute Map: Vsan 2 Route ID: 12 [Status: Active]
Match Criteria
==============
Source FCID Source FCID Mask Dest FCID     Dest FCID Mask    Status
----------- ---------------- --------- -------------- -------------
0x123456    0xffffff         0x567890      0xffffff          Active
Set Criteria
============
Preference select strict: Yes (Operational: Yes)
Preference Level Interface IVR Nexthop Vsan Status
---------------- --------------- -----------------
```

```
1             fc8/1 --                  Active*
5             fc8/2 3                   Active
```

Note The asterisk (*) indicates the currently active path.

show fcs

To display the status of the fabric configuration, Use the **show fcs** commands.

show *fcroute-map* [*vsan vsan-id route-map-identifier*]

Syntax Description

database	Displays local database of FCS.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
ie	Displays Interconnect Element objects information.
nwwn *wwn*	(Optional) Specifies a node WWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is 1 to 4093.
platform	Displays Platform Objects Information.
name *string*	(Optional) Specifies a platform name. Maximum length is 255 characters.
port	Displays Port Objects Information.
pwwn *wwn*	(Optional) Specifies a port WWN id. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
statistics	Displays statistics for FCS packets.
vsan	Displays list of all the VSANs and plat-check-mode for each.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays FCS database information:

```
switch# show fcs database
FCS Local Database in VSAN: 1
------------------------------
Switch WWN               : 20:01:00:05:30:00:16:df
Switch Domain Id         : 0x7f(127)
Switch Mgmt-Addresses    : snmp://172.22.92.58/eth-ip
                           http://172.22.92.58/eth-ip
Fabric-Name              : 20:01:00:05:30:00:16:df
```

```
Switch Logical-Name      : 172.22.92.58
Switch Information List  : [Cisco Systems*DS-C9509*0*20:00:00:05:30:00
Switch Ports:
-------------------------------------------------------------------
Interface  pWWN                      Type     Attached-pWWNs
-------------------------------------------------------------------
fc2/1      20:41:00:05:30:00:16:de  TE       20:01:00:05:30:00:20:de
fc2/2      20:42:00:05:30:00:16:de  Unknown  None
fc2/17     20:51:00:05:30:00:16:de  TE       20:0a:00:05:30:00:20:de
FCS Local Database in VSAN: 5
------------------------------
Switch WWN               : 20:05:00:05:30:00:12:5f
Switch Domain Id         : 0xef(239)
Switch Mgmt-Addresses    : http://172.22.90.171/eth-ip
                           snmp://172.22.90.171/eth-ip
                           http://10.10.15.10/vsan-ip
                           snmp://10.10.15.10/vsan-ip
Fabric-Name              : 20:05:00:05:30:00:12:5f
Switch Logical-Name      : 172.22.90.171
Switch Information List  : [Cisco Systems*DS-C9509**20:00:00:05:30:00:12:5e]
Switch Ports:
-------------------------------------------------------------------
Interface  pWWN                      Type     Attached-pWWNs
-------------------------------------------------------------------
fc3/1      20:81:00:05:30:00:12:5e  TE       22:01:00:05:30:00:12:9e
fc3/2      20:82:00:05:30:00:12:5e  TE       22:02:00:05:30:00:12:9e
fc3/3      20:83:00:05:30:00:12:5e  TE       22:03:00:05:30:00:12:9e
```

The following example displays Interconnect Element object information for a specific VSAN:

```
switch# show fcs ie vsan  1
IE List for VSAN: 1
-------------------------------------------------------------------
IE-WWN                   IE-Type                          Mgmt-Id
-------------------------------------------------------------------
20:01:00:05:30:00:16:df  Switch (Local)                    0xfffc7f
20:01:00:05:30:00:20:df  Switch (Adjacent)                 0xfffc64
[Total 2 IEs in Fabric]
```

This command displays Interconnect Element object information for a specific WWN:

```
switch# show fcs ie nwwn 20:01:00:05:30:00:16:df vsan 1
IE Attributes
-------------
Domain-Id = 0x7f(127)
Management-Id = 0xfffc7f
Fabric-Name = 20:01:00:05:30:00:16:df
Logical-Name = 172.22.92.58
Management Address List =
        snmp://172.22.92.58/eth-ip
        http://172.22.92.58/eth-ip
Information List:
        Vendor-Name = Cisco Systems
        Model Name/Number = DS-C9509
        Release-Code = 0
```

This command displays platform information:

```
switch# show fcs platform name SamplePlatform vsan 1
Platform Attributes
-------------------
Platform Node Names:
        11:22:33:44:55:66:77:88
```

```
Platform Type = Gateway
Platform Management Addresses:
        1.1.1.1
```

This command displays platform information within a specified VSAN:

```
switch# show fcs platform vsan 1
Platform List for VSAN: 1
Platform-Names
--------------
SamplePlatform
[Total 1 Platforms in Fabric]
```

This command displays FCS port information within a specified VSAN:

```
switch# show fcs port vsan 24
Port List in VSAN: 24
                -- IE WWN: 20:18:00:05:30:00:16:df  --
------------------------------------------------------------------------
Port-WWN                 Type      Module-Type            Tx-Type
------------------------------------------------------------------------
20:41:00:05:30:00:16:de  TE_Port   SFP with Serial Id      Shortwave Laser
20:51:00:05:30:00:16:de  TE_Port   SFP with Serial Id      Shortwave Laser
[Total 2 switch-ports in IE]
                -- IE WWN: 20:18:00:05:30:00:20:df  --
------------------------------------------------------------------------
Port-WWN                 Type      Module-Type            Tx-Type
------------------------------------------------------------------------
20:01:00:05:30:00:20:de  TE_Port   SFP with Serial Id      Shortwave Laser
20:0a:00:05:30:00:20:de  TE_Port   SFP with Serial Id      Shortwave Laser
[Total 2 switch-ports in IE]
```

This command displays ports within a specified WWN:

```
switch# show fcs port pwwn 20:51:00:05:30:00:16:de vsan 24
Port Attributes
---------------
Port Type = TE_Port
Port Number = 0x1090000
Attached-Port-WWNs:
        20:0a:00:05:30:00:20:de
Port State = Online
```

This command displays FCS statistics:

```
switch# show fcs statistics
FCS Statistics for VSAN: 1
--------------------------
FCS Rx Get Reqs   :2
FCS Tx Get Reqs   :7
FCS Rx Reg Reqs   :0
FCS Tx Reg Reqs   :0
FCS Rx Dereg Reqs :0
FCS Tx Dereg Reqs :0
FCS Rx RSCNs      :0
FCS Tx RSCNs      :3
FCS Rx RJTs       :3
FCS Tx RJTs       :0
FCS Rx ACCs       :4
FCS Tx ACCs       :2
FCS No Response   :0
FCS Retransmit    :0
```

```
FCS Statistics for VSAN: 30
---------------------------
FCS Rx Get Reqs   :2
FCS Tx Get Reqs   :2
FCS Rx Reg Reqs   :0
FCS Tx Reg Reqs   :0
FCS Rx Dereg Reqs :0
FCS Tx Dereg Reqs :0
FCS Rx RSCNs      :0
FCS Tx RSCNs      :0
FCS Rx RJTs       :0
FCS Tx RJTs       :0
FCS Rx ACCs       :2
FCS Tx ACCs       :2
FCS No Response   :0
FCS Retransmit    :0
```

show fcsp

To display the status of the Fibre Channel Security Protocol (FC-SP) configuration, use the **show fcsp** command.

show fcs p [{**asciiwwn** *ascii-wwn*|**dhchap [database]**|**interface fc** *slot/port* [{**statistics**|**wwn**}]|**fcip** *interface-number* [{**statistics**|**wwn**}]}]

Syntax Description

asciiwwn *ascii-wwn*	(Optional) Displays the ASCII representation of the WWN used with AAA server.
dhchap	(Optional) Displays the DHCHAP hash algorithm status.
database	(Optional) Displays the contents of the local DHCHAP database.
interface	(Optional) Displays the FC-SP settings for a FC or FCIP interface.
fc *slot/port*	(Optional) Displays the Fibre Channel interface in the specified slot and port.
statistics	(Optional) Displays the statistics for the specified interface.
wwn	(Optional) Displays the FC-SP identity of the other device.
fcip *interface-number*	(Optional) Displays the description of the specified FCIP interface. The range is 1 to 255.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays DHCHAP configurations in FC interfaces:

```
switch# show fcsp interface fc1/9

fc1/9:
        fcsp authentication mode:SEC_MODE_ON
        Status: Successfully authenticated
```

The following example displays DHCHAP statistics for a FC interfaces:

```
switch# show fcsp interface fc1/9 statistics

fc1/9:
        fcsp authentication mode:SEC_MODE_ON
        Status: Successfully authenticated
        Statistics:
```

```
        FC-SP Authentication Succeeded:5
        FC-SP Authentication Failed:0
        FC-SP Authentication Bypassed:0
```

The following example displays the FC-SP WWN of the device connected through a specified interface:

```
switch# show fcsp interface fc 2/1 wwn
fc2/1:
        fcsp authentication mode:SEC_MODE_ON
        Status: Successfully authenticated
        Other device's WWN:20:00:00:e0:8b:0a:5d:e7
```

The following example displays hash algorithm and DHCHAP groups configured for the local switch:

```
switch# show fcsp dhchap
Supported Hash algorithms (in order of preference):
DHCHAP_HASH_MD5
DHCHAP_HASH_SHA_1
Supported Diffie Hellman group ids (in order of preference):
DHCHAP_GROUP_NULL
DHCHAP_GROUP_1536
DHCHAP_GROUP_1024
DHCHAP_GROUP_1280
DHCHAP_GROUP_2048
```

The following example displays the DHCHAP local password database:

```
switch# show fcsp dhchap database
DHCHAP Local Password:
        Non-device specific password:********
        Password for device with WWN:29:11:bb:cc:dd:33:11:22 is ********
        Password for device with WWN:30:11:bb:cc:dd:33:11:22 is ********
Other Devices' Passwords:
        Password for device with WWN:00:11:22:33:44:aa:bb:cc is ********
```

The following example displays he ASCII representation of the device WWN:

```
switch# show fcsp asciiwwn 30:11:bb:cc:dd:33:11:22
Ascii representation of WWN to be used with AAA servers:Ox_3011bbccdd331122
```

Related Commands

Command	Description
fcsp enable	Enables the FC-SP feature for this switch.

show fcsp interface

To display the FC-SP- related information for a specific interface, use the show fcsp interface command.

show fcsp interface {**fc** *slot*/*port*|**fcip** *slot*/*port*}

Syntax Description

fc slot/port	Specifies FC slot number and port number.
fcip slot/port	Specifies FCIP slot number and port number.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the FC-SP related information for a specific interface:

```
switch# show fcsp interface fc7/41
fc7/41:
fcsp authentication mode:SEC_MODE_OFF
ESP is enabled
configured mode is: GCM
programmed ingress SA: 300, 303
programmed egress SA: 300
Status:FC-SP protocol in progress
```

Related Commands

Command	Description
fcsp enable	Enables FC-SP.

show fctimer

To view the Fibre Channel timers (fctimer), use the **show fctimer** command.

show fctimer [{**d_s_tov** [**vsan vsan-id**]|**distribution status**|**e_d_tov** [**vsan vsan-id**]|**f_s_tov** [**vsan vsan-id**]|**last action status**|**pending**|**pending-diff**|**r_a_tov** [**vsan vsan-id**]|**session-status**|[**vsan** *vsan-id*]}]

Syntax Description

d_s_tov	(Optional) Displays the distributed services time out value (D_S_TOV) in milliseconds.
vsan *vsan-id*	(Optional) Displays information for a VSAN. The range is 1 to 4093.
distribution status	(Optional) Displays Cisco Fabric Services (CFS) distribution status information.
e_d_tov	(Optional) Displays the error detection time out value (E_D_TOV) in milliseconds.
f_s_tov	(Optional) Displays the fabric stability time out value (F_S_TOV) in milliseconds.
last action status	(Optional) Displays the status of the last CFS commit or discard operation.
pending	(Optional) Displays the status of pending fctimer commands.
pending-diff	(Optional) Displays the difference between pending database and running config.
r_a_tov	(Optional) Displays the resource allocation time out value (R_A_TOV) in milliseconds.
session-status	(Optional) Displays the state of fctimer CFS session.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(x)	Added the distribution status , last action status , pending , pending-diff , and session-status keywords.

Usage Guidelines

None.

Examples

The following example displays configured global TOVs:

```
switch# show fctimer
F_S_TOV   D_S_TOV   E_D_TOV   R_A_TOV
---------------------------------------:
5000 ms   5000 ms   2000 ms   10000 ms
```

The following example displays configured TOVs for a specified VSAN:

```
switch# show fctimer vsan 10
vsan no.  F_S_TOV   D_S_TOV   E_D_TOV   R_A_TOV
-------------------------------------------------
10        5000 ms   5000 ms   3000 ms   10000 ms
```

Related Commands

Command	Description
fctimer	Configures fctimer parameters.

show fc-tunnel

To display configured Fibre Channel tunnel information, use the **show fc-tunnel** command.

show fc-tunnel [{**explicit-path** [*name*]|**tunnel-id-map**}]

Syntax Description

explicit-path	(Optional) Displays all configured explicit paths.
name	(Optional) Specifies the explicit path name. The maximum length is 16 characters.
tunnel-id-map	(Optional) Displays the mapping information for the outgoing interface.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(5)	This command was deprecated.
1.2(1)	This command was introduced.

Usage Guidelines

Multiple tunnel IDs can terminate at the same interface.

Examples

The following example displays the FC tunnel status:

```
switch# show fc-tunnel
fc-tunnel is enabled
```

The following example displays the FC tunnel egress mapping information:

```
switch# show fc-tunnel tunnel-id-map
tunnel id egress interface
    150     fc3/1
 100  fc3/1
```

The following example displays explicit mapping information of the FC tunnel:

```
switch# show fc-tunnel explicit-path
Explicit path name: Alternate1
       10.20.1.2 loose
       10.20.1.3 strict
Explicit path name: User2
       10.20.50.1 strict
       10.20.50.4 loose
```

show fdmi

To display the Fabric-Device Management Interface (FDMI) database information, use the **show fdmi** command.

show fdmi database [**detail** [{**hba-id** [{*hba-id* **vsan** *vsan-id*|**vsan** *vsan-id*}]|**vsan** *vsan-id*}]]

Syntax Description

database	Displays the FDMI database contents.
detail	(Optional) Specifies detailed FDMI information.
hba-id	(Optional) Displays detailed information for the specified HBA entry.
hba-id	(Optional) Displays detailed information for the specified HBA entry.
vsan *vsan-id*	(Optional) Specifies FDMI information for the specified VSAN. The range is 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays all HBA management servers:

```
switch# show fdmi database
Registered HBA List for VSAN 1
  10:00:00:00:c9:32:8d:77
  21:01:00:e0:8b:2a:f6:54
switch# show fdmi database detail
Registered HBA List for VSAN 1
-------------------------------
HBA-ID: 10:00:00:00:c9:32:8d:77
-------------------------------
Node Name        :20:00:00:00:c9:32:8d:77
Manufacturer     :Emulex Corporation
Serial Num       :0000c9328d77
Model            :LP9002
Model Description:Emulex LightPulse LP9002 2 Gigabit PCI Fibre Channel Adapter
Hardware Ver     :2002606D
Driver Ver       :SLI-2 SW_DATE:Feb 27 2003, v5-2.20a12
ROM Ver          :3.11A0
Firmware Ver     :3.90A7
OS Name/Ver      :Window 2000
CT Payload Len   :1300000
  Port-id: 10:00:00:00:c9:32:8d:77
-------------------------------
```

```
HBA-ID: 21:01:00:e0:8b:2a:f6:54
------------------------------
Node Name        :20:01:00:e0:8b:2a:f6:54
Manufacturer     :QLogic Corporation
Serial Num       :\74262
Model            :QLA2342
Model Description:QLogic QLA2342 PCI Fibre Channel Adapter
Hardware Ver     :FC5010409-10
Driver Ver       :8.2.3.10 Beta 2 Test 1 DBG (W2K VI)
ROM Ver          :1.24
Firmware Ver     :03.02.13.
OS Name/Ver      :500
CT Payload Len   :2040
  Port-id: 21:01:00:e0:8b:2a:f6:54
```

The following example displays VSAN1-specific FDMI information:

```
switch# show fdmi database detail vsan 1
Registered HBA List for VSAN 1
------------------------------
HBA-ID: 10:00:00:00:c9:32:8d:77
------------------------------
Node Name        :20:00:00:00:c9:32:8d:77
Manufacturer     :Emulex Corporation
Serial Num       :0000c9328d77
Model            :LP9002
Model Description:Emulex LightPulse LP9002 2 Gigabit PCI Fibre Channel Adapter
Hardware Ver     :2002606D
Driver Ver       :SLI-2 SW_DATE:Feb 27 2003, v5-2.20a12
ROM Ver          :3.11A0
Firmware Ver     :3.90A7
OS Name/Ver      :Window 2000
CT Payload Len   :1300000
  Port-id: 10:00:00:00:c9:32:8d:77
------------------------------
HBA-ID: 21:01:00:e0:8b:2a:f6:54
------------------------------
Node Name        :20:01:00:e0:8b:2a:f6:54
Manufacturer     :QLogic Corporation
Serial Num       :\74262
Model            :QLA2342
Model Description:QLogic QLA2342 PCI Fibre Channel Adapter
Hardware Ver     :FC5010409-10
Driver Ver       :8.2.3.10 Beta 2 Test 1 DBG (W2K VI)
ROM Ver          :1.24
Firmware Ver     :03.02.13.
OS Name/Ver      :500
CT Payload Len   :2040
  Port-id: 21:01:00:e0:8b:2a:f6:54
```

The following example displays details for the specified HBA entry:

```
switch# show fdmi database detail Hba-id 21:01:00:e0:8b:2a:f6:54 vsan 1
Node Name        :20:01:00:e0:8b:2a:f6:54
Manufacturer     :QLogic Corporation
Serial Num       :\74262
Model            :QLA2342
Model Description:QLogic QLA2342 PCI Fibre Channel Adapter
Hardware Ver     :FC5010409-10
Driver Ver       :8.2.3.10 Beta 2 Test 1 DBG (W2K VI)
ROM Ver          :1.24
Firmware Ver     :03.02.13.
OS Name/Ver      :500
```

```
CT Payload Len   :2040
  Port-id: 21:01:00:e0:8b:2a:f6:54
```

show ficon

To display configured FICON information, use the **show ficon** command.

show ficon [{**control-device sb3** [**vsan** *vsan-id*]|**first-available port-number**|**port default-state**|**port-numbers** {**assign** [{*slot*|**logical-port**|**slot** *slot*}]|**interface**}|**stat**|**vsan** *vsan-id* [{**allegiance**|**directory-history** [**key-counter** *value*]|**file** {**all**|**name** *filename* [**portaddress** *port*]}}]|**interface** {**fc slot** / *port*|**fcip** *fcip-id*|**port-channel** *port*}|**portaddress** [{*port* **[counters]**|**portnumber** [{*port-numbers*|**duplicate**|**undefined**}] **[brief] [installed]**}]}]

Syntax Description

control-device sb3	(Optional) Displays FICON control device information.
vsan *vsan-id*	Specifies FICON information for the specified VSAN ranging from1 to 4093.
first-available port-number	(Optional) Displays the available port numbers.
port default-state	(Optional) Displays the default FICON port prohibit state.
port-numbers	(Optional) Displays FICON port numbers.
assign *slot*	(Optional) Displays the FICON port numbers assigned to the specified slot, 1 though 6.
logical port	(Optional) Displays FICON port numbers assigned to logical interfaces.
slot *slot*	(Optional) Displays the FICON port numbers assigned to the specified slot, 1 though 6.
interface	(Optional) Displays FICON information for an interface.
stat	(Optional) Displays information about FICONSTAT.
allegiance	(Optional) Displays FICON device allegiance information.
directory-history	(Optional) Displays FICON directory history.
key-counter *value*	(Optional) Specifies a key counter.
file	(Optional) Displays FICON information for a file.
all	(Optional) Specifies all files.
name *filename*	(Optional) Specifies the name for a file.
portaddress *port*	(Optional) Specifies a port address for a file.
fc *slot*/*port*	Specifies a Fibre Channel interface.
fcip *fcip-id*	Specifies an FC IP interface.
port-channel *port*	Specifies a PortChannel interface.
counters	(Optional) Displays counter information for the port address.

portnumber *port-numbers*	(Optional) Displays FICON information for a port number in the specified range, 0 through 153 or 0x0 through 0x99.
duplicate	(Optional) Displays FICON interfaces with duplicate port numbers and port addresses.
undefined	(Optional) Displays FICON interfaces without port numbers and port addresses.
brief	(Optional) Displays brief FICON information for the port address.
installed	(Optional) Displays FICON information for the installed port address.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	• Added the **port-numbers** and **stat** options. • Added the **portnumber** keyword.
3.0(2)	Added the **port default-state** option.

Usage Guidelines

If FICON is not enabled on a VSAN, you will not be able to view FICON configuration information for that VSAN.

Examples

The following example displays configured FICON information:

```
switch# show ficon
Ficon information for VSAN 20
  Ficon is online
  VSAN is active
  Host port control is Enabled
  Host offline control is Enabled
  User alert mode is Enabled
  SNMP port control is Enabled
  Host set director timestamp is Enabled
  Active=Saved is Disabled
  Number of implemented ports are 240
  Key Counter is 73723
  FCID last byte is 0
  Date/Time is set by host to Sun Jun 26 00:04:06.991999 1904
  Device allegiance is locked by Host
  Codepage is us-canada
  Saved configuration files
    IPL
    _TSIRN00
```

The following example displays the default prohibit state:

```
switch# show ficon port default-state
Port default state is allow-all
```

The following example displays assigned FICON port numbers:

```
switch# show ficon port-numbers assign
ficon slot 1 assign port-numbers 0-31
ficon slot 2 assign port-numbers 32-63
ficon slot 3 assign port-numbers 64-95
ficon slot 4 assign port-numbers 96-127
ficon logical-port assign port-numbers 128-153
```

The following example displays port address information:

```
switch# show ficon vsan 2 portaddress
Port Address 1 is not installed in vsan 2
    Port number is 1, Interface is fc1/1
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255
Port Address 2 is not installed in vsan 2
    Port number is 2, Interface is fc1/2
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255
...
Port Address 239 is not installed in vsan 2
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255
Port Address 240 is not installed in vsan 2
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255
```

The following example displays port address information in a brief format:

```
switch# show ficon vsan 2 portaddress 50-55 brief
--------------------------------------------------------------------------------
Port    Port    Interface          Admin     Status           Oper   FCID
Address Number                     Blocked                    Mode
--------------------------------------------------------------------------------
50      50      fc2/18             on             fcotAbsent       --     --
51      51      fc2/19             off       fcotAbsent       --     --
52      52      fc2/20             off       fcotAbsent       --     --
53      53      fc2/21             off       fcotAbsent       --     --
54      54      fc2/22             off       notConnected     --     --
55      55      fc2/23             off       up               FL     0xea0000
56  55          off       up               FL     0xea0000
```

The following example displays port address counter information:

```
switch# show ficon vsan 20 portaddress 8 counters
Port Address 8(0x8) is up in vsan 20
    Port number is 8(0x8), Interface is fc1/8
    Version presented 1, Counter size 32b
    242811 frames input, 9912794 words
      484 class-2 frames, 242302 class-3 frames
      0 link control frames, 0 multicast frames
      0 disparity errors inside frames
      0 disparity errors outside frames
```

```
      0 frames too big, 0 frames too small
      0 crc errors, 0 eof errors
      0 invalid ordered sets
      0 frames discarded c3
      0 address id errors
    116620 frames output, 10609188 words
      0 frame pacing time
    0 link failures
    0 loss of sync
    0 loss of signal
    0 primitive seq prot errors
    0 invalid transmission words
    1 lrr input, 0 ols input, 5 ols output
    0 error summary
```

The following example displays the contents of the specified FICON configuration file:

```
switch# show ficon vsan 3 file IPL
FICON configuration file IPL      in vsan 3
    Port address 1
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255
    Port address 2
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255
    Port address 3
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255
    Port address 4
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255
...
Port address 80
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255
    Port address 254
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255
```

The following example displays all FICON configuration files:

```
switch# show ficon vsan 2
Ficon information for VSAN 2
  Ficon is enabled
  VSAN is active
  Host control is Enabled
  Host offline control is Enabled
  Clock alert mode is Disabled
  User alert mode is Disabled
  SNMP control is Disabled
  Active=Saved is Disabled
  Number of implemented ports are 240
  Key Counter is 9
  FCID last byte is 0
  Date/Time is same as system time (Sun Dec 14 01:26:30.273402 1980)
  Device Allegiance not locked
  Codepage is us-canada
```

```
  Saved configuration files
    IPL
    IPLFILE1
```

The following example displays the specified port addresses for a FICON configuration file:

```
switch# show ficon vsan 2 file iplfile1 portaddress 1-7
FICON configuration file IPLFILE1 in vsan 2
    Port address 1
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,241-253,255
    Port address 2
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,241-253,255
    Port address 3
        Port name is P3
        Port is not blocked
        Prohibited port addresses are 0,241-253,255
...
    Port address 7
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,241-253,255
```

The following example displays the specified port address when FICON is enabled:

```
switch# show ficon
 vsan 2 portaddress 55
Port Address 55 is not installed in vsan 2
    Port number is 55, Interface is fc2/23
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255
    Admin port mode is FL
    Port mode is FL, FCID is 0xea0000
```

The following example displays two port addresses configured with different states:

```
switch# show ficon vsan 2 portaddress 2
Port Address 2(0x2) is not installed in vsan 2
    Port number is 2(0x2), Interface is fc1/2
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255(0,0xf1-0xfd,0xff)
    Admin port mode is auto
    Peer was type model manufactured by
switch# show ficon vsan 2 portaddress 1
Port Address 2(0x2) is not installed in vsan 2
    Port number is 2(0x2), Interface is fc1/2
    Port name is
 Port name is SampleName
    Port is admin blocked
 Prohibited port addresses are 0,241-253,255(0,0xf1-0xfd,0xff)
    Admin port mode is auto
    Peer was type model manufactured by
```

The following example displays control unit information:

```
switch# show ficon control-device sb3
Control Unit Image:0x80b9c2c
```

```
VSAN:20 CU:0x20fe00 CUI:0 CUD:0 CURLP:(nil)
ASYNC LP:(nil) MODE:1 STATE:1 CQ LEN:0 MAX:0
PRIMARY LP:   VSAN:0 CH:0x0 CHI:0 CU:0x0 CUI:0
ALTERNATE LP: VSAN:0 CH:0x0 CHI:0 CU:0x0 CUI:0
Logical Path:0x80b9fb4
VSAN:20 CH:0x200600 CHI:15 CU:0x20fe00 CUI:0 STATE:1 FLAGS:0x1
LINK: OH:0x0 OC:0x0 IH:0x0 IC:0x0
DEV:  OH:0x0 OC:0x0 IH:0x0 IC:0x0
SENSE: 00 00 00 00 00 00 00 46
       30 20 00 00 00 00 00 00
       00 00 00 00 00 00 00 00
       00 00 00 00 00 00 00 00
IUI:0x0 DHF:0x0 CCW:0x0 TOKEN:0x0 PCCW:0x0 FCCW:0x0 PTOKEN:0x0 FTOKEN:0x0
CMD:0x0 CCW_FLAGS:0x0 CCW_COUNT:0 CMD_FLAGS:0x0 PRIO:0x0 DATA_COUNT:0
STATUS:0x0 FLAGS:0x0 PARAM:0x0 QTP:0x0 DTP:0x0
CQ LEN:0 MAX:0 DESTATUS:0x0
```

The following example displays the history buffer for the specified VSAN:

```
switch# show ficon vsan 20 director-history
Director History Buffer for vsan 20
-------------------------------------------
Key Counter           Ports Address
                      Changed
-------------------------------------------
74556                 43
74557                 44
74558                 45
74559                 46
74560                 47
74561                 48
74562                 49
74563                 50
74564                 51
74565                 52
74566                 53
74567                 54
74568                 55
74569                 56
74570                 57
74571                 58
74572                 59
74573                 60
74574                 61
74575                 62
74576                 63
74577                 64
74578
74579
74580                 1-3,5,10,12,14-16,34-40,43-45,47-54,56-57,59-64
74581                 3,5
74582                 64
74583
74584                 1-3,10,12,14-16,34-40,43-45,47-54,56-57,59-64
74585                 1
74586                 2
74587                 3
```

The following example displays the running configuration information:

```
switch# show running-config
...
ficon vsan 2
```

```
portaddress 1
block
name SampleName
prohibit portaddress 3
portaddress 3
prohibit portaddress 1
file IPL
```

The following example displays the available port numbers:

```
switch# show ficon first-available port-number
Port number 129(0x81) is available
```

show file

To display the contents of a specified file in the file system, use the **show file** command.

show file filename [{**cksum**|**md5sum**}]

Syntax Description

filename	Specifies a filename.
cksum	(Optional) Displays CRC checksum for a file.
md5sum	(Optional) Displays MD5 checksum for a file.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the contents of the test file that resides in the slot0 directory:

```
switch# show file slot0:test
config t
Int fc1/1
no shut
end
show int
```

The following example displays the contents of a file residing in the current directory:

```
switch# show file myfile
```

The following example displays the CRC checksum for a file:

```
switch# show file bootflash:vboot-1 cksum
838096258
```

The following example displays the MD5 checksum for a file:

```
switch# show file bootflash:vboot-1 md5sum
3d8e05790155150734eb8639ce98a331
```

show flex-attach

To display the FlexAttach distribution status, use the show flex-attach command.

show flex-attach

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the FlexAttach distribution status:

```
switch# show flex-attach
Fabric distribution status
----------------------
fabric distribution enabled
Last Action Time Stamp     : Sun Mar  2 02:32:04 2008
Last Action                : Commit
Last Action Result         : Success
Last Action Failure Reason : none
```

Related Commands

Command	Description
show flex-attach virtual-pwwn	Displays the current list of virtual pWWNs on a specified interface.

show flex-attach info

To display the FlexAttach information, use the show flex-attach info command.

show flex-attach info

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Exec mode

Command History

Release	Modification
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the FlexAttach information:

```
switch# show flex-attach info
Global Auto Flag : TRUE
------------------------------------------------------------
                Local Interface->vpwwn
------------------------------------------------------------
vsan       intf       vpwwn                     auto    intf-state
------------------------------------------------------------
all        fc1/1      20:00:00:05:30:01:71:ba   auto    DOWN
all        fc1/2      20:01:00:05:30:01:71:ba   auto    DOWN
all        fc1/3      20:02:00:05:30:01:71:ba   auto    DOWN
all        fc1/4      20:03:00:05:30:01:71:ba   auto    DOWN
all        fc1/20     20:13:00:05:30:01:71:ba   auto    DOWN
all        fc1/21     20:14:00:05:30:01:71:ba   auto    DOWN
all        fc1/22     20:15:00:05:30:01:71:ba   auto    DOWN
all        fc1/23     20:16:00:05:30:01:71:ba   auto    DOWN
all        fc1/24     20:17:00:05:30:01:71:ba   auto    DOWN
Number of local virtual pwwn entries = 24
------------------------------------------------------------------------
                Remote Interface->vpwwn
------------------------------------------------------------------------
swwn                     vsan     intf     vpwwn                     auto
------------------------------------------------------------------------
20:00:00:05:30:01:6e:1c  all      fc1/1    23:46:00:05:30:01:6e:1e   auto
20:00:00:05:30:01:6e:1c  all      fc1/2    23:47:00:05:30:01:6e:1e   auto
20:00:00:05:30:01:6e:1c  all      fc1/3    23:48:00:05:30:01:6e:1e   auto
20:00:00:05:30:01:6e:1c  all      fc1/4    23:49:00:05:30:01:6e:1e   auto
20:00:00:05:30:01:6e:1c  all      fc1/5    23:4a:00:05:30:01:6e:1e   auto
20:00:00:05:30:01:6e:1c  all      fc1/6    23:4b:00:05:30:01:6e:1e   auto
20:00:00:05:30:01:6e:1c  all      fc1/7    23:4c:00:05:30:01:6e:1e   auto
20:00:00:05:30:01:6e:1c  all      fc1/8    23:4d:00:05:30:01:6e:1e   auto
20:00:00:05:30:01:6e:1c  all      fc1/9    23:4e:00:05:30:01:6e:1e   auto
20:00:00:05:30:01:6e:1c  all      fc1/10   23:4f:00:05:30:01:6e:1e   auto
20:00:00:05:30:01:6e:1c  all      fc1/11   23:50:00:05:30:01:6e:1e   auto
20:00:00:05:30:01:6e:1c  all      fc1/12   23:51:00:05:30:01:6e:1e   auto
```

```
20:00:00:05:30:01:6e:1c   all      fc1/13   23:52:00:05:30:01:6e:1e   auto
20:00:00:05:30:01:6e:1c   all      fc1/14   23:53:00:05:30:01:6e:1e   auto
20:00:00:05:30:01:6e:1c   all      fc1/15   23:54:00:05:30:01:6e:1e   auto
20:00:00:05:30:01:6e:1c   all      fc1/23   23:5c:00:05:30:01:6e:1e   auto
20:00:00:05:30:01:6e:1c   all      fc1/24   23:5d:00:05:30:01:6e:1e   auto
Number of remote virtual pwwn entries = 24
------------------------------------------------------------
                PWWN -> VPWWN Mappings
------------------------------------------------------------
pwwn                      vpwwn
------------------------------------------------------------
20:14:00:05:30:01:71:11    20:14:00:05:30:01:71:99
20:14:00:05:30:01:71:44    20:14:00:05:30:01:71:88
Number of real pwwn to virtual pwwn entries = 2
------------------------------------------------------------
                OXID INFO
------------------------------------------------------------
vsan       sid          did          oxid       els-cmd      phy-pwwn
       vpwwn
------------------------------------------------------------
Number of outstanding ELS frames = 0
-------------------------------------------------------------------------------
                srv fcid to srv ifindex map
-------------------------------------------------------------------------------
--
vsan    srvfcid  srvif  pwwn                    vpwwn                    flogi?
-------------------------------------------------------------------------------
--
Number of logged-in devices = 0
```

Related Commands

Command	Description
show flex-attach	Displays the FlexAttach distribution status.
show flex-attach merger status	Displays the FlexAttach merger status.
show flex-attach virtual-pwwn	Displays the current list of virtual pWWN on a specified interface.

show flex-attach merge status

To display the FlexAttach merger status, use the show flex-attach merge status command.

show flex-attach merger status

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Exec mode

Command History

Release	Modification
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the FlexAttach merge status:

```
switch# show flex-attach merge status
Flex-Attach merge status
----------------
Status         : Success
Failure reason :
```

Related Commands

Command	Description
show flex-attach	Displays the FlexAttach distribution status.
show flex-attach virtual-pwwn	Displays the current list of virtual pWWN on a specified interface.

show flex-attach virtual-pwwn

To display the current list of virtual pWWN on a specified interface, use the show flex-attach virtual-pwwn command.

show flex-attach virtual-pwwn

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Exec mode

Command History

Release	Modification
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the current list of virtual pWWN on an interface:

```
switch# show flex-attach virtual-pwwn
Global auto virtual port WWN generation enabled
             VIRTUAL PORT WWNS ASSIGNED TO INTERFACES
------------------------------------------------------------------------------
-----
VSAN     INTERFACE  VIRTUAL-PWWN              AUTO    LAST-CHANGE
------------------------------------------------------------------------------
-----
all      fc1/1      20:00:00:05:30:01:71:ba   TRUE   Sat Mar  1 14:10:07 2008
all      fc1/2      20:01:00:05:30:01:71:ba   TRUE   Sat Mar  1 14:10:07 2008
all      fc1/19     20:12:00:05:30:01:71:ba   TRUE   Sat Mar  1 14:10:07 2008
all      fc1/20     20:13:00:05:30:01:71:ba   TRUE   Sat Mar  1 14:10:07 2008
all      fc1/21     20:14:00:05:30:01:71:ba   TRUE   Sat Mar  1 14:10:07 2008
all      fc1/22     20:15:00:05:30:01:71:ba   TRUE   Sat Mar  1 14:10:07 2008
all      fc1/23     20:16:00:05:30:01:71:ba   TRUE   Sat Mar  1 14:10:07 2008
all      fc1/24     20:17:00:05:30:01:71:ba   TRUE   Sat Mar  1 14:10:07 2008
Number of virtual pwwn assigned to local interfaces = 24
                   VIRTUAL PORT WWNS ASSIGNED TO PHYSICAL PORT WWNs
------------------------------------------------------------------------------
-----
PWWN                       VIRTUAL-PWWN              LAST-CHANGE
------------------------------------------------------------------------------
-----
20:14:00:05:30:01:71:11   20:14:00:05:30:01:71:99  Sat Mar  1 14:56:07 2008
20:14:00:05:30:01:71:44   20:14:00:05:30:01:71:88  Sat Mar  1 14:56:07 2008
Number of virtual pwwn assigned to real pwwns = 2
```

Related Commands

Command	Description
flex-attach virtual-pwwn auto	Enables the FlexAttach virtual pWWN on a specific interface.

Command	Description
flex-attach virtual-pwwn interface	Sets the user-specified FlexAttach virtual pWWN.

show flogi

To list all the FLOGI sessions through all interfaces across all VSANs, use the **show flogi** command.

show flogi auto-area-list|database {fcid fcid-id|interface {fa slot/port|fc slot/port|fv module-number}|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

auto-area-list	Displays the list of OUIs that are allocated areas.
database	Displays information about FLOGI sessions.
fcid fcid-id	Displays FLOGI database entries based on the FCID allocated. The format is 0xhhhhhh.
interface	Displays FLOGI database entries based on the logged in interface.
fa slot/port	Specifies the FA port interface to configure by slot and port number on all switches.
fc slot/port	(Optional) Specifies the Fibre Channel interface to configure by slot and port number on an MDS 9000 Family switch.
bay *port* **| ext** *port*	(Optional) Specifies the Fibre Channel interface by bay or by external 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.
fv module-number	Specifies the Fibre Channel Virtualization interface by module on all switches.
vsan *vsan-id*	Displays FLOGI database entries based on the VSAN ID. The range is1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.1(2)	Added the **interface bay** | **ext** option.

Usage Guidelines

Output of this command is first sorted by interface and then by VSANs.

In a Fibre Channel fabric, each host or disk requires an FCID. Use the **show flogi database** command to verify if a storage device is displayed in the Fabric login (FLOGI) table as in the examples below. If the required device is displayed in the FLOGI table, the fabric login is successful. Examine the FLOGI database on a switch that is directly connected to the host HBA and connected ports.

Examples

The following example displays details on the FLOGI database:

```
switch# show flogi database
--------------------------------------------------------------------------------
INTERFACE  VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
sup-fc0    2     0xb30100  10:00:00:05:30:00:49:63  20:00:00:05:30:00:49:5e
fc9/13     1     0xb200e2  21:00:00:04:cf:27:25:2c  20:00:00:04:cf:27:25:2c
fc9/13     1     0xb200e1  21:00:00:04:cf:4c:18:61  20:00:00:04:cf:4c:18:61
fc9/13     1     0xb200d1  21:00:00:04:cf:4c:18:64  20:00:00:04:cf:4c:18:64
fc9/13     1     0xb200ce  21:00:00:04:cf:4c:16:fb  20:00:00:04:cf:4c:16:fb
fc9/13     1     0xb200cd  21:00:00:04:cf:4c:18:f7  20:00:00:04:cf:4c:18:f7
Total number of flogi = 6.
```

The following example displays the FLOGI interface.

```
switch# show flogi database interface fc 1/11
INTERFACE       VSAN   FCID           PORT NAME               NODE NAME
-------------------- ---- -------- ----------------------- ----------------------
fc9/13    1 0xa002ef 21:00:00:20:37:18:17:d2 20:00:00:20:37:18:17:d2
fc9/13    1 0xa002e8 21:00:00:20:37:38:a7:c1 20:00:00:20:37:38:a7:c1
fc9/13    1 0xa002e4 21:00:00:20:37:6b:d7:18 20:00:00:20:37:6b:d7:18
fc9/13    1 0xa002e2 21:00:00:20:37:18:d2:45 20:00:00:20:37:18:d2:45
fc9/13    1 0xa002e1 21:00:00:20:37:39:90:6a 20:00:00:20:37:39:90:6a
fc9/13    1 0xa002e0 21:00:00:20:37:36:0b:4d 20:00:00:20:37:36:0b:4d
fc9/13    1 0xa002dc 21:00:00:20:37:5a:5b:27 20:00:00:20:37:5a:5b:27
fc9/13    1 0xa002da 21:00:00:20:37:18:6f:90 20:00:00:20:37:18:6f:90
fc9/13    1 0xa002d9 21:00:00:20:37:5b:cf:b9 20:00:00:20:37:5b:cf:b9
fc9/13    1 0xa002d6 21:00:00:20:37:46:78:97 20:00:00:20:37:46:78:97
Total number of flogi = 10.
```

The following example displays the FLOGI VSAN:

```
switch# show flogi database vsan 1
--------------------------------------------------------------------------------
INTERFACE  VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
fc9/13      1     0xef02ef  22:00:00:20:37:18:17:d2  20:00:00:20:37:18:17:d2
fc9/13      1     0xef02e8  22:00:00:20:37:38:a7:c1  20:00:00:20:37:38:a7:c1
fc9/13      1     0xef02e4  22:00:00:20:37:6b:d7:18  20:00:00:20:37:6b:d7:18
fc9/13      1     0xef02e2  22:00:00:20:37:18:d2:45  20:00:00:20:37:18:d2:45
fc9/13      1     0xef02e1  22:00:00:20:37:39:90:6a  20:00:00:20:37:39:90:6a
fc9/13      1     0xef02e0  22:00:00:20:37:36:0b:4d  20:00:00:20:37:36:0b:4d
fc9/13      1     0xef02dc  22:00:00:20:37:5a:5b:27  20:00:00:20:37:5a:5b:27
fc9/13      1     0xef02da  22:00:00:20:37:18:6f:90  20:00:00:20:37:18:6f:90
fc9/13      1     0xef02d9  22:00:00:20:37:5b:cf:b9  20:00:00:20:37:5b:cf:b9
fc9/13      1     0xef02d6  22:00:00:20:37:46:78:97  20:00:00:20:37:46:78:97
Total number of flogi = 10.
```

The following example displays the FLOGI FCID:

```
switch# show flogi database fcid 0xef02e2
--------------------------------------------------------------------------------
INTERFACE  VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
fc9/13      1     0xef02e2  22:00:00:20:37:18:d2:45  20:00:00:20:37:18:d2:45
Total number of flogi = 1.
```

Related Commands

Command	Description
show fcns database	Displays all the local and remote name server entries.

show flogi database interface

To list all the FLOGI sessions through all of the interfaces, use the **show flogi database interface** command.

show flogi database interface {**fa slot/port**|**fc slot/port**|**fv module-number**|**port-channel port-channel number details**}

Syntax Description

fa slot/port	Specifies the FA port interface to configure by slot and port number on all switches.
fc slot/port	Specifies the Fibre Channel interface to configure by slot and port number on an MDS 9000 Family switch.
fv module-number	Specifies the Fibre Channel virtualization interface by module on all switches.
port-channel	Specifies the PortChannel interface.
port-channel number	Specifies the PortChannel number. The range is from 1 to 256.
details	Specifies FCID allocation details.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the PortChannel FCID allocation details:

```
switch# show flogi database interface port-channel 1 details
No flogi sessions found.
switch#
```

Related Commands

Command	Description
show fcns database	Displays all the local and remote name server entries.

show fspf

To display global FSPF information, use the **show fspf** command.

show fspf [{**database vsan vsan-id** [{**detail**|**domain domain-id detail**}]|**interface**|**vsan vsan-id interface** [{**fc** *slot/port*|**port-channel port-channel**}]}]

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

database	(Optional) Displays the FSPF link state database.
vsan *vsan-id*	(Optional) Specifies the VSAN ID. The range is 1 to 4093.
detail	(Optional) Displays detailed FSPF information.
domain domain-id	(Optional) Specifies the domain of the database. The range is 0 to 255.
interface	(Optional) Specifies the FSPF interface.
fc slot/port	(Optional) Specifies the Fibre Channel interface to configure by slot and port number on an MDS 9000 Family switch.
bay *port* **| ext** *port*	(Optional) Specifies the Fibre Channel interface by bay or by external 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 port-channel	(Optional) Specifies the PortChannel interface. The range is 1 to 256.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If no other parameters are given, all the LSRs in the database are displayed. If more specific information is required, then the domain number of the owner of the LSR may be given. **Detail** gives more detailed information on each LSR.

Examples

The following example displays FSPF interface information:

```
switch# show fspf interface vsan 1 fc1/1
FSPF interface fc1/1 in VSAN 1
FSPF routing administrative state is active
```

```
Interface cost is 500
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is FULL
Neighbor Domain Id is 0x0c(12), Neighbor Interface index is 0x0f100000
Statistics counters :
   Number of packets received : LSU  8  LSA  8  Hello 118  Error packets 0
   Number of packets transmitted : LSU  8  LSA  8  Hello 119  Retransmitted LSU
 0
  Number of times inactivity timer expired for the interface = 0
```

The following example displays FSPF database information:

```
switch# show fspf database vsan 1
FSPF Link State Database for VSAN 1 Domain 0x0c(12)
LSR Type                = 1
Advertising domain ID   = 0x0c(12)
LSR Age                 = 1686
LSR Incarnation number  = 0x80000024
LSR Checksum            = 0x3caf
Number of links         = 2
 NbrDomainId      IfIndex   NbrIfIndex    Link Type         Cost
-------------------------------------------------------------------------------
   0x65(101) 0x0000100e     0x00001081               1          500
   0x65(101) 0x0000100f     0x00001080               1          500
FSPF Link State Database for VSAN 1 Domain 0x65(101)
LSR Type                = 1
Advertising domain ID   = 0x65(101)
LSR Age                 = 1685
LSR Incarnation number  = 0x80000028
LSR Checksum            = 0x8443
Number of links         = 6
 NbrDomainId      IfIndex   NbrIfIndex    Link Type         Cost
-------------------------------------------------------------------------------
   0xc3(195) 0x00001085     0x00001095               1          500
   0xc3(195) 0x00001086     0x00001096               1          500
   0xc3(195) 0x00001087     0x00001097               1          500
   0xc3(195) 0x00001084     0x00001094               1          500
    0x0c(12) 0x00001081     0x0000100e               1          500
    0x0c(12) 0x00001080     0x0000100f               1          500
FSPF Link State Database for VSAN 1 Domain 0xc3(195)
LSR Type                = 1
Advertising domain ID   = 0xc3(195)
LSR Age                 = 1686
LSR Incarnation number  = 0x80000033
LSR Checksum            = 0x6799
Number of links         = 4
 NbrDomainId      IfIndex   NbrIfIndex    Link Type         Cost
-------------------------------------------------------------------------------
   0x65(101) 0x00001095     0x00001085               1          500
   0x65(101) 0x00001096     0x00001086               1          500
   0x65(101) 0x00001097     0x00001087               1          500
   0x65(101) 0x00001094     0x00001084               1          500
```

This command displays FSPF information for a specified VSAN:

```
switch# show fspf vsan 1
FSPF routing for VSAN 1
FSPF routing administration status is enabled
FSPF routing operational status is UP
It is an intra-domain router
Autonomous region is 0
SPF hold time is 0 msec
MinLsArrival = 1000 msec , MinLsInterval = 5000 msec
```

```
Local Domain is 0x65(101)
Number of LSRs = 3, Total Checksum = 0x0001288b
Protocol constants :
   LS_REFRESH_TIME = 1800 sec
   MAX_AGE         = 3600 sec
Statistics counters :
   Number of LSR that reached MaxAge = 0
   Number of SPF computations        = 7
   Number of Checksum Errors         = 0
   Number of Transmitted packets :  LSU 65 LSA 55 Hello 474 Retranmsitted LSU 0
   Number of received packets :  LSU 55 LSA 60 Hello 464 Error packets 10
```

show hardware

To display switch hardware inventory details, use the **show hardware** command.

show hardware [**ipc-channel status**]

Syntax Description

ipc-channel status	(Optional) Displays the status of the interprocess communication (IPC) channels.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.
NX-OS 4.1(1b)	Changed the command output from SAN-OS to NX-OS.

Usage Guidelines

None.

Examples

The following example displays the switch hardware inventory details:

```
switch# show hardware
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2008, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
Software
  BIOS:      version 3.17.0
  loader:    version N/A
  kickstart: version 4.0(3) [gdb]
  system:    version 4.0(3) [gdb]
  BIOS compile time:       03/23/08
  kickstart image file is: bootflash:/n7000-s1-kickstart.4.0.3.gbin.S17
  kickstart compile time:  7/24/2008 12:00:00 [07/28/2008 03:28:06]
  system image file is:    bootflash:/n7000-s1-dk9.4.0.3.gbin.S17
  system compile time:     7/24/2008 12:00:00 [07/28/2008 04:10:26]
Hardware
  cisco Nexus7000 C7010 (10 Slot) Chassis ("Supervisor module-1X")
  Intel(R) Xeon(R) CPU         with 2063436 kB of memory.
  Processor Board ID JAB10380101
  Device name: switch
  bootflash:    1023120 kB
  slot0:              0 kB (expansion flash)
  bootflash:  251904 kB
  slot0:      251904 kB
```

```
Kernel uptime is 0 day(s), 10 hour(s), 32 minute(s), 43 secon
Last reset at 231551 usecs after  Wed Jul 30 00:07:18 2008
  Reason: Reset Requested by CLI command reload
  System version: 4.0(3)
  Service:
plugin
  Core Plugin, Ethernet Plugin
CMP (Module 6) no response
--------------------------------
Switch hardware ID information
--------------------------------
Switch is booted up
  Switch type is : Nexus7000 C7010 (10 Slot) Chassis
  Model number is MOSPORT10P
  H/W version is 0.403
  Part Number is 73-10900-04
  Part Revision is 03
  Manufacture Date is Year 11 Week 25
  Serial number is TBM11256507
  CLEI code is
--------------------------------
Chassis has 10 Module slots and 5 Fabric slots
--------------------------------
Module1  empty
Module2  ok
  Module type is : 10/100/1000 Mbps Ethernet Module
  1 submodules are present
  Model number is NURBURGRING
  H/W version is 0.407
  Part Number is 73-10098-04
  Part Revision is 13
  Manufacture Date is Year 10 Week 44
  Serial number is JAB104400P0
  CLEI code is
Module3  empty
Module4  empty
Module5  empty
Module6  ok
  Module type is : Supervisor module-1X
  0 submodules are present
  Model number is CATALUNYA
  H/W version is 0.311
  Part Number is 73-10877-03
  Part Revision is 09
  Manufacture Date is Year 10 Week 38
  Serial number is JAB10380101
  CLEI code is TBD
Module7  empty
Module8  empty
Module9  empty
Module10  empty
Xbar1  ok
  Module type is : Fabric card module
  0 submodules are present
  Model number is Estoril
  H/W version is 0.203
  Part Number is 73-10624-02
  Part Revision is 06
  Manufacture Date is Year 10 Week 43
  Serial number is JAB104300HM
  CLEI code is
Xbar2  empty
Xbar3  empty
```

```
Xbar4  empty
Xbar5  empty
-------------------------------------
Chassis has 3 PowerSupply Slots
-------------------------------------
PS1 ok
  Power supply type is: 0.00W 220v AC
  Model number is FIORANO
  H/W version is 0.103
  Part Number is 341-0230-01
  Part Revision is 03
  Manufacture Date is Year 11 Week 17
  Serial number is DTH1117T005
  CLEI code is
PS2 ok
  Power supply type is: 0.00W 220v AC
  Model number is FIORANO
  H/W version is 0.103
  Part Number is 341-0230-01
  Part Revision is 03
  Manufacture Date is Year 11 Week 17
  Serial number is DTH1117T009
  CLEI code is
PS3 absent
---------------------------------
Chassis has 4 Fan slots
---------------------------------
Fan1(sys_fan1) ok
  Model number is
  H/W version is 0.0
  Part Number is
  Part Revision is
  Manufacture Date is Year 0 Week 0
  Serial number is
  CLEI code is
Fan2(sys_fan2) ok
  Model number is
  H/W version is 0.0
  Part Number is
  Part Revision is
  Manufacture Date is Year 0 Week 0
  Serial number is
  CLEI code is
Fan3(fab_fan1) ok
  Model number is
  H/W version is 0.0
  Part Number is
  Part Revision is
  Manufacture Date is Year 0 Week 0
  Serial number is
  CLEI code is
switch#
```

The following example displays the status of the IPC channel:

```
switch# show hardware ipc-channel status
Active IPC-Channel:            A
switch#
```

show hardware capacity

To display the information about the hardware capabilities and current hardware utilization by the system, use the show hardware capacity command.

show hardware capacity [{**eobc**|**fabric-utilization**|**forwarding**|**interface**|**module**|**power**}]

Syntax Description

eobc	Displays the EOBC resources.
fabric-utilization	Displays the fabric utilization.
forwarding	Displays the L2 L3 forwarding resources.
interface	Displays the interface resources.
module	Displays the SUP, LC, Xbar.
power	Displays the power supply.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the information about the hardware capabilities and current hardware utilization by the system:

```
switch# show hardware capacity fabric-utilization
--------------------------------------------------------------------------------
Fabric Planes:
A -- Unicast fabric packets
B -- Multicast/Multidestination fabric packets
--------------------------------------------------------------------------------
Bandwidth is in Gbps and shared by both Fabric Planes (A+B)
-----------------------------PEAK FABRIC UTILIZATION-----------------------------
Mod Fab Fab Fab  ASIC Band Fab      Ingress                  Egress
    Lnk Mod ASIC Port wdth Pln Util%       Time         Util%       Time
--------------------------------------------------------------------------------
1    9   3    1   16   55   A     4 2009-06-26@21:06:04    4 2009-06-26@21:06:04
1    9   3    1   16   55   B     0          --            0          --
1   10   3    1   17   55   A     6 2009-06-26@21:06:04    6 2009-06-26@21:06:04
1   10   3    1   17   55   B     0          --            0          --
1   11   3    2    0   55   A     4 2009-06-26@21:06:19    4 2009-06-26@21:06:19
1   11   3    2    0   55   B     0          --            0          --
1   12   3    2   24   55   A     0          --            0          --
1   12   3    2   24   55   B     0          --            0          --
```

```
1   13   4    1   16   55   A     3 2009-06-26@21:06:04    3 2009-06-26@21:06:04
1   13   4    1   16   55   B     0         --             0         --
1   14   4    1   17   55   A     3 2009-06-26@21:06:04    3 2009-06-26@21:06:04
1   14   4    1   17   55   B     0         --             0         --
1   15   4    2    0   55   A     3 2009-06-26@21:06:19    3 2009-06-26@21:06:19
1   15   4    2    0   55   B     0         --             0         --
1   16   4    2   24   55   A     0         --             0         --
1   16   4    2   24   55   B     0         --             0         --
1   17   5    1   16   55   A     3 2009-06-26@21:06:04    3 2009-06-26@21:06:04
1   17   5    1   16   55   B     0         --             0         --
1   18   5    1   17   55   A     3 2009-06-26@21:06:04    3 2009-06-26@21:06:04
1   18   5    1   17   55   B     0         --             0         --
1   19   5    2    0   55   A     3 2009-06-26@21:06:19    3 2009-06-26@21:06:19
1   19   5    2    0   55   B     0         --             0         --
1   20   5    2   24   55   A     0         --             0         --
--More--
```

```
switch(config)# show hardware capacity power
Power Resources Summary:
------------------------
Power Supply redundancy mode(administratively):  PS-Redundant
Power Supply redundancy mode(operationally):     PS-Redundant
Total Power Capacity                             6000.00 W
Power reserved for SUP,Fabric,and Fan Module(s)  3230.00 W (
53.83 % )
Power currently used by Modules                   650.00 W (
10.83 % )
Total Power Available                            2120.00 W (
35.33 % )
Total Power Output (actual draw)                    0.00 W
switch#
```

Related Commands

Commands	Description
debug sme	Debugs Cisco SME features.

show hardware fabric-mode

To display fabric operation mode, use the **show hardware fabric mode** command.

show hardware fabric-mode

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the fabric operation mode:

```
switch# show hardware fabric-mode
Fabric mode supports Gen3 and above linecards.
switch#
```

Related Commands

Command	Description
show hardware	Displays brief information about the list of field replacable units (FRUs) in the switch.

show hosts

To display DNS host configuration details, use the **show hosts** command.

show hosts

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the configures hosts including the default domain, domain list, and name servers:

```
switch# show hosts
```

Default domain is cisco.com

Domain list: ucsc.edu harvard.edu yale.edu stanford.edu

Name/address lookup uses domain service

```
Name servers are 15.1.0.1 15.2.0.0
```

show incompatibility system

To display the high availability compatibility status between the current system image on both supervisors and the new system image to be installed on both supervisors, use the **show incompatibility system** command.

show incompatibility system [{**bootflash:**|**slot0:**|**volatile:**}] *image-filename*

Syntax Description

bootflash:	(Optional) Source or destination location for internal bootflash memory.
slot0:	(Optional) Source or destination location for the CompactFlash memory or PCMCIA card.
volatile:	(Optional) Source or destination location for the volatile directory.
image-filename	Specifies the name of the system image.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.
3.0(1)	Provided an example to show that the command output provides the commands needed to disable incompatible features.

Usage Guidelines

If the high availability compatibility is strict then the upgrade to that image will be disruptive for both supervisors.

If the high availability compatibility is loose , the synchronization may happen without errors, but some resources may become unusable when a switchover happens.

Examples

The following example displays kernel core settings:

```
switch# show incompatibility system bootflash:old-image-y
The following configurations on active are incompatible with the system image
1) Feature Index : 67 , Capability : CAP_FEATURE_SPAN_FC_TUNNEL_CFG
Description : SPAN - Remote SPAN feature using fc-tunnels
Capability requirement : STRICT
2) Feature Index : 119 , Capability : CAP_FEATURE_FC_TUNNEL_CFG
Description : fc-tunnel is enabled
Capability requirement : STRICT
```

The following example shows commands needed to disable incompatible features:

```
switch# show incompatibility system bootflash:m9200-ek9-mz.1.3.4b.bin
The following configurations on active are incompatible with the system image:
1) Service : cfs , Capability : CAP_FEATURE_CFS_ENABLED_DEVICE_ALIAS
Description : CFS - Distribution is enabled for DEVICE-ALIAS
Capability requirement : STRICT
Disable command : no device-alias distribute
```

show in-order-guarantee

To display the present configured state of the in-order delivery feature, use the **show in-order-guarantee** command.

show in-order-guarantee

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the present configuration status of the in-order delivery feature:

```
switch# show in-order-guarantee
global inorder delivery configuration:guaranteed
VSAN specific settings
vsan 1 inorder delivery:guaranteed
vsan 101 inorder delivery:not guaranteed
vsan 1000 inorder delivery:guaranteed
vsan 1001 inorder delivery:guaranteed
vsan 1682 inorder delivery:guaranteed
vsan 2001 inorder delivery:guaranteed
vsan 2009 inorder delivery:guaranteed
vsan 2456 inorder delivery:guaranteed
vsan 3277 inorder delivery:guaranteed
vsan 3451 inorder delivery:guaranteed
vsan 3452 inorder delivery:guaranteed
vsan 3453 inorder delivery:guaranteed
```

show install all failure-reason

To identify the cause of a nondisruptive software upgrade failure, use the show install all failure-reason command when prompted by the system.

show install all failure-reason

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

If an upgrade failure is due to some other cause, nothing is displayed when you enter the command. This command displays a valid output only if a service aborts an upgrade and a message instructing you to issue this command is returned to the CLI.

Examples

The following example displays the output during an unsuccessful nondisruptive software upgrade, and it shows the reason for the failure:

```
Do you want to continue with the installation (y/n)?  [n] y

Install is in progress, please wait.

Notifying services about the upgrade.
[#                   ]   0% -- FAIL. Return code 0x401E0066 (request timed out).

Please issue "show install all failure-reason" to find the cause of the failure.

Install has failed. Return code 0x401E0066 (request timed out).
Please identify the cause of the failure, and try 'install all' again.
switch# show install all failure-reason
Service: "cfs" failed to respond within the given time period.
switch#
```

Related Commands

Command	Description
show install all status	Displays the status of an installation or ISSU.

show install all impact

To display the software compatibility matrix of a specific image, use the **show install all impact** command.

show install all impact [**asm-sfn** *image-filename*] [**kickstart** *image-filename*] [**ssi** *image-filename*] [**system** *image-filename*]

Syntax Description

asm-sfn	(Optional) Specifies the ASM SFN boot variable.
image-filename	(Optional) Specifies the name of an image.
kickstart	(Optional) Specifies the kickstart boot variable.
ssi	(Optional) Specifies the SSI boot variable.
system	(Optional) Specifies the system boot variable.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

Use the **show install all impact** command to view the effect of updating the system from the running image to another specified image:

```
switch# show install all impact
Verifying image bootflash:/ilc1.bin
[####################] 100% -- SUCCESS
Verifying image bootflash:/vk73a
[####################] 100% -- SUCCESS
Verifying image bootflash:/vs73a
[####################] 100% -- SUCCESS
Extracting "slc" version from image bootflash:/vs73a.
[####################] 100% -- SUCCESS
Extracting "slc" version from image bootflash:/vs73a.
[####################] 100% -- SUCCESS
Extracting "system" version from image bootflash:/vs73a.
[####################] 100% -- SUCCESS
Extracting "kickstart" version from image bootflash:/vk73a.
[####################] 100% -- SUCCESS
Extracting "loader" version from image bootflash:/vk73a.
[####################] 100% -- SUCCESS
Extracting "slc" version from image bootflash:/vs73a.
[####################] 100% -- SUCCESS
Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
```

```
     2       yes  non-disruptive          none
     4       yes  non-disruptive          none
     6       yes  non-disruptive          none
     9       yes  non-disruptive          none
Images will be upgraded according to following table:
Module       Image       Running-Version           New-Version  Upg-Required
------  ----------  --------------------  --------------------  ------------
     2         slc                1.2(1)                1.2(1)            no
     2        bios      v1.0.7(03/20/03)      v1.0.7(03/20/03)            no
     4         slc                1.2(1)                1.2(1)            no
     4        ilce                1.2(1)                1.2(1)            no
     4        bios      v1.0.7(03/20/03)      v1.0.7(03/20/03)            no
     6      system                1.2(1)                1.2(1)            no
     6   kickstart                1.2(1)                1.2(1)            no
     6        bios      v1.0.7(03/20/03)      v1.0.7(03/20/03)            no
     6      loader               1.0(3a)               1.0(3a)            no
     9         slc                1.2(1)                1.2(1)            no
     9        bios      v1.0.7(03/20/03)      v1.0.7(03/20/03)            no
```

The following command displays the error message that is displayed if a wrong image is provided:

```
switch# show install all impact system bootflash:
Compatibility check failed. Return code 0x40930003 (Invalid bootvar specified in
 the input).
```

show install all status

To display the on going **install all** command status or the log of the last installed **install all** command from a console, SSH, or Telnet session, use the **show install all status** command.

show install all status

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

This command only displays the status of an **install all** command that is issued from the CLI, not Fabric Manager.

The show install all status command also displays the status of nondisruptive software upgrades on the Cisco MDS 9124 Fabric Switch (after the switch has rebooted and comes up with the new image). Actions that occurred before the reboot are not displayed in the output. So, if you issue the install all command via a Telnet session, the Telnet session will be disconnected when the switch reboots. After you reconnect to the switch using Telnet, the upgrade may already be complete; in this case, the show install all status command will display the status of the upgrade.

Examples

Use the **show install all status** command to view the output of a **install all** command process.

```
switch# show
 install all status
There is an on-going installation... <---------------------- in progress installation
Enter Ctrl-C to go back to the prompt.
Verifying image bootflash:/b-1.3.0.104
 -- SUCCESS
Verifying image bootflash:/i-1.3.0.104
 -- SUCCESS
Extracting "system" version from image bootflash:/i-1.3.0.104.
 -- SUCCESS
Extracting "kickstart" version from image bootflash:/b-1.3.0.104.
 -- SUCCESS
Extracting "loader" version from image bootflash:/b-1.3.0.104.
 -- SUCCESS
switch# show install all status
This is the log of last installation.          <<<<<< log of last install
Verifying image bootflash:/b-1.3.0.104
 -- SUCCESS
Verifying image bootflash:/i-1.3.0.104
 -- SUCCESS
Extracting "system" version from image bootflash:/i-1.3.0.104.
 -- SUCCESS
Extracting "kickstart" version from image bootflash:/b-1.3.0.104.
```

```
 -- SUCCESS
Extracting "loader" version from image bootflash:/b-1.3.0.104.
 -- SUCCESS
```

Use the show install all status command to view the output of a nondisrtuptive software upgrade process on the Cisco MDS 9124 Fabric Switch.

```
switch# show install all status
This is the log of last installation.
Continuing with installation process, please wait.
The login will be disabled until the installation is completed.
Status for linecard upgrade.
 -- SUCCESS
Performing supervisor state verification.
 -- SUCCESS
Install has been successful.
```

show interface

You can check the status of an interface, use the **show interface** command.

show interface [*interface-range*] [{**aggregate-counters [brief]**|**bbcredit**|**brief**|**capabilities**|**counters** [{**brief** [**module** *number*]|**debouncedetailed** **[snmp]**}]|**description**|**fcoe**|**flowcontrol**|**mac-address**|**status**|**switchport**|**transceiver** [{**calibrations**|**details**}]|**trunk vsan** [*vsan-id*]|**vlan mapping**}]

Syntax Description

interface-range	(Optional) Displays the type of interface.
aggregate-counters	(Optional) Displays interface aggregate counters for Fibre Channel interfaces.
bbcredit	(Optional) Displays buffer-to-buffer credit information for Fibre Channel interfaces.
brief	(Optional) Displays brief information for Fibre Channel and Ethernet interfaces.
capabilities	(Optional) Displays hardware port capabilities for Fibre Channel and Ethernet interfaces.
counters	(Optional) Displays the interface counter information for Fibre Channel and Ethernet interfaces.
module *number*	(Optional) Displays interface counter information of a module for Ethernet interfaces.
detailed	(Optional) Displays detailed transceiver diagnostics information for Fibre Channel and Ethernet interface.
all	(Optional) Displays detailed information of all counters for Ethernet interfaces.
snmp	(Optional) Displays Simple Network Management Protocol (SNMP) MIB values for Ethernet interfaces.
storm-control	(Optional) Displays storm-control counter information for Ethernet interfaces.
debounce	(Optional) Displays debounce time information for Ethernet interfaces.
description	(Optional) Displays the interface description for Fibre Channel and Ethernet interfaces.
fcoe	(Optional) Displays Fibre Channel over Ethernet (FCoE) information for Ethernet interfaces.
flowcontrol	(Optional) Displays FlowControl information for Ethernet interfaces.
mac-address	(Optional) Displays Ethernet MAC address for Ethernet interfaces.
status	(Optional) Displays status for Ethernet interfaces.
err-disabled	(Optional) Displays error disabled status for Ethernet interfaces.
err-vlans	(Optional) Displays VLANs that have errors for Ethernet interfaces.
switchport	(Optional) Displays switch port information for Ethernet interfaces.

transceiver	(Optional) Displays the transceiver information for Fibre Channel and Ethernet interfaces.
calibrations	(Optional) Displays transceiver calibration information for Fibre Channel and Ethernet interfaces.
sprom	(Optional) Displays transceiver sprom information for Ethernet interfaces.
trunk	(Optional) Displays the trunking status of all VSANs for Fibre Channel and Ethernet interfaces.
vsan *vsan-id*	(Optional) Displays the trunking status of the specified VSANs for Fibre Channel interfaces. The range is 1 to 4093.
vlan mapping	(Optional) Displays VLAN mapping information for Ethernet interfaces.

Command Default

Displays information for all interfaces on the switch.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
6.2(7)	Added FEC-related command output.
6.2(5)	Added the Cisco MDS 9250i Multiservice Fabric Switch output to the **show interface capabilities** command.
6.2(5)	Added the command output for detailed FCIP Interface Standard Counter Information, FCIP Interface Summary of Counters for a Specified Interface, and brief FCIP Interface Counter Information for Cisco MDS 9250i Multiservice Fabric Switch.
6.2(3)	Deprecated the **show interface counters performance** command.
6.2(1)	Added the **performance**, **module interval** keywords to the syntax description.
4.1(1b)	Added the command output for BB_credit information for a switch port.
4.1(1b)	Added the command output for interface capabilities on a 48 port module.
3.1(2)	Added the **bay** | **ext** interface.
3.0(1)	Added the **capabilities** option for Fibre Channel interfaces.
1.3(1)	Added the **bbcredit** keyword and support for cpp and fv interfaces.
1.0(2)	This command was introduced.

Usage Guidelines

You can specify a range of interfaces by issuing a command with the following example format:

interface fc1/1 - 5 , fc2/5 - 7

The spaces are required before and after the dash (-) and before and after the comma (,).

The **show interface** *slot/port* **transceiver** command can only be issued on a switch in the Cisco MDS 9100 Series if the SFP is present.

Note The **show interface counter** command will not display any output, if FCoE plug-in is not installed.

Table 9: Interface Types for the Show Interface Command, on page 1354 lists the interface types supported by the **show interface** command.

In the **show interface** *port/slot* **counters detailed** command output, the *Transmit B2B credit transitions to zero* counter increments every time the transmit buffer-to-buffer credits goes to zero. When the ISLs are in Hi-Lo mode, the buffer-to-buffer credits are divided for high priority and low-priority traffic. However, when the ISLs are in Hi-Lo mode, this counter does not increment though the low-priority credits go to zero because the high priority credits are still available.

Table 9: Interface Types for the Show Interface Command

Interface Type	Description
bay *port* | **ext** *port*	Displays information for a Fibre Channel interface on a Cisco Fabric Switch for HP c-Class BladeSystem or a Cisco Fabric Switch for IBM BladeCenter.
cpp *slot/port*	Displays information for a virtualization interface.
fc *slot/port*	Displays the Fibre Channel interface in the specified slot or port.
fc-tunnel *tunnel-id*	Displays description of the specified Fibre Channel tunnel from 1 to 4095.
fcip *interface-number*	Specifies an FCIP interface. The range is 1 to 255.
fv *slot/dpp-number/fv-port*	Displays information for the virtual F port (FV port) interface in the specified slot along with the data path processor (DPP) number and the FV port number.
gigabitethernet *slot/port*	Displays information for a Gigabit Ethernet interface at the specified slot and port.
gigabitethernet *slot/port.* *subinterface-number*	Displays information for a Gigabit Ethernet subinterface at the specified slot and port followed by a dot (.) indicator and the subinterface number. The subinterface range is 1 to 4093.
iscsi *slot/port*	Displays the description of the iSCSI interface in the specified slot and port.
mgmt 0	Displays the description of the management interface.
port-channel *port-channel-number*	Displays the port-channel interface specified by the port-channel number. The range is 1 to 128.

Interface Type	Description
port-channel *port-channel-number.subinterface-number*	Displays the port-channel subinterface specified by the port-channel number followed by a dot (.) indicator and the subinterface number. The port channel number range is 1 to 128. The subinterface range is 1 to 4093.
sup-fc 0	Displays the in-band interface details.
vsan *vsan-id*	Displays information for a VSAN. The range is 1 to 4093.

Examples

The following example shows how to display information about a Fibre Channel interface:

```
switch# show interface fc5/25
fc5/25 is up
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 21:19:8c:60:4f:54:54:00
    Peer port WWN is 20:19:00:2a:6a:fd:04:a0
    Admin port mode is auto, trunk mode is off
    snmp link state traps are enabled
    Port mode is E
    Port vsan is 1
    Admin Speed is auto
    Operating Speed is 4 Gbps
    Rate mode is dedicated
    Port flow-control is R_RDY
    Transmit B2B Credit is 64
    Receive B2B Credit is 500
    B2B State Change Number is 14
    Receive data field Size is 2112
    Beacon is turned off
    Local beaconing is on, warning @ 1.0 Hz, 175 sec remaining
    Peer beaconing is on, warning @ 1.0 Hz, 175 sec remaining
    Logical type is core
    Belongs to port-channel5
    5 minutes input rate 800 bits/sec,100 bytes/sec, 0 frames/sec
    5 minutes output rate 320 bits/sec,40 bytes/sec, 0 frames/sec
      57144 frames input,5333328 bytes
        0 discards,0 errors
        0 invalid CRC/FCS,0 unknown class
        0 too long,0 too short
      57172 frames output,2403756 bytes
        0 discards,0 errors
      0 input OLS,1  LRR,0 NOS,10 loop inits
      1 output OLS,1 LRR, 0 NOS, 1 loop inits
      500 receive B2B credit remaining
      64 transmit B2B credit remaining
      64 low priority transmit B2B credit remaining
    Last clearing of "show interface" counters :  never
```

The following example shows how to display detailed information for an interface:

```
switch# show interface fc2/1 detailed
fc2/1
      0 frames, 0 bytes received
      0 class-2 frames, 0 bytes received
      0 class-2 discards
      0 F_BSY frames, 0 F_RJT frames
```

```
      generated against class-2 frames
    0 port reject frames
    0 class-3 frames, 0 bytes received
    0 class-f frames, 0 bytes received
    0 discards, 0 errors received
    0 discards, 0 errors transmitted
    0 frames, 0 bytes transmitted
    0 class-2 frames, 0 bytes transmitted
    0 class-3 frames, 0 bytes transmitted
    0 class-3 frames discarded
    0 class-f frames, 0 bytes transmitted
    0 class-f frames discarded
    0 multicast packets received, 0 transmitted
    0 broadcast packets received, 0 transmitted
    0 unicast packets received, 0 transmitted
    0 timeout discards, 0 credit loss
    0 link failures, 0 sync losses,       0 signal losses
    0 primitive sequence protocol errors
    0 invalid transmission words
    0 invalid CRCs, 0 Delimiter Errors
    0 address identifier errors
    0 link reset received while link is active
    0 link reset transmitted while link is active
    0 Offline Sequence errors received
    0 Offline Sequence errors transmitted
    0 frames received that are shorter than
      the minimum allowable frame length
      regardless of the CRC/FCS error
    0 frames received that are longer than
      the maximum frame length and also have a
      CRC/FCS error
    0 2.5us TxWait due to lack of transmit credits
    0 frames received with length greater
      than what was agreed to in FLOGI/PLOGI
    0 frames received with length less than
      the minimum indicated by the frame header
    0 link reset responses received
    0 link reset responses transmitted
    0 non-operational sequences received
    0 non-operational sequences transmitted
    0 fragmented frames received
    0 frames received with EOF aborts
    0 unknown class frames received
    0 8b10b disparity errors
    0 frames discarded
    0 Exchange Link Parameters switch fabric
      internal link service request failures
    0 Transmit B2B credit transitions to zero
    0 Receive B2B credit transitions to zero
    0 Enhanced Inter Switch Link (EISL) frames
      discarded
    0 framing errors
    0 F8 type LIP sequence errors received
    0 F8 type LIP sequence errors issued
    0 Non F8 type LIP sequence errors received
    0 Non F8 type LIP sequence errors issued
    0 fec corrected blocks
    0 fec uncorrected blocks
    0 BB_SCs credit resend actions, 0 BB_SCr Tx credit increment actions
Percentage Tx credits not available for last 1s/1m/1h/72h: 0%/0%/0%/0%
```

The following example shows how to display detailed counters information for all interfaces:

```
switch# show interface counters detailed
fc1/1
      3837589242 frames, 7112275294800 bytes received
      0 class-2 frames, 0 bytes received
      0 class-2 discards
      0 F_BSY frames, 0 F_RJT frames
          generated against class-2 frames
      0 port reject frames
      3837589242 class-3 frames, 7112275294800 bytes received
      0 class-f frames, 0 bytes received
      0 discards, 0 errors received
      0 discards, 0 errors transmitted
      4014466889 frames, 7113138737884 bytes transmitted
      0 class-2 frames, 0 bytes transmitted
      4014466889 class-3 frames, 7113138737884 bytes transmitted
      0 class-3 frames discarded
      0 class-f frames, 0 bytes transmitted
      0 class-f frames discarded
      0 multicast packets received, 0 transmitted
      0 broadcast packets received, 0 transmitted
      3837589242 unicast packets received, 4014466889 transmitted
      0 Zone drops
      0 FIB drops for ports 1-16
      0 XBAR errors for ports 1-16
      0 Other drop count for ports 1-1
      0 timeout discards, 0 credit loss
      1 link failures, 0 sync losses,       0 signal losses
      0 primitive sequence protocol errors
      0 invalid transmission words
      0 invalid CRCs, 0 Delimiter Errors
      0 address identifier errors
      0 link reset received while link is active
      0 link reset transmitted while link is active
      2 Offline Sequence errors received
      1 Offline Sequence errors transmitted
      0 frames received that are shorter than
          the minimum allowable frame length
          regardless of the CRC/FCS error
      0 frames received that are longer than
          the maximum frame length and also have a
          CRC/FCS error
      0 2.5us TxWait due to lack of transmit credits
      0 frames received with length greater
          than what was agreed to in FLOGI/PLOGI
      0 frames received with length less than
          the minimum indicated by the frame header
      1 link reset responses received
      0 link reset responses transmitted
      3 non-operational sequences received
      3 non-operational sequences transmitted
      0 fragmented frames received
      0 frames received with EOF aborts
      0 unknown class frames received
      0 8b10b disparity errors
      0 frames discarded
      0 Exchange Link Parameters switch fabric
          internal link service request failures
      3 Transmit B2B credit transitions to zero
      1 Receive B2B credit transitions to zero
      0 Enhanced Inter Switch Link (EISL) frames
          discarded
      0 framing errors
      0 F8 type LIP sequence errors received
```

```
      0 F8 type LIP sequence errors issued
      0 Non F8 type LIP sequence errors received
      0 Non F8 type LIP sequence errors issued
      0 fec corrected blocks
      0 fec uncorrected blocks
      0 BB_SCs credit resend actions, 0 BB_SCr Tx credit increment actions
Percentage Tx credits not available for last 1s/1m/1h/72h: 0%/0%/0%/0%
fc1/2
      1 frames, 124 bytes received
      0 class-2 frames, 0 bytes received
      0 class-2 discards
      0 F_BSY frames, 0 F_RJT frames
          generated against class-2 frames
      0 port reject frames
      1 class-3 frames, 124 bytes received
      0 class-f frames, 0 bytes received
      0 discards, 0 errors received
      0 discards, 0 errors transmitted
      1 frames, 124 bytes transmitted
      0 class-2 frames, 0 bytes transmitted
      1 class-3 frames, 124 bytes transmitted
      0 class-3 frames discarded
      0 class-f frames, 0 bytes transmitted
      0 class-f frames discarded
      0 multicast packets received, 0 transmitted
      0 broadcast packets received, 0 transmitted
      1 unicast packets received, 1 transmitted
      0 Zone drops
      0 FIB drops for ports 1-16
      0 XBAR errors for ports 1-16
      0 Other drop count for ports 2-2
      0 timeout discards, 0 credit loss
      0 link failures, 0 sync losses,       0 signal losses
      0 primitive sequence protocol errors
      0 invalid transmission words
      0 invalid CRCs, 0 Delimiter Errors
      0 address identifier errors
      1 link reset received while link is active
      0 link reset transmitted while link is active
      0 Offline Sequence errors received
      2 Offline Sequence errors transmitted
      0 frames received that are shorter than
          the minimum allowable frame length
          regardless of the CRC/FCS error
      0 frames received that are longer than
          the maximum frame length and also have a
          CRC/FCS error
      0 2.5us TxWait due to lack of transmit credits
      0 frames received with length greater
          than what was agreed to in FLOGI/PLOGI
      0 frames received with length less than
          the minimum indicated by the frame header
      0 link reset responses received
      2 link reset responses transmitted
      0 non-operational sequences received
      0 non-operational sequences transmitted
      0 fragmented frames received
      0 frames received with EOF aborts
      0 unknown class frames received
      0 8b10b disparity errors
      0 frames discarded
      0 Exchange Link Parameters switch fabric
          internal link service request failures
      3 Transmit B2B credit transitions to zero
```

```
      2 Receive B2B credit transitions to zero
      0 Enhanced Inter Switch Link (EISL) frames
          discarded
      0 framing errors
      0 F8 type LIP sequence errors received
      0 F8 type LIP sequence errors issued
      0 Non F8 type LIP sequence errors received
      0 Non F8 type LIP sequence errors issued
      0 fec corrected blocks
      0 fec uncorrected blocks
      0 BB_SCs credit resend actions, 0 BB_SCr Tx credit increment actions
Percentage Tx credits not available for last 1s/1m/1h/72h: 0%/0%/0%/0%
fc1/3
      3837597762 frames, 7112201084308 bytes received
      0 class-2 frames, 0 bytes received
      0 class-2 discards
      0 F_BSY frames, 0 F_RJT frames
          generated against class-2 frames
      0 port reject frames
      3837597762 class-3 frames, 7112201084308 bytes received
      0 class-f frames, 0 bytes received
      0 discards, 0 errors received
      0 discards, 0 errors transmitted
      4016213212 frames, 7116625022780 bytes transmitted
      0 class-2 frames, 0 bytes transmitted
      4016213212 class-3 frames, 7116625022780 bytes transmitted
      0 class-3 frames discarded
      0 class-f frames, 0 bytes transmitted
      0 class-f frames discarded
      0 multicast packets received, 0 transmitted
      0 broadcast packets received, 0 transmitted
      3837597762 unicast packets received, 4016213212 transmitted
      0 Zone drops
      0 FIB drops for ports 1-16
      0 XBAR errors for ports 1-16
      0 Other drop count for ports 3-3
      0 timeout discards, 0 credit loss
      1 link failures, 0 sync losses,       0 signal losses
      0 primitive sequence protocol errors
      0 invalid transmission words
      0 invalid CRCs, 0 Delimiter Errors
      0 address identifier errors
      0 link reset received while link is active
      0 link reset transmitted while link is active
      2 Offline Sequence errors received
      1 Offline Sequence errors transmitted
      0 frames received that are shorter than
          the minimum allowable frame length
          regardless of the CRC/FCS error
      0 frames received that are longer than
          the maximum frame length and also have a
          CRC/FCS error
      0 2.5us TxWait due to lack of transmit credits
      0 frames received with length greater
          than what was agreed to in FLOGI/PLOGI
      0 frames received with length less than
          the minimum indicated by the frame header
      1 link reset responses received
      0 link reset responses transmitted
      2 non-operational sequences received
      2 non-operational sequences transmitted
      0 fragmented frames received
      0 frames received with EOF aborts
      0 unknown class frames received
```

```
      0 8b10b disparity errors
      0 frames discarded
      0 Exchange Link Parameters switch fabric
          internal link service request failures
      3 Transmit B2B credit transitions to zero
      1 Receive B2B credit transitions to zero
      0 Enhanced Inter Switch Link (EISL) frames
          discarded
      0 framing errors
      0 F8 type LIP sequence errors received
      0 F8 type LIP sequence errors issued
      0 Non F8 type LIP sequence errors received
      0 Non F8 type LIP sequence errors issued
      0 fec corrected blocks
      0 fec uncorrected blocks
      0 BB_SCs credit resend actions, 0 BB_SCr Tx credit increment actions
Percentage Tx credits not available for last 1s/1m/1h/72h: 0%/0%/0%/0%
.
.
.
```

The following example shows how to display aggregate counters information for an interface:

```
switch# show interface fc1/3 aggregate-counters
fc1/3
    5 minutes input rate 192 bits/sec, 24 bytes/sec, 0 frames/sec
    5 minutes output rate 160 bits/sec, 20 bytes/sec, 0 frames/sec
    40022 frames input, 2081144 bytes
      0 class-2 frames, 0 bytes
      40022 class-3 frames, 2081144 bytes
      0 class-f frames, 0 bytes
      0 discards, 0 errors, 0 CRC/FCS
      0 unknown class, 0 too long, 0 too short
    40022 frames output, 1760968 bytes
      0 class-2 frames, 0 bytes
      40022 class-3 frames, 1760968 bytes
      0 class-f frames, 0 bytes
      0 discards, 0 errors
    0 input OLS, 0 LRR, 0 NOS, 0 loop inits
    0 output OLS, 0 LRR, 0 NOS, 0 loop inits
    0 link failures, 0 sync losses, 0 signal losses
     0 transmit B2B credit transitions to zero
     0 receive B2B credit transitions to zero
      32 receive B2B credit remaining
      80 transmit B2B credit remaining
      80 low priority transmit B2B credit remaining
```

The following example shows how to display the BB_credit information for a switch port:

```
switch# show interface fc1/1 bbcredit
fc1/1 is up
    Transmit B2B Credit is 16
    Receive B2B Credit is 16
      17 receive B2B credit remaining
      16 transmit B2B credit remaining
```

The following example shows how to display information about the in-band interface:

```
switch# show interface sup-fc0
sup-fc0 is up
    Hardware is FastEthernet, address is 0000.0000.0000
    MTU 2596 bytes, BW 1000000 Kbit
    66 packets input, 7316 bytes
    Received 0 multicast frames, 0 compressed
    0 input errors, 0 frame, 0 overrun 0 fifo
    64 packets output, 28068 bytes, 0 underruns
    0 output errors, 0 collisions, 0 fifo
    0 carrier errors
```

The following example shows how to display information about a VSAN interface:

```
switch# show interface vsan 2
vsan2 is up, line protocol is up
    WWPN is 10:00:00:05:30:00:59:1f, FCID is 0xb90100
    Internet address is 10.1.1.1/24
    MTU 1500 bytes, BW 1000000 Kbit
    0 packets input, 0 bytes, 0 errors, 0 multicast
    0 packets output, 0 bytes, 0 errors, 0 dropped
```

The following example shows how to display description information for all interfaces:

```
switch# show interface description
fc1/1
    no description
fc1/2
    no description
fc1/15
fcAnl
sup-fc0 is up
mgmt0 is up
vsan1 - IPFC interface
port-channel 15
no description
port-channel 98
no description
```

The following example shows how to display the debounce time information for Ethernet interfaces:

```
switch# show interface ethernet1/3 debounce

--------------------------------------------------------------------------------
Port          Debounce time   Value(ms)    Debounce(link-up)    Value(ms)
--------------------------------------------------------------------------------
Eth1/3        enable              100
```

The following example shows how to display the FCoE interface information:

```
switch# show interface ethernet1/3 fcoe
Ethernet1/3 is FCoE UP
vfc1/3 is bound
```

The following example shows how to display the FlowControl information for Ethernet interfaces:

```
switch# show interface ethernet1/3 flowcontrol

--------------------------------------------------------------------------------
Port         Send FlowControl  Receive FlowControl  RxPause   TxPause
             admin    oper     admin    oper
--------------------------------------------------------------------------------
Eth1/3       off      off      off      off         0         0
```

The following example shows how to display the switch port information for Ethernet interfaces:

```
switch# show interface ethernet1/3 switchport
Name: Ethernet1/3
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: trunk
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Allowed: 1-4094
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs: none
  Operational private-vlan: none
```

The following example shows how to display brief information for a range of interfaces:

```
switch# show interface fc1/1 - 16 brief
--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          Oper  Oper   Port-channel
                  Mode   Trunk                   Mode  Speed
                         Mode                          (Gbps)
--------------------------------------------------------------------------------
fc1/1      1      auto   on      down            --    --     --
fc1/2      1      auto   on      fcotAbsent      --    --     --
fc1/3      1      F      --      notConnected    --    --     --
fc1/4      1      auto   on      fcotAbsent      --    --     --
fc1/5      1      F      --      up              F     2      --
fc1/6      1      auto   on      fcotAbsent      --    --     --
fc1/7      1      auto   on      down            --    --     --
fc1/8      1      auto   on      fcotAbsent      --    --     --
fc1/9      1      auto   on      fcotAbsent      --    --     --
fc1/10     1      auto   on      fcotAbsent      --    --     --
fc1/11     1      auto   on      down            --    --     --
fc1/12     1      auto   on      fcotAbsent      --    --     --
fc1/13     1      auto   on      down            --    --     --
fc1/14     1      auto   on      fcotAbsent      --    --     --
fc1/15     1      auto   on      down            --    --     --
fc1/16     1      auto   on      fcotAbsent      --    --     --
--------------------------------------------------------------------------------
Interface          Status   IP Address              Speed        MTU
--------------------------------------------------------------------------------
sup-fc0            up       --                      1 Gbps       2596
--------------------------------------------------------------------------------
Interface          Status   IP Address              Speed        MTU
```

```
--------------------------------------------------------------------------------
mgmt0              up       173.95.112/24         100 Mbps     1500
--------------------------------------------------------------------------------
Interface          Status   IP Address               Speed        MTU
--------------------------------------------------------------------------------
vsan1                 up    10.1.1.1/24              1 Gbps       1500
```

The following example shows how to display counter information for an FCIP interface:

```
switch# show interface fcip 3 counters
fcip3
    TCP Connection Information
      2 Active TCP connections
        Control connection: Local 43.1.1.2:3225, Remote 43.1.1.1:65532
        Data connection: Local 43.1.1.2:3225, Remote 43.1.1.1:65534
      30 Attempts for active connections, 0 close of connections
    TCP Parameters
      Path MTU 1500 bytes
      Current retransmission timeout is 300 ms
      Round trip time: Smoothed 10 ms, Variance: 5
      Advertised window: Current: 122 KB, Maximum: 122 KB, Scale: 1
      Peer receive window: Current: 114 KB, Maximum: 114 KB, Scale: 1
      Congestion window: Current: 2 KB, Slow start threshold: 1048560 KB
    5 minutes input rate 64 bits/sec, 8 bytes/sec, 0 frames/sec
    5 minutes output rate 64 bits/sec, 8 bytes/sec, 0 frames/sec
      910 frames input, 84652 bytes
         910 Class F frames input, 84652 bytes
         0 Class 2/3 frames input, 0 bytes
         0 Error frames timestamp error 0
      908 frames output, 84096 bytes
         908 Class F frames output, 84096 bytes
         0 Class 2/3 frames output, 0 bytes
         0 Error frames 0 reass frames
```

The following example displays Detailed FCIP Interface Standard Counter Information (Cisco MDS 9250i Multiservice Fabric Switch):

```
switch# show interface fcip 1 counters
fcip1
    TCP Connection Information
      4 Active TCP connections
        Local 20.1.1.1:3225, Remote 20.1.1.2:65461
        0 host table full 0 target entries in use
        9 Attempts for active connections, 1 close of connections
    TCP Parameters
      Path MTU 2500 bytes
      Current retransmission timeout is 200 ms
      Round trip time: Smoothed 1 ms, Variance: 1 Jitter: 160 us
      Advertized window: Current: 21 KB, Maximum: 24580 KB, Scale: 5
      Peer receive window: Current: 22 KB, Maximum: 23 KB, Scale: 5
      Congestion window: Current: 50 KB, Slow start threshold: 1950 KB
      Current Send Buffer Size: 16406 KB, Requested Send Buffer Size:             16384 KB
      CWM Burst Size: 50 KB
      Measured RTT : 14 us Min RTT: 14 us Max RTT: 123 us
      5 minutes input rate 1606526656 bits/sec, 200815832 bytes/sec, 91936 frames/sec
      5 minutes output rate 1895239000 bits/sec, 236904875 bytes/sec, 108473 frames/sec
         1153194273 frames input, 2518904877636 bytes
      5307 Class F frames input, 703296 bytes
      1153188966 Class 2/3 frames input, 2518904174340 bytes
      45778 Reass frames
      0 Error frames timestamp error 0
```

```
      1360260711 frames output, 2970799627892 bytes
    4652 Class F frames output, 516420 bytes
    1360256059 Class 2/3 frames output, 2970799111472 bytes
    0 Error frames
  IP compression statistics
    3487446379048 rxbytes
    43870538612 rxbytes compressed, 53208 rxbytes non-compressed
    79.49 rx compression ratio
          2762188144144 txbytes
          34388048802 txbytes compressed, 39096 txbytes non-compressed
          80.32 tx compression ratio
    34391222079 txbytes compressed
    IP compression flow control statistics
    0 bytes queued for hw compression
    0 queued for hardware compression
    4294967280 queued for hardware decompression
    2182 slowed tcp flow control
    101547965 accelerated tcp flow control
    127206019 side band flow control ON
    7048198 side band flow control OFF
```

The following example displays brief FCIP Interface Counter Information (SSN-16/18+4):

```
switch# show interface fcip 3 counters brief
2-42
Cisco MDS 9000 Family NX-OS IP Services Configuration Guide
OL-29294-02
Chapter 2 Configuring FCIP
Configuring FCIP
--------------------------------------------------------------------------------
Interface Input (rate is 5 min avg) Output (rate is 5 min avg)
------------------------------ ------------------------------
Rate Total Rate Total
Mbits/s Frames Mbits/s Frames
--------------------------------------------------------------------------------
fcip3 9 0 9 0
```

The following example displays brief FCIP Interface Counter Information (Cisco MDS 9250i Multiservice Fabric Switch):

```
switch# show interface fcip 1-12 counters brief
------------------------------------------------------------------------
Interface Input (rate is 5 min avg)     Output (rate is 5 min avg)
------------------------------ ------------------------------
 Rate Total           Rate Total
 MB/s Frames          MB/s Frames
------------------------------------------------------------------------
fcip1  191 1155974124        225 1363537690
fcip2  173 1046686124        227 1372311228
fcip3  0 0       0   0
fcip4  0 0       0   0
fcip5  0 0       0   0
fcip6  0 0       0   0
fcip7  189 1143612956        221 1339130294
fcip8  194 1167499884        218 1317700800
fcip9  0 0       0   0
fcip10 0 0       0   0
```

The following example shows how to display counter information for all interfaces:

```
switch# show interface fc9/1-48 counters brief
-------------------------------------------------------------------------------
Interface          Input (rate is 5 min avg)      Output (rate is 5 min avg)
                   ---------------------------  ---------------------------
                   Rate     Total               Rate     Total
                   MB/s     Frames              MB/s     Frames
-------------------------------------------------------------------------------
fc9/1              0        0                   0        0
fc9/2              0        0                   0        0
fc9/3              0        0                   0        0
fc9/4              0        0                   0        0
.
.
.
-------------------------------------------------------------------------------
Interface          Input (rate is 5 min avg)      Output (rate is 5 min avg)
                   ---------------------------  ---------------------------
                   Rate     Total               Rate     Total
                   MB/s     Frames              MB/s     Frames
-------------------------------------------------------------------------------
iscsi4/1           0        0                   0        0
iscsi4/2           0        0                   0        0
iscsi4/3           0        0                   0        0
iscsi4/4           0        0                   0        0
.
.
.
vsan10 is up, line protocol is up
    WWPN is 10:00:00:05:30:00:07:23, FCID is 0xee0001
    Internet address is 10.1.1.5/24
    MTU 1500 bytes, BW 1000000 Kbit
    0 packets input, 0 bytes, 0 errors, 0 multicast
    0 packets output, 0 bytes, 0 errors, 0 dropped
-------------------------------------------------------------------------------
Interface          Input (rate is 5 min avg)      Output (rate is 5 min avg)
                   ---------------------------  ---------------------------
                   Rate     Total               Rate     Total
                   MB/s     Frames              MB/s     Frames
-------------------------------------------------------------------------------
port-channel 100   0        0                   0        0
-------------------------------------------------------------------------------
Interface          Input (rate is 5 min avg)      Output (rate is 5 min avg)
                   ---------------------------  ---------------------------
                   Rate     Total               Rate     Total
                   Mbits/s  Frames              Mbits/s  Frames
-------------------------------------------------------------------------------
fcip2              0        0                   0        0
fcip3              9        0                   9        0
fcip6              8        0                   8        0
fcip7              8        0                   8        0
```

The following example displays the FCIP Interface Summary of Counters for a Specified Interface (SSN-16/18+4):

```
switch# show interface fcip 10
fcip10 is up
Hardware is GigabitEthernet
Port WWN is 20:d0:00:0c:85:90:3e:80
Peer port WWN is 20:d4:00:0c:85:90:3e:80
Admin port mode is auto, trunk mode is on
Port mode is E, FCID is 0x720000
```

```
Port vsan is 91
Speed is 1 Gbps
2-39
Cisco MDS 9000 Family NX-OS IP Services Configuration Guide
OL-29294-02
Chapter 2 Configuring FCIP
Configuring FCIP
Using Profile id 91 (interface GigabitEthernet4/1)
Peer Information
Peer Internet address is 3.3.3.2 and port is 3225
Write acceleration mode is off
Tape acceleration mode is off
Tape Accelerator flow control buffer size is 256 KBytes
IP Compression is disabled
Special Frame is disabled
Maximum number of TCP connections is 2
Time Stamp is disabled
QOS control code point is 0
QOS data code point is 0
B-port mode disabled
TCP Connection Information
50529025 Active TCP connections
Local 0.0.0.7:6, Remote 0.0.0.200:0
0 host table full 0 target entries in use
211419104 Attempts for active connections, 1500 close of connections
TCP Parameters
Path MTU 124160 bytes
Current retransmission timeout is 124160 ms
Round trip time: Smoothed 127829 ms, Variance: 14336
Advertized window: Current: 0 KB, Maximum: 14 KB, Scale: 14336
Peer receive window: Current: 0 KB, Maximum: 0 KB, Scale: 51200
Congestion window: Current: 14 KB, Slow start threshold: 49344 KB
Current Send Buffer Size: 206463 KB, Requested Send Buffer Size: 429496728
3 KB
CWM Burst Size: 49344 KB
5 minutes input rate 491913172779207224 bits/sec, 61489146597400903 bytes/se
c, 0 frames/sec
5 minutes output rate 491913175298921320 bits/sec, 61489146912365165 bytes/s
ec, 14316551 frames/sec
5702 frames input, 482288 bytes
5697 Class F frames input, 481736 bytes
5 Class 2/3 frames input, 552 bytes
0 Reass frames
0 Error frames timestamp error 0
5704 frames output, 482868 bytes
5698 Class F frames output, 482216 bytes
6 Class 2/3 frames output, 652 bytes
0 Error frames
```

The following example displays the FCIP interface counters for a specified interface (Cisco MDS 9250i Multiservice Fabric Switch):

```
switch# show interface fcip 1
fcip1 is trunking
Hardware is IPStorage
Port WWN is 20:2b:54:7f:ee:1c:2f:a0
Peer port WWN is 20:2b:00:2a:6a:1b:4f:90
Admin port mode is auto, trunk mode is on
snmp link state traps are enabled
Port mode is TE
Port vsan is 1
Speed is 5 Gbps
Trunk vsans (admin allowed and active) (1-2)
```

```
Trunk vsans (up) (1)
Trunk vsans (isolated) (2)
Trunk vsans (initializing) ()
Interface last changed at Fri Sep 15 05:23:27 2000
Using Profile id 1 (interface IPStorage1/1)
Peer Information
Peer Internet address is 20.1.1.2 and port is 3225
Write acceleration mode is configured off
Tape acceleration mode is configured off
Tape Accelerator flow control buffer size is automatic
FICON XRC Accelerator is configured off
Ficon Tape acceleration configured off for all vsans
IP Compression is enabled and set for auto
Maximum number of TCP connections is 4
QOS control code point is 0
QOS data code point is 0
TCP Connection Information
4 Active TCP connections
Local 20.1.1.1:3225, Remote 20.1.1.2:65461
0 host table full 0 target entries in use
9 Attempts for active connections, 1 close of connections
TCP Parameters
Path MTU 2500 bytes
Current retransmission timeout is 200 ms
Round trip time: Smoothed 2 ms, Variance: 3 Jitter: 157 us
Advertized window: Current: 21 KB, Maximum: 24580 KB, Scale: 5
Peer receive window: Current: 22 KB, Maximum: 23 KB, Scale: 5
Congestion window: Current: 50 KB, Slow start threshold: 1950 KB
Current Send Buffer Size: 16406 KB, Requested Send Buffer Size: 16384 KB
CWM Burst Size: 50 KB
Measured RTT : 14 us Min RTT: 14 us Max RTT: 118 us
5 minutes input rate 1606903776 bits/sec, 200862972 bytes/sec, 91958 frames/sec
5 minutes output rate 1895828792 bits/sec, 236978599 bytes/sec, 108506 frames/sec
1150774702 frames input, 2513619834588 bytes
5299 Class F frames input, 702192 bytes
1150769403 Class 2/3 frames input, 2513619132396 bytes
45778 Reass frames
0 Error frames timestamp error 0
1357408380 frames output, 2964570149576 bytes
4646 Class F frames output, 515904 bytes
1357403734 Class 2/3 frames output, 2964569633672 bytes
0 Error frames
```

The following example shows how to display information about a Gigabit Ethernet interface:

```
switch# show interface gigabitethernet 4/1
GigabitEthernet4/1 is up
    Hardware is GigabitEthernet, address is 0005.3000.2e12
    Internet address is 100.1.1.2/24
    MTU 1500 bytes, BW 1000000 Kbit
    Port mode is IPS
    Speed is 1 Gbps
    Beacon is turned off
    5 minutes input rate 32 bits/sec, 4 bytes/sec, 0 frames/sec
    5 minutes output rate 88 bits/sec, 11 bytes/sec, 0 frames/sec
    637 packets input, 49950 bytes
      0 multicast frames, 0 compressed
      0 input errors, 0 frame, 0 overrun 0 fifo
    659 packets output, 101474 bytes, 0 underruns
      0 output errors, 0 collisions, 0 fifo
      0 carrier errors
```

The following example shows how to display information about an iSCSI interface:

```
switch# show interface iscsi 2/1
iscsi2/1 is up
    Hardware is GigabitEthernet
    Port WWN is 20:41:00:05:30:00:50:de
    Admin port mode is ISCSI
    Port mode is ISCSI
    Speed is 1 Gbps
    iSCSI initiator is identified by name
    Number of iSCSI session: 7, Number of TCP connection: 7
    Configured TCP parameters
        Local Port is 3260
        PMTU discover is disabled
        Keepalive-timeout is 1 sec
        Minimum-retransmit-time is 300 ms
        Max-retransmissions 8
        Sack is disabled
        Minimum available bandwidth is 0 kbps
        Estimated round trip time is 0 usec
    5 minutes input rate 265184 bits/sec, 33148 bytes/sec, 690 frames/sec
    5 minutes output rate 375002168 bits/sec, 46875271 bytes/sec, 33833 frames/sec
    iSCSI statistics
      6202235 packets input, 299732864 bytes
        Command 6189718 pdus, Data-out 1937 pdus, 1983488 bytes, 0 fragments
      146738794 packets output, 196613551108 bytes
        Response 6184282 pdus (with sense 4), R2T 547 pdus
        Data-in 140543388 pdus, 189570075420 bytes
```

The following example shows how to display transceiver information for a Fibre Channel interface:

```
switch# show interface fc2/5 transceiver
fc2/5 fcot is present
    name is CISCO-INFINEON
    part number is V23848-M305-C56C
    revision is A3
    serial number is 30000474
    fc-transmitter type is short wave laser
    cisco extended id is unknown (0x0)
```

The following example shows how to display information about a Fibre Channel tunnel interface:

```
switch# show interface fc-tunnel 200
fc-tunnel 200 is up
Dest   IP Addr: 200.200.200.7   Tunnel ID: 200
Source IP Addr: 200.200.200.4   LSP ID: 1
Explicit Path Name:
```

The following example shows how to display interface capabilities on a 48 port line card:

```
switch# show interface fc1/24 linecard
Min Speed is 1 Gbps
Max Speed is 2 Gbps
FC-PH Version (high, low)                       (32,32)
Receive data field size (max/min)               (2112/256) bytes
Transmit data field size (max/min)              (2112/128) bytes
Classes of Service supported are                Class 2, Class 3, Class
Class 2 sequential delivery                     supported
Class 3 sequential delivery                     supported
```

```
Hold time (max/min)                                (100000/1) micro sec
BB state change notification                       supported
Maximum BB state change notifications              14
Rate Mode change                                   not supported
Rate Mode Capabilities                             Dedicated
 Receive BB Credit modification supported            yes
 FX mode Receive BB Credit (min/max/default) (1/255/16)
 ISL mode Receive BB Credit (min/max/default) (2/255/255)
 Performance buffer modification supported       yes
 FX mode Performance buffers (min/max/default) (1/145/0)
 ISL mode Performance buffers (min/max/default) (1/145/0)
Out of Service capable                              no
Beacon mode configurable                            yes
```

The following example shows how to display hardware port information for a Fibre Channel interface:

```
switch# show interface fc1/24 capabilities
 Min Speed is 1 Gbps
 Max Speed is 4 Gbps
 FC-PH Version (high, low)                          (0,6)
 Receive data field size (max/min)                  (2112/256)  bytes
 Transmit data field size (max/min)                 (2112/128)  bytes
 Classes of Service supported are                   Class 2, Class 3, Class F
 Class 2 sequential delivery                        supported
 Class 3 sequential delivery                        supported
 Hold time (max/min)                                (100/1) micro sec
 BB state change notification                       supported
 Maximum BB state change notifications              14
 Rate Mode change                                   supported
 Rate Mode Capabilities                             Shared        Dedicated
  Receive BB Credit modification supported             yes             yes
  FX mode Receive BB Credit (min/max/default)      (0/0/0)         (1/60/16)
  ISL mode Receive BB Credit (min/max/default)         --          (2/60/16)
  Performace buffer modification supported             no               no
 Out of Service capable                              yes
 Beacon mode configurable                            yes
```

Note The maximum credit can be configured only if we move other ports to minimum credits.

```
switch(config-if)# show interface capabilities
fc1/1
Min Speed is 2 Gbps
Max Speed is 16 Gbps
FC-PH Version (high, low)                    (0,6)
Receive data field size (max/min)            (2112/256) bytes
Transmit data field size (max/min)           (2112/128) bytes
Classes of Service supported are              Class 2, Class 3, Class F
Class 2 sequential delivery                   supported
Class 3 sequential delivery                   supported
Hold time (max/min)                           (100000/1) micro sec
BB state change notification                  supported
Maximum BB state change notifications         14
Rate Mode change                              not supported
Rate Mode Capabilities                        Dedicated
Receive BB Credit modification supported      yes
FX mode Receive BB Credit (min/max/default)   (1/64/64)
ISL mode Receive BB Credit (min/max/default)  (2/64/64)
Performance buffer modification supported     no
```

```
Out of Service capable                          yes
Beacon mode configurable                        yes
Extended B2B credit capable                     no
On demand port activation license supported   yes
.
.
.
```

The following example shows how to display information about a Fibre Channel interface on a Cisco Fabric Switch for HP c-Class BladeSystem:

```
switch# show interface bay 11
bay11 is down (Externally Disabled)
 Hardware is Fibre Channel
 Port WWN is 20:0c:00:05:30:01:f9:f2
 Admin port mode is auto, trunk mode is on
 snmp link state traps are enabled
 Port vsan is 1
 Receive data field Size is 2112
 Beacon is turned off
 5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
 5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
 0 frames input, 0 bytes
 0 discards, 0 errors
 0 CRC, 0 unknown class
 0 too long, 0 too short
 0 frames output, 0 bytes
 0 discards, 0 errors
 0 input OLS, 0 LRR, 0 NOS, 0 loop inits
 0 output OLS, 0 LRR, 0 NOS, 0 loop inits
```

The following example shows how to display the performance counter values for all the ports in all the modules with default interval of 20.

```
switch# show interface counters performance module 1 interval 20
switch#
```

show interface ioa

To display IOA interface, use the show interface ioa command.

show interface ioa *slot/port* {**brief**|**counters brief**|**description**}

Syntax Description

slot /port	Specifies an IOA slot or port number. The range is from 1 to 16 for the slot and for the port the range is from 1 to 4.
brief	Specifies brief information about the interface.
counters	Specifies the interface counters.
description	Specifies the interface description.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 6.2(5)	Added the show interface ioa 1/1 counters brief command to show the average for 5minutes , 12 hour and 24 hour respectively.
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to displayan IOA interface:

```
switch# show interface ioa 2/1
ioa2/1 is down (Not in any Cluster)
0 device packets in, 0 device packets out
0 device bytes in, 0 device bytes out
0 peer packets in, 0 peer packets out
0 peer bytes in, 0 peer bytes out
0 i-t create request, 0 i-t create destroy
0 i-t activate request, 0 i-t deactivate request
```

The following example shows how to display IOA interface counters:

```
switch# show interface ioa 2/1 counters
ioa1/1
4454232796 device packets in, 375748229 device packets out
8948409208760 device bytes in, 24047886946 device bytes out
526563297 peer packets in, 2471396408 peer packets out
45198770258 peer bytes in, 4697995629324 peer bytes out
8 i-t create request, 4 i-t create destroy
8 i-t activate request, 0 i-t deactivate request
```

The following example shows how to display IOA interface counters in brief:

```
switch# show int ioa 2/1 counters brief
------------------------------------------------------------------------------
Interface To Device (rate is 5 min avg) To Peer (rate is 5 min avg)
---------------------------- ----------------------------
Rate Total Rate Total
MB/s Bytes MB/s Bytes
------------------------------------------------------------------------------
ioa1/1 0.56 24049257618 109.66 4698262901274
sjc-sw2# show ioa int int ioa 2/1 summary
---- ---------------------- ---- ------------- ---- ---
FLOW HOST VSAN STATUS COMP ACC
TARGET
---- ---------------------- ---- ------------- ---- ---
1 10:00:00:00:00:00:03:00 200 ACTIVE YES WA
11:00:00:00:00:00:03:00
2 10:00:00:00:00:00:02:00 200 ACTIVE NO WA
11:00:00:00:00:00:02:00
3 10:00:00:00:00:00:01:00 100 ACTIVE YES TA
11:00:00:00:00:00:01:00
4 10:00:00:00:00:00:00:00 100 ACTIVE NO TA
11:00:00:00:00:00:00:00
switch(config-if)# show interface ioa 1/1 counters brief
------------------------------------------------------------------------------
Interface          Rate          Rate          Rate          Total
                        MB/s          MB/s          MB/s          Bytes
                       (5min)        (12hr)        (24hr)         (MB)
------------------------------------------------------------------------------
                       To  Device (Average)
ioa1/1              0.00        0.00             0.00             0.02
                       To  Peer   (Average)
                        0.00             0.00         0.00             0.05
```

Related Commands

Command	Description
show ioa cluster summary	Displays the summary of all the IOA clusters.

show interface sme

To display the information about Cisco SME interface, use the show interface sme command.

show interface sme *slot/port* {**brief**|**counters**|**description**}

Syntax Description

slot	Identifies the number of the MPS-18/4 module slot.
port	Identifies the number of the Cisco SME port.
brief	Displays the brief information about Cisco SME interface.
counters	Displays the interface counters.
description	Displays the description of the interface.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the brief description of the Cisco SME interface:

```
switch# show interface sme 3/1 brief
--------------------------------------------------------------------------------
Interface          Status        Cluster
--------------------------------------------------------------------------------
sme3/1             up            c2
```

The following example displays the counters of the interface:

```
switch# show interface sme 3/1 description
sme3/1
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0.00 KB/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0.00 KB/sec
    SME statistics
      input 0 bytes, 5 second rate 0 bytes/sec, 0.00 KB/sec
        clear 0 bytes, encrypt 0 bytes, decrypt 0
        compress 0 bytes, decompress 0 bytes
      output 0 bytes, 5 second rate 0 bytes/sec, 0.00 KB/sec
        clear 0 bytes, encrypt 0 bytes, decrypt 0
        compress 0 bytes, decompress 0 bytes
          compression ratio 0:0
      flows 0 encrypt, 0 clear
      clear luns 0, encrypted luns 0
      errors
         0 CTH, 0 authentication
```

```
        0 key generation, 0 incorrect read
        0 incompressible, 0 bad target responses
```

Related Commands

Command	Description
interface sme	Configures Cisco SME interface on the switch.

show interface transceiver

To display the SFP and X2 digital monitoring information for a transceiver, use the show interface transceiver details command.

show interface *fc-id* **transceiver details**

Syntax Description

fc-id	Specifies the Fiber Channel interface ID.
transceiver details	

Command Default

None.

Command Modes

Exec mode

Command History

Release	Modification
3.0	This command was introduced.

Usage Guidelines

Note The output for the **show interface transceiver** command will vary based on the transceiver type, name, part number, revision, and link length of the device.

When the small form-factor pluggable (SFP) port is shut down and the laser is turned off, the value of the *Current* field in the output will be close to zero and the *Tx power* value will be at a minimum (close to -40 dBm).

When the SFP port is shutdown and the laser is not turned off, the *Current* and *Tx power* values in the output will stay at operational levels. The *Rx power* value will depend on the behavior of the remote side of the link and the interface status—the value can be at an operational level, at a minimum (close to -40 dBm), or N/A.

This command displays the attributes of a transceiver such as, the vendor, the kind of laser it emits and receives, compatible fiber-optic cable, distances supported, vendor's firmware revision, faults the unit experienced since the last insertion or since the last linecard boot (whichever is the latest) and the diagnostics information (if supported by the unit).

Examples

The following example displays the SFP digital monitoring information for a transceiver (DOM unsupported SFP):

```
switch#show interface fc4/1 transceiver details
fc4/1 sfp is present
    name is CISCO-FINISAR
    part number is FTRJ8519P1BNL-C1
    revision is A
    serial number is FNS0838B0CX
    fc-transmitter type is short wave laser w/o OFC (SN)
    fc-transmitter supports intermediate distance link length
```

```
    media type is multi-mode, 62.5m (M6)
    Supported speed is 200 MBytes/sec
    Nominal bit rate is 2100 MBits/sec
    Link length supported for 50/125mm fiber is 500 m(s)
    Link length supported for 62.5/125mm fiber is 300 m(s)
    cisco extended id is unknown (0x0)
    no tx fault, rx loss, no sync exists, Diag mon type 136
    Digital diagnostics feature not supported in SFP
```

The following example displays the X2 digital monitoring information for a transceiver:

```
switch# show interface fc1/1 transceiver details
fc1/1 sfp is present
    name is CISCO
    part number is FTLX8541E2-C1
    revision is C
    serial number is FNS11151B0V
    FC Transceiver Type is X2 Medium
    FC Connector Type is SC
    Bit Encoding is NRZ
    Protocol Type is 10GbE
    Standards Compliance Codes :
    10GbE Code Byte 0 : 10GBASE-SR
    Fiber type Byte 0 : MM-Generic
    Fiber type Byte 1 : Unspecified
    Transmission Range is 30 (in 10m increments)
    cisco extended id is Unknown (0x0)
    no tx fault, rx loss, no sync exists, Diag mon type 193
    SFP Detail Diagnostics Information
  ------------------------------------------------------------------------------
                                  Alarms                  Warnings
                               High        Low         High          Low
  ------------------------------------------------------------------------------
  Temperature  41.35 C         74.00 C     -4.00 C     70.00 C        0.00 C
  Voltage       0.00 V          0.00 V      0.00 V      0.00 V        0.00 V
  Current       8.10 mA        12.00 mA     4.00 mA    11.00 mA       5.00 mA
  Tx Power     -2.58 dBm        3.00 dBm  -11.30 dBm   -1.00 dBm     -7.30 dBm
  Rx Power    -28.54 dBm --     3.00 dBm  -13.90 dBm   -1.00 dBm     -9.90 dBm
  Transmit Fault Count = 7
  ------------------------------------------------------------------------------
  Note: ++  high-alarm; +  high-warning; --  low-alarm; -  low-warning
```

Related Commands

Command	Description
show interface	Displays the status of an interface.

show inventory

To display the system hardware inventory, use the **show inventory** command.

show inventory

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

This command displays information about the field replaceable units (FRUs) in the switch, including product IDs, serial numbers, and version IDs.

Examples

The following example displays the system inventory information:

```
switch# show inventory
NAME: "Chassis",  DESCR: "MDS 9506 chassis"
PID: DS-C9506            ,  VID: 0.1,  SN: FOX0712S007
NAME: "Slot 1",  DESCR: "2x1GE IPS, 14x1/2Gbps FC Module"
PID: DS-X9302-14K9       ,  VID: 0.301,  SN: JAB083100JY
NAME: "Slot 5",  DESCR: "Supervisor/Fabric-1"
PID: DS-X9530-SF1-K9     ,  VID: 0.0,  SN: JAB0747080H
NAME: "Slot 6",  DESCR: "Supervisor/Fabric-1"
PID: DS-X9530-SF1-K9     ,  VID: 4.0,  SN: JAB074004VE
NAME: "Slot 17",  DESCR: "MDS 9506 Power Supply"
PID: DS-CAC-1900W        ,  VID: 1.0,  SN: DCA0702601V
NAME: "Slot 18",  DESCR: "MDS 9506 Power Supply"
PID: DS-CAC-1900W        ,  VID: 1.0,  SN: DCA0702601U
NAME: "Slot 19",  DESCR: "MDS 9506 Fan Module"
PID: DS-6SLOT-FAN        ,  VID: 0.1,  SN: FOX0638S150
```

show ioa cluster

To display detailed information of all the IOA clusters, use the show ioa cluster command.

show ioa cluster cluster name

Syntax Description

cluster name	Specifies IOA cluster name. The maximum size is 31 characters.

Command Default

None.

Command Modes

Cluster Configuration submode.

Command History

Release	Modification
6.2(5)	Added the show ioa cluster tape_vault flows command output. (with and without delice alias).
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

```
The following example shows how to display detailed information of all IOA clusters:
switch# show ioa cluster
IOA Cluster is tape_vault
Cluster ID is 0x213a000dec3ee782
Cluster status is online
Is between sites SJC and RTP
Total Nodes are 2
Cluster Infra Status : Operational
Cluster is Administratively Up
Cluster Config Version : 26
SSL for ICN : Not Configured
switch#
The following example shows how to display the interfaces in an IOA cluster:
switch# show ioa cluster tape_vault interface
Interface ioa2/1 belongs to 172.23.144.97(L)(M)
  Status is up
Interface ioa2/2 belongs to 172.23.144.97(L)(M)
  Status is up
Interface ioa2/1 belongs to 172.23.144.98
  Status is up
Interface ioa2/2 belongs to 172.23.144.98
  Status is up
switch#
The following example shows how to display the summary of interfaces in a IOA cluster:
switch# show ioa cluster tape_vault interface summary
--------------------------------------------------------------------------------
Switch             Interface         Status       Flows
--------------------------------------------------------------------------------
172.23.144.97(L)   ioa2/1            up           --
172.23.144.97(L)   ioa2/2            up           --
172.23.144.98      ioa2/1            up           --
```

```
172.23.144.98      ioa2/2            up           --
switch#
The following example shows how to display the N ports configuration:
switch# show ioa cluster tape_vault nports
--------------------------------------------------------------------------------
P-WWN Site Vsan
--------------------------------------------------------------------------------
10:00:00:00:00:00:00:01 SJC 100
11:00:00:00:00:00:00:01 RTP 100
10:00:00:00:00:00:00:02 SJC 100
10:00:00:00:00:00:00:02 RTP 100
The following example shows how to display an IOA cluster node:
sjc-sw1# show ioa cluster tape_vault node
Node 172.23.144.95 is local switch
  Node ID is 1
  Status is online
  Belongs to Site sjc
  Node is the master switch
Node 172.23.144.96 is remote switch
  Node ID is 2
  Status is offline
  Belongs to Site new_jersey
  Node is not master switch
switch#
The following example shows how to display an IOA cluster node summary:
switch# show ioa cluster tape_vault node summary
--------------------------------------------------------------------------------
Switch Site Status Master
--------------------------------------------------------------------------------
172.23.144.97(L) SJC online yes
172.23.144.98 RTP online no
The following example shows how to display the configured flow information without device
alias:
switch# show ioa cluster tape_vault flows
--------------------------------------------------------------------------------
Host WWN,                VSAN     WA  TA  Comp  Status    Switch,Interface
Target WWN                                              Pair
--------------------------------------------------------------------------------
10:00:00:00:00:00:00:01, 100      Y    Y    N   online    172.23.144.97, ioa2/1
11:00:00:00:00:00:00:01, 100                              172.23.144.98, ioa2/1
10:00:00:00:00:00:00:02, 100      Y    Y    Y   online    172.23.144.97, ioa2/2
11:00:00:00:00:00:00:02, 100                              172.23.144.98, ioa2/2
switch#
The following example shows how to display the configured flow information with device
alias:
sjc-sw2# show ioa cluster tape_vault flows
--------------------------------------------------------------------------------
Host WWN,                VSAN     WA  TA  Comp  Status    Switch,Interface
Target WWN                                              Pair
--------------------------------------------------------------------------------
host-1                  , 100      Y    Y    N   online     172.23.144.97, ioa2/1
target-1                , 100                               172.23.144.98, ioa2/1
host-2                  , 100      Y    Y    Y   online     172.23.144.97, ioa2/2
target-2                , 100                               172.23.144.98, ioa2/2
The following example shows how to display the detailed information of the flows that are
accelerated in the cluster:
switch# show ioa cluster tape_vault flows detail
Host 10:00:00:00:00:00:00:01, Target 11:00:00:00:00:00:00:01, VSAN 100
  Is online
  Belongs to flowgroup fg1
  Is enabled for WA, TA,
  Is assigned to
    Switch 172.23.144.97    Interface ioa2/1 (Host Site)
    Switch 172.23.144.98    Interface ioa2/1 (Target Site)
```

```
Host 10:00:00:00:00:00:00:02, Target 11:00:00:00:00:00:00:02, VSAN 100
  Is online
  Belongs to flowgroup fg1
  Is enabled for WA, TA, Compressi
  Is assigned to
    Switch 172.23.144.97    Interface ioa2/2 (Host Site)
    Switch 172.23.144.98    Interface ioa2/2 (Target Site)
```

Related Commands

Command	Description
interface ioa	Configures the IOA interface.

show ioa cluster summary

To display a summary of all the IOA clusters, use the show ioa cluster summary command.

show ioa cluster summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display IOA cluster summary information:

```
switch# show ioa cluster summary
--------------------------------------------------------------------------------
Cluster          Sites              Status    Master Switch
--------------------------------------------------------------------------------
tape_vault       SJC,               online    172.23.144.97
                 RTP
tape_vault_site2 SAC,               online    172.23.144.97
                 SJC
switch#
```

Related Commands

Command	Description
interface ioa	Configures the IOA interface.

show ioa internal interface ioa

To display summary of all the IOA clusters, use the show ioa internal interface ioa command.

show ioa internal interface ioa slot number {**els-table**|**errors**|**init-pwwn pwwn targ-pwwn pwwn vsan vsan-id counters brief**|**plogi-info**|**stats**|**summary**|**trace log**|**vit-table**}

Syntax Description

slot number	Specifies the IOA slot or port number. The range is from 1 to 16 for the slot and for the port the range is from 1 to 4.
els-table	Specifies the IOA ELS table.
errors	Specifies IOA errors.
init-pwwn pwwn	Specifies the initiator PWWN.
targ-pwwn pwwn	Specifies the target PWWN.
vsan vsan-id	Specifies the VSAN ID. The range is from 1 to 4093.
counters	Specifies interface counters.
brief	Specifies brief information about the interface.
plogi-info	Specifies PLOGI counters for IOA interface.
stats	Specifies the IOA statistics.
summary	Specifies the IOA host map table.
trace log	Specifies the IOA stats
vit-table	Specifies the IOA vit table.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display an IOA host map table:

```
switch# show ioa int int ioa 2/1 summary
---- ---------------------- ---- ------------- ---- ---
FLOW HOST VSAN STATUS COMP ACC
TARGET
```

```
---- ---------------------- ---- ------------- ---- ---
1 10:00:00:00:00:00:03:00 200 ACTIVE YES WA
11:00:00:00:00:00:03:00
2 10:00:00:00:00:00:02:00 200 ACTIVE NO WA
11:00:00:00:00:00:02:00
3 10:00:00:00:00:00:01:00 100 ACTIVE YES TA
11:00:00:00:00:00:01:00
4 10:00:00:00:00:00:00:00 100 ACTIVE NO TA
11:00:00:00:00:00:00:00
```

The following example shows how to display IOA statistics:

```
switch# show ioa int int ioa 2/1 stats
Adapter Layer Stats
4457312829 device packets in, 376008035 device packets out
8954596919462 device bytes in, 24064514554 device bytes out
526927441 peer packets in, 2473105321 peer packets out
45230025550 peer bytes in, 4701244024682 peer bytes out
8 i-t create request, 4 i-t create destroy
8 i-t activate request, 0 i-t deactivate request
0 i-t create error, 0 i-t destroy error
0 i-t activate error, 0 i-t deactivate error
48 i-t-n not found, 0 i-t-n stale logo timer expiry
4 logo sent, 8 logo timer started
4 logo timer fired, 4 logo timer cancelled
4 plogi 4 plogi-acc 4 logo-acc 4 prli 4 prli-acc 0 els-q-err
to-device 214279940 orig pkts 12743547488 orig bytes
to-peer 8748538 orig pkts 682386268 orig bytes
0 queued 0 flushed 0 discarded
LRTP Stats
0 retransmitted pkts, 0 flow control
2464072014 app sent 2464072014 frags sent 0 tx wait
0 rexmt bulk attempts 0 rexmt bulk pkts 2 delayed acks
376008013 in-order 0 reass-order 0 reass-wait 0 dup-drop
376008013 app deliver 376008013 frags rcvd
150919428 pure acks rx 376008013 data pkts rx 0 old data pkts
0 remove reass node, 0 cleanup reass table
Tape Accelerator statistics
2 Host Tape Sessions
0 Target Tape Sessions
Host End statistics
Received 26275926 writes, 26275920 good status, 2 bad status
Sent 26275914 proxy status, 10 not proxied
Estimated Write buffer 4 writes 524288 bytes
Received 0 reads, 0 status
Sent 0 cached reads
Read buffer 0 reads, 0 bytes
Host End error recovery statistics
Sent REC 0, received 0 ACCs, 0 Rejects
Sent ABTS 0, received 0 ACCs
Received 0 RECs, sent 0 ACCs, 0 Rejects
Received 0 SRRs, sent 0 ACCs, 0 Rejects
Received 0 TMF commands
Target End statistics
Received 0 writes, 0 good status, 0 bad status
Write Buffer 0 writes, 0 bytes
Received 0 reads, 0 good status, 0 bad status
Sent 0 reads, received 0 good status, 0 bad status
Sent 0 rewinds, received 0 good status, 0 bad status
Estimated Read buffer 0 reads, 0 bytes
Target End error recovery statistics
Sent REC 0, received 0 ACCs, 0 Rejects
Sent SRR 0, received 0 ACCs
Sent ABTS 0, received 0 ACCs
```

```
Write Accelerator statistics
Received 726357548 frames, Sent 529605035 frames
0 frames dropped, 0 CRC errors
0 rejected due to table full, 0 scsi busy
0 ABTS sent, 0 ABTS received
0 tunnel synchronization errors
Host End statistics
Received 188004026 writes, 188004000 XFER_RDY
Sent 188004026 proxy XFER_RDY, 0 not proxied
Estimated Write buffer 1146880 bytes
Timed out 0 exchanges, 0 writes
Target End statistics
Received 0 writes, 0 XFER_RDY
Write buffer 0 bytes
TCP flow control 0 times, 0 bytes current
Timed out 0 exchanges, 0 writes
Compression Statistics
Pre Comp Batch size 131072
Post Comp Batch size 2048
4375494911078 input bytes, 50140348947 output compressed bytes
0 non-compressed bytes, 0 incompressible bytes
0 compression errors
0 Compression Ratio
De-Compression Statistics
0 input bytes, 0 output decompressed bytes
11883488326 non-compressed bytes
0 de-compression errors
```

The following example shows how to display the initiator PWWN:

```
switch# show ioa int int ioa 2/1 init-pwwn 10:00:00:00:00:00:03:00 targ-pwwn
11:00:00:00:00:00:03:00 vsan 200 counters
Adapter Layer Stats
1366529601 device packets in, 160768174 device packets out
2699458644986 device bytes in, 10289163140 device bytes out
160844041 peer packets in, 165188790 peer packets out
18652597246 peer bytes in, 47736122724 peer bytes out
0 i-t create request, 0 i-t create destroy
0 i-t activate request, 0 i-t deactivate request
0 i-t create error, 0 i-t destroy error
0 i-t activate error, 0 i-t deactivate error
0 i-t-n not found, 0 i-t-n stale logo timer expiry
1 logo sent, 2 logo timer started
1 logo timer fired, 1 logo timer cancelled
1 plogi 1 plogi-acc 1 logo-acc 1 prli 1 prli-acc 0 els-q-err
to-device 80384094 orig pkts 4662277452 orig bytes
to-peer 0 orig pkts 0 orig bytes
0 queued 0 flushed 0 discarded
LRTP Stats
0 retransmitted pkts, 0 flow control
160768190 app sent 160768190 frags sent 0 tx wait
0 rexmt bulk attempts 0 rexmt bulk pkts 1 delayed acks
160768162 in-order 0 reass-order 0 reass-wait 0 dup-drop
160768162 app deliver 160768162 frags rcvd
75879 pure acks rx 160768162 data pkts rx 0 old data pkts
0 remove reass node, 0 cleanup reass table
Write Accelerator statistics
Received 1607681842 frames, Sent 1527297774 frames
0 frames dropped, 0 CRC errors
0 rejected due to table full, 0 scsi busy
0 ABTS sent, 0 ABTS received
0 tunnel synchronization errors
Host End statistics
Received 80384094 writes, 80384082 XFER_RDY
```

```
Sent 80384094 proxy XFER_RDY, 0 not proxied
Estimated Write buffer 524288 bytes
Timed out 0 exchanges, 0 writes
Target End statistics
Received 0 writes, 0 XFER_RDY
Write buffer 0 bytes
TCP flow control 0 times, 0 bytes current
Timed out 0 exchanges, 0 writes
```

The following example shows how to display the initiator PWWN:

```
switch# show ioa int int ioa 2/1 init-pwwn 10:00:00:00:00:00:03:00 targ-pwwn
11:00:00:00:00:00:03:00 vsan 200 counters brief
------------------------------------------------------------------------------
Interface Input (rate is 5 min avg) Output (rate is 5 min avg)
---------------------------- ----------------------------
Rate Total Rate Total
MB/s Frames MB/s Frames
------------------------------------------------------------------------------
ioa1/1
Device 60 9573683 0 1126308
Peer 0 1126833 1 1157161
switch#
```

show ip access-list

To display the IP access control lists (IP-ACLs) currently active, use the **show ip access-list** command.

show ip access-list [{*list-number*|**usage**}]

Syntax Description

list-number	(Optional) Specifies the IP-ACL. The range is 1 to 256.
usage	(Optional) Specifies the interface type.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays configured IP-ACLs:

```
switch# show ip access-list usage
Access List Name/Number          Filters IF   Status    Creation Time
-------------------------------- ------- ---- --------- -------------
abc                              3       7    active    Tue Jun 24 17:51:40 2003
x1                               3       1    active    Tue Jun 24 18:32:25 2003
x3         0   1   not-ready Tue Jun 24 18:32:28 2003
```

The following example displays a summary of the specified IP-ACL:

```
switch# show ip access-list abc
ip access-list abc permit tcp any any (0 matches)
ip access-list abc permit udp any any (0 matches)
ip access-list abc permit icmp any any (0 matches)
ip access-list abc permit ip 10.1.1.0 0.0.0.255 (2 matches)
ip access-list abc permit ip 10.3.70.0 0.0.0.255 (7 matches)
```

show ip arp

To display IP neighbors for the system, use the **show ip arp** command.

show ips arp interface gigabitethernet *slot / port*

Syntax Description

interface	(Optional) Displays the IP neighbors for a specified interface.
cpp *module-number*	(Optional) Specifies the virtualization IP over Fibre Channel (IPFC) interface by control plane processor (CPP) module number. The range is 1 to 6.
gigabitethernet *slot/port*	(Optional) Specifies the Gigabit Ethernet interface by slot and port number. The range is 1 to 6.
mgmt	(Optional) Specifies the management interface.
vsan *vsan-id*	(Optional) Specifies the IPFC VSAN interface by VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays IP neighbor information:

```
switch# show ip arp
IP Address       Age(min)   Link-layer Addr         Type  Interface
209.165.200.226 0          0006.d623.4008          ARPA  GigabitEthernet1/1
209.165.200.227 5          0002.b3d9.ba6f          ARPA  GigabitEthernet1/1
209.165.200.228 11         0004.23bd.677b          ARPA  GigabitEthernet1/1
209.165.200.229 67         0000.0c07.ac01          ARPA  mgmt0
209.165.200.230 0          000e.d68f.c3fc          ARPA  mgmt0
209.165.200.231 0          000e.d68f.43fc          ARPA  mgmt0
209.165.200.232 1067       00e0.8152.7f8d          ARPA  mgmt0
```

Related Commands

Command	Description
show ip interface	Displays IP interface status and configuration information.
show ip traffic	Displays IP protocol statistics for the system.

show ip interface

To display IP interface status and configuration information, use the **show ip interface** command.

show ip interface [{**cpp** *module-number*|**gigabitethernet** *slot/port*|**mgmt**|**port-channel** *number*|**vsan** *vsan-id*}]

Syntax Description

cpp *module-number*	(Optional) Specifies the virtualization IP over Fibre Channel (IPFC) interface by CPP module number. The range is 1 to 6.
gigabitethernet *slot/port*	(Optional) Specifies the Gigabit Ethernet interface by slot and port number. The range is 1 to 6.
mgmt	(Optional) Specifies the management interface.
port-channel *number*	(Optional) Specifies the PortChannel interface. The range is 1 to 256.
vsan *vsan-id*	(Optional) Specifies the IPFC VSAN interface by VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays IP interface status and configuration information:

```
switch# show ip interface
GigabitEthernet1/1 is up
  Internet address is 10.10.10.1/24
  Broadcast address is 255.255.255.255
GigabitEthernet1/2 is up
  Internet address is 10.10.60.1/24
  Broadcast address is 255.255.255.255
GigabitEthernet2/2 is up
  Internet address is 10.10.20.1/24
  Broadcast address is 255.255.255.255
mgmt0 is up
  Internet address is 172.22.31.110/24
  Broadcast address is 255.255.255.255
```

Related Commands

Command	Description
show ip arp	Displays IP neighbors for the system.

Command	Description
show ip traffic	Displays IP protocol statistics for the system.

show ip route

To display the currently active IP routes currently active, use the **show ip route** command.

show ip route [configured]

Syntax Description

configured	(Optional) Displays configured IP routes.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays active IP routes:

```
switch# show ip route
Codes: C - connected, S - static
Default gateway is 172.22.95.1
C 10.0.0.0/24 is directly connected, vsan1
C 172.22.95.0/24 is directly connected, mgmt0
```

The following example displays configured IP routes.

```
switch# show ip route configured
         default      172.22.31.1          0.0.0.0      0            mgmt0
      10.10.11.0       10.10.11.1    255.255.255.0      0 GigabitEthernet1/1
      10.10.50.0       10.10.50.1    255.255.255.0      0 GigabitEthernet1/2.1
      10.10.51.0       10.10.51.1    255.255.255.0      0 GigabitEthernet1/2.2
      10.10.60.0       10.10.60.1    255.255.255.0      0 GigabitEthernet1/2
     172.22.31.0    172.22.31.110    255.255.255.0      0            mgmt0
```

show ip routing

To display the IP routing state, use the **show ip routing** command.

show ip routing

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows the IP routing state:

```
switch# show ip routing
ip routing is disabled
```

show ip traffic

To display IP protocol statistics for the system, use the **show ip traffic** command.

show ip traffic [**interface gigabitethernet** *slot/port*]

Syntax Description

interface	(Optional) Displays the IP neighbors for a specified interface.
gigabitethernet *slot/port*	(Optional) Specifies the Gigabit Ethernet interface by slot and port number. The range is 1 to 6.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays IP protocol statistics for the Gigabit Ethernet interface:

```
switch# show ip traffic interface gigabitethernet 2/2
IP Statistics for GigabitEthernet2/2
  Rcvd:  0 total, 0 local destination
         0 errors, 0 unknown protocol, 0 dropped
  Sent:  30 total, 0 forwarded 0 dropped
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 fragments created, 0 couldn't fragment
ICMP Statistics:
  Rcvd:  0 total, 0 errors, 0 unreachables, 0 time exceeded
         0 echo, 0 echo reply, 0 mask requests, 0 mask replies
         0 redirects, 0 timestamp requests, 0 timestamp replies
  Sent:  0 total, 0 errors, 0 unreachables, 0 time exceeded
         0 echo, 0 echo reply, 0 mask requests, 0 mask replies
         0 redirects, 0 timestamp requests, 0 timestamp replies
```

Related Commands

Command	Description
show ip arp	Displays IP neighbors for the system.
show ip interface	Displays IP interface status and configuration information.

show ips arp

To display the IP storage ARP cache information, use the show ips arp command.

show ips arp interface gigabitethernet *slot / port*

Syntax Description

interface gigabitethernet *slot*/*port*	Specifies a Gigabit Ethernet interface by the slot and port.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Use the **show ips arp interface gigabitethernet** command to display the ARP cache on the Gigabit Ethernet interfaces. This command takes the main Ethernet interface and as a parameter and returns the ARP cache for that interface.

Examples

The following example displays ARP caches in the specified interface:

```
switch# show ips arp interface gigabitethernet 4/1
Protocol         Address   Age (min)   Hardware Addr  Type   Interface
Protocol         Address   Age (min)   Hardware Addr  Type   Interface
Internet     172.22.91.1    2    -  00:00:0c:07:ac:01  ARPA  GigabitEthernet4/4
Internet     172.22.91.2    0    -  00:02:7e:6b:a8:08  ARPA  GigabitEthernet4/4
Internet    172.22.91.17    0    -  00:e0:81:20:45:f5  ARPA  GigabitEthernet4/4
Internet    172.22.91.18    0    -  00:e0:81:05:f7:64  ARPA  GigabitEthernet4/4
Internet    172.22.91.30    0    -  00:e0:18:2e:9d:19  ARPA  GigabitEthernet4/4
...
```

show ips ip route

To show the IP storage route table information, use the show ips ip route command.

show ips ip route interface gigabitethernet *slot / port*

Syntax Description

interface gigabitethernet *slot*/*port*	Specifies a Gigabit Ethernet interface by the slot and port.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the IP route table information for a Gigabit Ethernet interface:

```
switch# show ips ip route interface gigabitethernet 8/1
Codes: C - connected, S - static
No default gateway
C 10.1.3.0/24 is directly connected, GigabitEthernet8/1
```

show ips ipv6

To display an IPv6 storage routing table, use the **show ips ipv6** command.

show ips ipv6 {**neighbors interface gigabitethernet** *slot/port*|**prefix-list interface gigabitethernet** *slot/port*|**route interface gigabitethernet** *slot/port*|**routers interface gigabitethernet** *slot/port*|**traffic interface gigabitethernet** *slot/port*}

Syntax Description

neighbors	Displays the IPv6 neighbors table.
interface	Displays the interface status and configuration.
gigabitethernet	Displays a Gigabit Ethernet interface.
slot/port	Specifies the slot and port number.
prefix-list	Displays the IPv6 prefix-list table.
route	Displays the IPv6 route table.
routers	Displays the IPv6 routers table.
traffic	Displays the IPv6 traffic table.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

You can use the **show ips ipv6 command to display information about IPv6 routing.**

Examples

The following example displays IPv6 neighbors information:

```
switch# show ips ipv6 neighbours interface gigabitethernet 1/1
IPv6 Address                              Age (min)  Link-layer Addr  State  Inter
face
fe80::206:d6ff:fe23:4008                  0          0006.d623.4008      S   GigabitEthernet1/1
```

The following example displays the IPv6 prefix-list information:

```
switch# show ips ipv6 prefix-list interface gigabitethernet 1/1
Prefix                                  Prefix-len   Addr
     Valid   Preferred
2000::                                    64         2000::205:30ff:fe01:a6be
       1000     1000
```

The following example displays the IPv6 routing table:

```
switch# show ips ipv6 route interface gigabitethernet 4/2
IPv6 Routing Table - 4 entries
Codes: C - Connected, L - Local, S - Static, G - Gateway, M - Multicast
C 3000:8::/64 is directly connected, GigabitEthernet4/2.250
C 3000:7::/64 is directly connected, GigabitEthernet4/2
C fe80::/64 is directly connected, GigabitEthernet4/2
C fe80::/64 is directly connected, GigabitEthernet4/2.250
M ff02::/32 is multicast, GigabitEthernet4/2
M ff02::/32 is multicast, GigabitEthernet4/2.250
```

The following example displays IPv6 routers information:

```
switch# show ips ipv6 routers interface gigabitethernet 1/1
Addr                              Lifetime   Expire
fe80::206:d6ff:fe23:4008          3600      3600
```

The following example displays IPv6 traffic statistics:

```
switch#  show ips ipv6 traffic interface gigabitethernet 4/2
IPv6 statistics:
  Rcvd:  0 total
         0 bad header, 0 unknown option, 0 unknown protocol
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  20 generated
         0 fragmented into 0 fragments, 0 failed
         2 no route
ICMP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 too short
         0 unknown info type, 0 unknown error type
         unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
         parameter: 0 error, 0 header, 0 option
         0 hopcount expired, 0 reassembly timeout,0 too big
         0 echo request, 0 echo reply
         0 group query, 0 group report, 0 group reduce
         0 router solicit, 0 router advert, 0 redirects
         0 neighbor solicit, 0 neighbor advert
  Sent: 20 output, 0 rate-limited
         unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
         parameter: 0 error, 0 header, 0 option
         0 hopcount expired, 0 reassembly timeout,0 too big
         0 echo request, 0 echo reply
         0 group query, 6 group report, 0 group reduce
         2 router solicit, 0 router advert, 0 redirects
         0 neighbor solicit, 12 neighbor advert
```

Related Commands

Command	Description
ipv6 enable	Enables IPv6 processing.
show ipv6 route	Displays IPv6 routes configured on the system.

show ips netsim

To display a summary of the IP Network Simulator interface status currently operating, use the **show ips netsim** command.

show ips netsim

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

None**.**

Examples

The following example shows the IP Network Simulator interfaces operating in network simulation mode:

```
switch# show ips netsim
Following ports operate in network simulator mode
GigabitEthernet2/3 and GigabitEthernet2/4
```

Related Commands

Command	Description
ips netsim enable	Enables two Gigabit Ethernet interfaces to operate in network simulation mode.

show ips stats

To display IP storage statistics, use the show ips stats command.

show ips stats {**buffer**|**dma-bridge**|**icmp**|**ip**|**mac**} **interface gigabitethernet** *slot* / *port*
show ips stats {**hw-comp**|**tcp**} {**all**|**interface gigabitethernet** *slot* / *port*}

Syntax Description

buffer	Displays IP storage buffer information.
dma-bridge	Displays the direct memory access (DMA) statistics.
icmp	Displays ICMP statistics.
ip	Displays IP statistics.
mac	Displays MAC statistics.
hw-comp	Displays hardware compression statistics.
tcp	Displays TCP statistics
all	Displays statistical information for all interfaces.
interface gigabitethernet *slot*/*port*	Specifies a Gigabit Ethernet interface by the slot and port.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Use the **show ips stats icmp interface gigabitethernet** command to obtain ICMP statistics for the selected interface.

Use the **show ips stats ip interface gigabitethernet 2/1** command to obtain IP statistics for the selected interface.

Use the **show ips stats mac interface gigabitethernet** command to obtain Ethernet statistics for the selected interface.

Use the **show ips stats tcp interface gigabitethernet** command to obtain TCP statistics along with the connection list and TCP state or the selected interface.

Examples

The following example displays iSCSI buffer statistics:

```
switch# show ips stats buffer interface gigabitethernet 1/2
Buffer Statistics for port GigabitEthernet1/2
    Mbuf stats
```

```
      164248 total mbufs, 82119 free mbufs, 0 mbuf alloc failures
      123186 mbuf high watermark, 20531 mbuf low watermark
      0 free shared mbufs, 0 shared mbuf alloc failures
      82124 total clusters, 77005 free clusters, 0 cluster alloc failures
      86230 mbuf high watermark, 78017 mbuf low watermark
      0 free shared clusters, 0 shared cluster alloc failures
    Ether channel stats
      0 tcp segments sent, 0 tcp segments received
      0 xmit packets sent, 0 xmit packets received
      0 config packets sent, 0 config packets received
      0 MPQ packet send errors
```

The following example displays ICMP statistics:

```
switch# show ips stats icmp interface gigabitethernet 8/1
ICMP Statistics for port GigabitEthernet8/1
    2 ICMP messages received
    0 ICMP messages dropped due to errors
    ICMP input histogram
      2 echo request
    ICMP output histogram
      2 echo reply
```

The following example displays IP statistics:

```
switch# show ips stats ip interface gigabitethernet 8/1
Internet Protocol Statistics for port GigabitEthernet8/1
    22511807 total received, 22509468 good, 2459 error
    0 reassembly required, 0 reassembled ok, 0 dropped after timeout
    27935633 packets sent, 0 outgoing dropped, 0 dropped no route
    0 fragments created, 0 cannot fragment
```

The following example displays MAC statistics:

```
switch# show ips stats mac interface gigabitethernet 8/1
DPP HW GigabitEthernet8/1 statistics

  dropped         : 0          octs,   0          pkts
  oversize        : 0          pkts,   0          crcpkts
  runt            : 0          pkts,   0          crcpkts
  inband          : 88542331034 octs,   1193721449 pkts,      0      err
  pci raw         : 0          pkts
  fcs_align_err   : 0          pkts

  total           : 2642985114 octs,   1193721449 pkts

  length of [pkts]:-
   [64B]          : 226          [65B-127B]       : 1138408009
   [128B-255B]    : 55292581     [256B-511B]      : 20497
   [512B-1023B]   : 90           [1024B-1518B]    : 0
   [1519B-MAX]    : 46
```

The following example displays TCP statistics:

```
switch# show ips stats tcp interface gigabitethernet 8/1
TCP Statistics for port GigabitEthernet8/1
    Connection Stats
      0 active openings, 0 accepts
      0 failed attempts, 0 reset received, 0 established
    Segment stats
      23657893 received, 29361174 sent, 0 retransmitted
      0 bad segments received, 0 reset sent
```

```
TCP Active Connections
  Local  Address        Remote Address        State      Send-Q   Recv-Q
  10.1.3.3:3260         10.1.3.106:51935      ESTABLISH  0        0
  10.1.3.3:3260         10.1.3.106:51936      ESTABLISH  0        0
  10.1.3.3:3260         10.1.3.106:51937      ESTABLISH  0        0
  10.1.3.3:3260         10.1.3.106:51938      ESTABLISH  0        0
  10.1.3.3:3260         10.1.3.106:51939      ESTABLISH  0        0
  10.1.3.3:3260         10.1.3.106:51940      ESTABLISH  0        0
  10.1.3.3:3260         10.1.3.106:51941      ESTABLISH  0        0
  10.1.3.3:3260         10.1.3.106:51942      ESTABLISH  0        0
  10.1.3.3:3260         10.1.3.106:51943      ESTABLISH  0        0
  10.1.3.3:3260         10.1.3.106:51944      ESTABLISH  0        0
  10.1.3.3:3260         10.1.3.115:1026       ESTABLISH  0        0
  10.1.3.3:3260         10.1.3.115:1027       ESTABLISH  0        0
  10.1.3.3:3260         10.1.3.115:1028       ESTABLISH  0        0
  10.1.3.3:3260         10.1.3.115:1029       ESTABLISH  0        0
  10.1.3.3:3260         10.1.3.115:1030       ESTABLISH  48       0
  10.1.3.3:3260         10.1.3.115:1031       ESTABLISH  48       0
  10.1.3.3:3260         10.1.3.115:1032       ESTABLISH  0        0
  10.1.3.3:3260         10.1.3.115:1033       ESTABLISH  0        0
  10.1.3.3:3260         10.1.3.115:1034       ESTABLISH  0        0
  0.0.0.0:3260          0.0.0.0:0             LISTEN     0        0
```

show ips stats fabric interface

To display the fabric-related statistics for the given iSCSI or FCIP interface on a Cisco MDS 9000 18/4-Port Multi Service Module IPS linecared, use the show ips stats fabric interface command.

show ips stats fabric interface [{**iscsi** *slot/port*|**fcip** **N**}]

Syntax Description

iscsi *slot/port*	(Optional) Displays Data Path Processor (DPP) fabric statistics for the iSCSI interface.
fcip *N*	(Optional) Displays DPP fabric statistics for the fcip interface.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

This command also displays information on flow control specific to DPP.

Examples

The following example shows the statistics for iSCSI on the specified interface:

```
switch# show ips stats fabric interface interface iscsi 1/1
DPP Fabric statistics for iscsi 1/1
    Software Egress Counters
      14049 good frames, 0 bad header cksum, 0 bad FIFO SOP
      0 parity error, 0 FC CRC error, 0 timestamp expired error
      0 unregistered port index, 0 unknown internal type
      0 RDL ok, 0 RDL drop (too big), 0 RDL ttl_1
      0 idle poll count, 0 loopback
      0 FCC PQ, 0 FCC EQ, 0 FCC generated
      Flow Control: 0 [0], 0 [1], 0 [2], 0 [3]
    Software Ingress Counters
      0 good frames, 0 header cksum error, 0 FC CRC error
      0 iSCSI CRC error, 0 descriptor SOP error, 0 parity error
      0 frames soft queued, 0 current Q, 0 max Q, 0 low memory
      0 out of memory drop, 0 queue full drop
      0 RDL ok, 0 RDL drop (too big)
      Flow Control: 0 [0], 0 [1], 0 [2], 0 [3]
```

The following example shows the statistics for FCIP on the specified interface:

```
switch# show ips stats fabric interface fcip 1
DPP Fabric statistics for fcip1
    Software Egress Counters
      14049 good frames, 0 bad header cksum, 0 bad FIFO SOP
      0 parity error, 0 FC CRC error, 0 timestamp expired error
      0 unregistered port index, 0 unknown internal type
      0 RDL ok, 0 RDL drop (too big), 0 RDL ttl_1
```

```
    0 idle poll count, 0 loopback
    0 FCC PQ, 0 FCC EQ, 0 FCC generated
    Flow Control: 0 [0], 0 [1], 0 [2], 0 [3]
  Software Ingress Counters
    0 good frames, 0 header cksum error, 0 FC CRC error
    0 iSCSI CRC error, 0 descriptor SOP error, 0 parity error
    0 frames soft queued, 0 current Q, 0 max Q, 0 low memory
    0 out of memory drop, 0 queue full drop
    0 RDL ok, 0 RDL drop (too big)
    Flow Control: 0 [0], 0 [1], 0 [2], 0 [3]
```

Related Commands

Command	Description
clear ips stats fabric interface	Clears the statistics for the given iSCSI or FCIP interface on a Cisco MDS 9000 18/4-Port Multi Service Module IPS linecard.

show ips stats netsim

To display IP Network Simulator interface statistics, use the **show ips stats netsim** command.

show ips stats netsim ingress gigabitethernet *slot/port*

Syntax Description

ingress	Specifies the ingress direction.
gigabitethernet *slot/port*	Specifies the the slot and port number of the Gigabit Ethernet interface.

Command Default

None.

Command Modes

EXEC.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The parameters displayed by default are delay, bandwidth, queue size, and queue delay. The network statistics displayed are number of packets dropped, queue size, number of packets reordered, and average speed.

Examples

The following example shows the IP Network Simulator statistics for interface 2/3:

```
switch# show ips stats netsim ingress gigabitethernet 2/3
Network Simulator Configuration for Ingress on GigabitEthernet2/3
Delay : 50000 microseconds
Rate : 1000000 kbps
Max_q : 100000 bytes
Max_qdelay : 600000 clocks
Random Drop % : 1.00%
Network Simulator Statistics for Ingress on GigabitEthernet2/3
Dropped (tot) = 28
Dropped (netsim) = 14
Reordered (netsim) = 0
Max Qlen(pkt) = 7
Qlen (pkt) = 0
Max Qlen (byte) = 326
Qlen (byte) = 0
Mintxdel(poll) = 852
Mintxdel(ethtx) = 360
empty = 757
txdel = 8
late = 617
Average speed = 0 Kbps
```

Related Commands

Command	Description
ips netsim enable	Enables two Gigabit Ethernet interfaces to operate in the network simulation mode.

show ips status

To display the IP storage status, use the show ips status command.

show ips status [**module** *slot*]

Syntax Description

module *slot*	(Optional) Identifies the module in the specified slot.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the IP storage status for all modules on the switch:

```
switch# show ips status
        Port 8/1 READY
        Port 8/2 READY
        Port 8/3 READY
        Port 8/4 READY
        Port 8/5 READY
        Port 8/6 READY
        Port 8/7 READY
        Port 8/8 READY
```

The following example displays the IP storage status for the module in slot 9:

```
switch# show ips status module 9
        Port 9/1 READY
        Port 9/2 READY
        Port 9/3 READY
        Port 9/4 READY
        Port 9/5 READY
        Port 9/6 READY
        Port 9/7 READY
        Port 9/8 READY
```

show ipv6 access-list

To display a summary of IPv6 access control lists (ACLs), use the **show ipv6 access-list** command.

show ipv6 access-list [list-name]

Syntax Description

list-name	(Optional) Specifies the name of the ACL. The maximum size is 64.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays an IPv6 access control list:

```
switch# show ipv6 access-list
Access List Name/Number          Filters IF   Status    Creation Time
-------------------------------- ------- ---- --------- -------------
abc                              3       7    active    Tue Jun 24 17:51:40 2003
x1                               3       1    active    Tue Jun 24 18:32:25 2003
x3                               0       1    not-ready Tue Jun 24 18:32:28 2003
```

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6-ACL.

show ipv6 interface

To display IPv6 interface status and configuration information, use the **show ipv6 interface** command.

show ipv6 interface [{**gigabitethernet** *slot/port*|**mgmt 0**|**port-channel** *port-channel-number*|**vsan** *vsan-id*}]

Syntax Description

gigabitethernet *slot/port*	(Optional) Displays a Gigabit Ethernet interface.
mgmt 0	(Optional) Displays the management interface.
port-channel	(Optional) Displays a PortChannel interface.
port-channel-*number*	(Optional) Specifies the PortChannel number. The range is 1 to 128.
vsan	(Optional) Displays an IPFC VSAN interface.
vsan-id	(Optional) Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays IPv6 interface information:

```
switch# show ipv6 interface
GigabitEthernet1/2 is up
  IPv6 is enabled
  Global address(es):
    5000::1/64
  Link-local address(es):
    fe80::205:30ff:fe01:a6bf
  ND DAD is disabled
  ND reachable time is 30000 milliseconds
  ND retransmission time is 1000 milliseconds
  Stateless autoconfig for addresses disabled
GigabitEthernet2/2 is up
  IPv6 is enabled
  Global address(es):
    6000::1/64
  Link-local address(es):
    fe80::205:30ff:fe00:a413
  ND DAD is disabled
  ND reachable time is 30000 milliseconds
  ND retransmission time is 1000 milliseconds
  Stateless autoconfig for addresses disabled
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address.
ipv6 nd	Configures IPv6 neighbor discovery commands.
ipv6 route	Configures an IPv6 static route.
show ipv6 neighbors	Displays information about IPv6 neighbors for the system.
show ipv6 route	Displays the IPv6 routes configured on the system.

show ipv6 neighbours

To display IPv6 neighbors configuration information, use the **show ipv6** neighbours command.

show ipv6 neighbours [**interface** {**gigabitethernet** *slot/port*|**mgmt 0**|**vsan** *vsan-id*}]

Syntax Description

interface	(Optional) Displays the IP interface status and configuration.
gigabitethernet *slot/port*	(Optional) Displays a Gigabit Ethernet interface slot and port number.
mgmt 0	(Optional) Displays the management interface.
vsan *vsan-id*	(Optional) Displays an IPFC VSAN interface and specifies the VSAN ID. The range is 1 to 4093

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays information about IPv6 neighbor discovery:

```
switch# show ipv6 neighbours gigabitethernet 2/1
IPv6 Address                                Age Link-layer Addr State Interface
2001:0DB8:0:4::2                              0 0003.a0d6.141e  REACH Ethernet2
FE80::XXXX:A0FF:FED6:141E                     0 0003.a0d6.141e  REACH Ethernet2
2001:0DB8:1::45a                              - 0002.7d1a.9472  REACH Ethernet2
```

Related Commands

Command	Description
ipv6 nd	Configures IPv6 neighbor discovery commands.

show ipv6 route

To display the IPv6 routes configured on the system, use the **show ipv6 route** command.

show ipv6 route

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays information about an IPv6 route:

```
switch# show ipv6 route
IPv6 Routing Table
Codes: C - Connected, L - Local, S - Static G - Gateway
C    5000::/64
     via fe80::205:30ff:fe01:a6bf, GigabitEthernet1/2
C    6000::/64
     via fe80::205:30ff:fe00:a413, GigabitEthernet2/2
L    fe80::/10
     via ::
L    ff00::/8
     via ::
```

Related Commands

Command	Description
ipv6 route	Configures an IPv6 route.

show ipv6 routing

To display IPv6 unicast routing information, use the **show ipv6 routing** command.

show ipv6 routing

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the ipv6 routing information:

```
switch# show ipv6 routing
ipv6 routing is enabled
```

Related Commands

Command	Description
ipv6 routing	Enables IPv6 unicast routing.

show ipv6 traffic

To display IPv6 protocol statistics for the system, use the **show ipv6 traffic** command.

show ipv6 traffic [**interface** {**gigabitethernet** *slot*/*port*|**mgmt 0**|**port-channel** *number*|**vsan** *vsan-id*}]

Syntax Description

interface	(Optional) Displays the IP interface status and configuration.
gigabitethernet *slot/port*	(Optional) Displays a Gigabit Ethernet interface slot and port number.
mgmt 0	(Optional) Displays the management interface.
port-channel *number*	(Optional) Dispalys the PortChannel interface. The range is 1 to 256.
vsan *vsan-id*	(Optional) Displays a IPFC VSAN interface and specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(0)	This command was introduced.

Usage Guidelines

None**.**

Examples

The following example displays IPv6 protocol statistics on the system:

```
switch# show ipv6 traffic
IPv6 Statistics:
  Rcvd:  1 total, 0 local destination
         0 errors, 0 truncated, 0 too big
         0 unknown protocol, 0 dropped
         0 fragments, 0 reassembled
         0 couldn't reassemble, 0 reassembly timeouts
  Sent:  0 generated, 0 forwarded 0 dropped
         0 fragmented, 0 fragments created, 0 couldn't fragment
ICMPv6 Statistics:
  Rcvd:  0 total, 0 errors, 0 unreachables, 0 time exceeded
         0 too big, 0 param probs, 0 admin prohibs
         0 echos, 0 echo reply, 0 redirects
         0 group query, 0 group report, 0 group reduce
         0 router solicit, 0 router advert
         0 neighbor solicit, 0 neighbor advert
  Sent:  74 total, 0 errors, 0 unreachables, 0 time exceeded
         0 too big, 0 param probs, 0 admin prohibs
         0 echos, 0 echo reply, 0 redirects
         0 group query, 53 group report, 0 group reduce
         0 router solicit, 0 router advert
         0 neighbor solicit, 21 neighbor advert
```

The following example displays IPv6 traffic on Gigabit Ethernet interface 2/2:

```
switch# show ipv6 traffic interface gigabitethernet 2/2
IPv6 Statistics for GigabitEthernet2/2
  Rcvd:  10 total, 0 local destination
         0 errors, 0 truncated, 0 too big
         0 unknown protocol, 0 dropped
         0 fragments, 0 reassembled
         0 couldn't reassemble, 0 reassembly timeouts
  Sent:  54 generated, 0 forwarded 0 dropped
         0 fragmented, 0 fragments created, 0 couldn't fragment
ICMPv6 Statistics for GigabitEthernet2/2
  Rcvd:  4 total, 0 errors, 0 unreachables, 0 time exceeded
         0 too big, 0 param probs, 0 admin prohibs
         0 echos, 0 echo reply, 0 redirects
         0 group query, 2 group report, 0 group reduce
         0 router solicit, 0 router advert
         0 neighbor solicit, 2 neighbor advert
  Sent:  21 total, 0 errors, 0 unreachables, 0 time exceeded
         0 too big, 0 param probs, 0 admin prohibs
         0 echos, 0 echo reply, 0 redirects
         0 group query, 6 group report, 3 group reduce
         2 router solicit, 0 router advert
         2 neighbor solicit, 8 neighbor advert
```

show isapi dpp

To obtain a list of ITLs for a specific Data Path Processor (DPP), use the show isapi dpp command.

show isapi dpp dpp-number

Syntax Description

dpp-number	Specifies the slot along with the DPP number.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the ISAPI infomation for DPP number 7:

```
module-3# show isapi dpp 7 queue
I_T 0x837c9140 [vsan 42 host 0x8d0005 vt 8d0014/92:81:00:00:08:50:ca:d4]: 0 tasks, mtu 2048,
 seqid 99, abts 0 BSY

Q 837cc380: LUN 3, status 0x22, R/W access 0x0/0x0, 0 tasks, 0 busy/TSF, 0 ho
  Tasks:

Q 837cbd80: LUN 2, status 0x22, R/W access 0x0/0x0, 0 tasks, 0 busy/TSF, 0 ho
  Tasks:

Q 837cb100: LUN 1, status 0x22, R/W access 0x0/0x0, 0 tasks, 0 busy/TSF, 0 ho
  Tasks:

Q 837cb080: LUN 0, status 0x22, R/W access 0x0/0x0, 0 tasks, 0 busy/TSF, 0 ho
  Tasks:
```

Related Commands

Command	Description
show isapi dpp all queue	Displays ITLs for all DPPs on the SSM.

show isapi tech-support santap file

To display ISAPI information for troubleshooting, use the show isapi tech-support santap file command.

show isapi tech-support santap file [name]

Syntax Description

name	(Optional) Specifies the name of the file. The file is stored on modflash.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 4.1(1b)	Added Usage Guidelines.

Usage Guidelines

SANTap tech support, collected through the above CLI, is stored in the line card modflash. It includes ISAPI tech support and the outputs of the show debug santap event-history and show santap tech-support command. These two outputs are not present in ISAPI tech support, and are not collected after a DPP crash.

The size of the modflash is limited, close to 60 MB in 4.1(1). If less space remains on modflash than the size of the output file, an unusable truncated file may get created. To ensure that the SANTap tech support file gets created in the modflash properly, enough space (at least 20 MB) should be made available before entering the command. Copy a tech support file after collecting the tech support, and delete it from the modflash.

ISAPI tech support collected through the show isapi tech-support file <filename> is stored in the line card log directory.

The size of the log directory also is limited to 180 MB. This is shared for some other purposes as well. Again, at least 20 MB should be made available in the log directory before collecting ISAPI tech support, and the file should be copied out and deleted from the log directory once done.

The following commands may be used for copying and deleting files from the modflash and log directories on the line card:

copy log:// module / file name target fs (entered on the supervisor module) will copies the isapi tech support file from /var/log/external.

copy modflash:// module -1/ file name target fs (entered on the supervisor module) copies the santap-isapi tech support file from the line card modflash.

clear debug-logfile filename (entered on the line card module) deletes logfiles in the line card log directory.

delete modflash://module-1/ filename (entered on the supervisor module) deletes logfiles in the line card modflash.

Examples

The following example shows how to display the ISAPI infomation for troubleshooting:

```
switch# attach module 13
Attaching to module 13 ...
To exit type 'exit', to abort type '$.'
```

```
Bad terminal type: "ansi". Will assume vt100.
switch# show isapi tech-support santap file cisco
Re-directing tech support information to file: cisco
switch#
```

Related Commands

Command	Description
show isapi dpp all queue	Displays ITLs for all DPPs on the SSM.

show iscsi global

To display global iSCSI configured information, use the **show iscsi global** command.

show iscsi global

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays all configured iSCSI initiators:

```
switch# show iscsi global
iSCSI Global informationAuthentication: CHAP, NONEImport FC Target: EnabledInitiator idle
timeout: 300 secondsDynamic Initiator: iSLBNumber of target node: 1Number of portals: 2Number
 of session: 0Failed session: 0, Last failed initiator name:
```

show iscsi initiator

To display information about all the iSCSI nodes that are remote to the switch, use the **show iscsi initiator** command.

show iscsi initiator [{**configured** [*initiator-name*]|**detail**|**fcp-session [detail]**|**iscsi-session [detail]**|**summary [name]**}]

Syntax Description

configured	(Optional) Displays the configured information for the iSCSI initiator.
initiator-name	(Optional) Specifies the name of an initiator.
detail	(Optional) Displays detailed iSCSI initiator information.
fcp-session	(Optional) Displays the Fibre Channel session details.
iscsi-session	(Optional) Displays iSCSI session details.
summary	(Optional) Displays summary information.
name	(Optional) Displays initiator name information.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

If no parameter is provided the command lists all the active iSCSI initiators. If the iSCSI node name is provided then the command lists the details of that iSCSI initiator.

Examples

The following example displays all iSCSI initiators:

```
switch# show iscsi initiator

iSCSI Node name is iqn.1987-05.com.cisco.01.15cee6e7925087abc82ed96377653c8
    iSCSI alias name: iscsi7-lnx
    Node WWN is 23:10:00:05:30:00:7e:a0 (dynamic)
    Member of vsans: 1
    Number of Virtual n_ports: 1
    Virtual Port WWN is 23:12:00:05:30:00:7e:a0 (dynamic)
      Interface iSCSI 8/3, Portal group tag: 0x382
        VSAN ID 1, FCID 0xdc0100
iSCSI Node name is iqn.1987-05.com.cisco:02.91b0ee2e8aa1.iscsi16-w2k
    iSCSI alias name: ISCSI16-W2K
    Node WWN is 23:1f:00:05:30:00:7e:a0 (dynamic)
    Member of vsans: 1
    Number of Virtual n_ports: 1
    Virtual Port WWN is 23:28:00:05:30:00:7e:a0 (dynamic)
```

```
      Interface iSCSI 8/3, Portal group tag: 0x382
        VSAN ID 1, FCID 0xdc0101
iSCSI Node name is iqn.1987-05.com.cisco.01.b6ca466f8b4d8e848ab17e92f24bf9cc
    iSCSI alias name: iscsi6-lnx
    Node WWN is 23:29:00:05:30:00:7e:a0 (dynamic)
    Member of vsans: 1, 2, 3, 4
    Number of Virtual n_ports: 1
    Virtual Port WWN is 23:2a:00:05:30:00:7e:a0 (dynamic)
      Interface iSCSI 8/3, Portal group tag: 0x382
        VSAN ID 4, FCID 0xee0000
        VSAN ID 3, FCID 0xee0100
        VSAN ID 2, FCID 0xee0000
        VSAN ID 1, FCID 0xdc0102
...
```

The following example displays detailed Information for all iSCSI initiators:

```
switch# show iscsi initiator
 detail
iSCSI Node name is iqn.1987-05.com.cisco.01.15cee6e7925087abc82ed96377653c8
    iSCSI alias name: iscsi7-lnx
    Node WWN is 23:10:00:05:30:00:7e:a0 (dynamic)
    Member of vsans: 1
    Number of Virtual n_ports: 1
    Virtual Port WWN is 23:10:00:05:30:00:7e:a0 (dynamic)
      Interface iSCSI 8/3, Portal group tag is 0x382
        VSAN ID 1, FCID 0xdc0100
        No. of FC sessions: 3
        No. of iSCSI sessions: 2
        iSCSI session details
          Target node: iqn.com.domainname.172.22.93.143.08-03.gw.22000020374b5247
          Statistics:
            PDU: Command: 0, Response: 0
            Bytes: TX: 0, RX: 0
            Number of connection: 1
          TCP parameters
            Connection Local 10.1.3.3:3260, Remote 10.1.3.107:34112
            Path MTU 1500 bytes
            Current retransmission timeout is 300 ms
            Round trip time: Smoothed 2 ms, Variance: 1
            Advertised window: Current: 6 KB, Maximum: 6 KB, Scale: 3
            Peer receive window: Current: 250 KB, Maximum: 250 KB, Scale: 2
            Congestion window: Current: 8 KB
          Target node: iqn.com.domainname.172.22.93.143.08-03.gw.22000020374b5247
          Statistics:
            PDU: Command: 0, Response: 0
            Bytes: TX: 0, RX: 0
            Number of connection: 1
          TCP parameters
            Connection Local 10.1.3.3:3260, Remote 10.1.3.107:34112
            Path MTU 1500 bytes
            Current retransmission timeout is 300 ms
            Round trip time: Smoothed 2 ms, Variance: 1
            Advertised window: Current: 6 KB, Maximum: 6 KB, Scale: 3
            Peer receive window: Current: 250 KB, Maximum: 250 KB, Scale: 2
            Congestion window: Current: 8 KB
...
```

show iscsi session

To display iSCSI session information, use the show iscsi session command.

show iscsi session [incoming] [**initiator** *name*] **[outgoing]** [**target** *name*] **[detail]**

Syntax Description

incoming	(Optional) Displays incoming iSCSI sessions.
initiator *name*	(Optional) Displays specific iSCSI initiator session information. Maximum length is 80 characters.
outgoing	(Optional) Displays outgoing iSCSI sessions
target *name*	(Optional) Displays specific iSCSI target session information. Maximum length is 80 characters.
detail	(Optional) Displays detailed iSCSI session information.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

All the parameters are optional in the **show iscsi session** commands. If no parameter is provided the command lists all the active iSCSI initiator or target sessions. If the IP address or iSCSI node name is provided, then the command lists details of all sessions from that initiator or to that target.

Examples

The following command displays the iSCSI session information:

```
switch# show iscsi session
Initiator iqn.1987-05.com.cisco.01.15cee6e7925087abc82ed96377653c8
  Session #1
    Target iqn.com.domainname.172.22.93.143.08-03.gw.22000020374b5247
    VSAN 1, ISID 000000000000, Status active, no reservation
  Session #2
    Target iqn.com.domainname.172.22.93.143.08-03.gw.220000203738e77d
    VSAN 1, ISID 000000000000, Status active, no reservation
Initiator iqn.1987-05.com.cisco:02.91b0ee2e8aa1.iscsi16-w2k
  Session #1
    Discovery session, ISID 00023d00022f, Status active
  Session #2
    Target iqn.com.domainname.172.22.93.143.08-03.gw.2200002037388bc2
    VSAN 1, ISID 00023d000230, Status active, no reservation
...
```

The following command displays the specified iSCSI target:

```
switch# show iscsi session target iqn.com.domainname.172.22.93.143.08-03.gw.220000203738e77d
```

```
Initiator iqn.1987-05.com.cisco.01.15cee6e7925087abc82ed96377653c8
  Session #1
    Target iqn.com.domainname.172.22.93.143.08-03.gw.220000203738e77d
    VSAN 1, ISID 000000000000, Status active, no reservation
```

Note On the IPS module, you can verify what iSCSI initiator IQN has been assigned which pWWN when it logs in by using the **show zone active vsan** *vsan-id* command. switch# **zone name iscsi_16_A vsan 16*** fcid 0x7700d4 [pwwn 21:00:00:20:37:c5:2d:6d]* fcid 0x7700d5 [pwwn 21:00:00:20:37:c5:2e:2e]* fcid 0x770100 [symbolic-nodename iqn.1987-05.com.cisco.02.BC3FEEFC431B199F81F33E97E2809C14.NUYEAR]

The following command displays the specified iSCSI initiator:

```
switch# show iscsi session initiator iqn.1987-05.com.cisco:02.91b0ee2e8aa1.iscsi16-w2k
Initiator iqn.1987-05.com.cisco:02.91b0ee2e8aa1.iscsi16-w2k
  Session #1
    Discovery session, ISID 00023d00022f, Status active
  Session #2
    Target iqn.com.domainname.172.22.93.143.08-03.gw.2200002037388bc2
    VSAN 1, ISID 00023d000230, Status active, no reservation
  Session #3
    Target iqn.com.domainname.172.22.93.143.08-03.gw.210000203739ad7f
    VSAN 1, ISID 00023d000235, Status active, no reservation
  Session #4
    Target iqn.com.domainname.172.22.93.143.08-03.gw.210000203739aa3a
    VSAN 1, ISID 00023d000236, Status active, no reservation
  Session #5
    Target iqn.com.domainname.172.22.93.143.08-03.gw.210000203739ada7
    VSAN 1, ISID 00023d000237, Status active, no reservation
  Session #6
    Target iqn.com.domainname.172.22.93.143.08-03.gw.2200002037381ccb
    VSAN 1, ISID 00023d000370, Status active, no reservation
  Session #7
    Target iqn.com.domainname.172.22.93.143.08-03.gw.2200002037388b54
    VSAN 1, ISID 00023d000371, Status active, no reservation
  Session #8
    Target iqn.com.domainname.172.22.93.143.08-03.gw.220000203738a194
    VSAN 1, ISID 00023d000372, Status active, no reservation
  Session #9
    Target iqn.com.domainname.172.22.93.143.08-03.gw.2200002037360053
    VSAN 1, ISID 00023d000373, Status active, no reservation
```

show iscsi stats

To display the iSCSI statistics information, use the show iscsi stats command.

show iscsi stats [**iscsi** *slot / port*] [{**clear**|**detail**}]

Syntax Description

iscsi *slot/port*	(Optional) Displays statistics for the specified iSCSI interface.
clear	(Optional) Clears iSCSI statistics for the session or interface.
detail	(Optional) Displays detailed iSCSI statistics for the session or interface.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following command displays brief iSCSI statistics:

```
switch# show iscsi stats
iscsi8/1
    5 minutes input rate 23334800 bits/sec, 2916850 bytes/sec, 2841 frames/sec
    5 minutes output rate 45318424 bits/sec, 5664803 bytes/sec, 4170 frames/sec
    iSCSI statistics
      86382665 packets input, 2689441036 bytes
        3916933 Command pdus, 82463404 Data-out pdus, 2837976576 Data-out bytes,
 0 fragments
      131109319 packets output, 2091677936 bytes
        3916876 Response pdus (with sense 0), 1289224 R2T pdus
        125900891 Data-in pdus, 93381152 Data-in bytes
iscsi8/2
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes
iscsi8/3
    5 minutes input rate 272 bits/sec, 34 bytes/sec, 0 frames/sec
    5 minutes output rate 40 bits/sec, 5 bytes/sec, 0 frames/sec
    iSCSI statistics
      30 packets input, 10228 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      30 packets output, 1744 bytes
```

```
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes
iscsi8/4
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes
iscsi8/5
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes
iscsi8/6
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes
iscsi8/7
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes
iscsi8/8
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes
```

The following command displays detailed iSCSI statistics:

```
switch# show iscsi stats detail
iscsi8/1
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes
  iSCSI Forward:
    Command: 0 PDUs (Received: 0)
    Data-Out (Write): 0 PDUs (Received 0), 0 fragments, 0 bytes
  FCP Forward:
```

```
    Xfer_rdy: 0 (Received: 0)
    Data-In: 0 (Received: 0), 0 bytes
    Response: 0 (Received: 0), with sense 0
    TMF Resp: 0
  iSCSI Stats:
    Login: attempt: 0, succeed: 0, fail: 0, authen fail: 0
    Rcvd: NOP-Out: 0, Sent: NOP-In: 0
          NOP-In: 0, Sent: NOP-Out: 0
          TMF-REQ: 0, Sent: TMF-RESP: 0
          Text-REQ: 0, Sent: Text-RESP: 0
          SNACK: 0
          Unrecognized Opcode: 0, Bad header digest: 0
          Command in window but not next: 0, exceed wait queue limit: 0
          Received PDU in wrong phase: 0
  FCP Stats:
    Total: Sent: 0
           Received: 0 (Error: 0, Unknown: 0)
    Sent: PLOGI: 0, Rcvd: PLOGI_ACC: 0, PLOGI_RJT: 0
          PRLI: 0, Rcvd: PRLI_ACC: 0, PRLI_RJT: 0, Error resp: 0
          LOGO: 0, Rcvd: LOGO_ACC: 0, LOGO_RJT: 0
          ABTS: 0, Rcvd: ABTS_ACC: 0
          TMF REQ: 0
          Self orig command: 0, Rcvd: data: 0, resp: 0
    Rcvd: PLOGI: 0, Sent: PLOGI_ACC: 0
          LOGO: 0, Sent: LOGO_ACC: 0
          PRLI: 0, Sent: PRLI_ACC: 0
          ABTS: 0
  iSCSI Drop:
    Command: Target down 0, Task in progress 0, LUN map fail 0
             CmdSeqNo not in window 0, No Exchange ID 0, Reject 0
             Persistent Resv 0    Data-Out: 0, TMF-Req: 0
  FCP Drop:
    Xfer_rdy: 0, Data-In: 0, Response: 0
  Buffer Stats:
    Buffer less than header size: 0, Partial: 0, Split: 0
    Pullup give new buf: 0, Out of contiguous buf: 0, Unaligned m_data: 0
iscsi8/2
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
        0 Response pdus (with sense 0), 0 R2T pdus
        0 Data-in pdus, 0 Data-in bytes
  iSCSI Forward:
    Command: 0 PDUs (Received: 0)
    Data-Out (Write): 0 PDUs (Received 0), 0 fragments, 0 bytes
  FCP Forward:
    Xfer_rdy: 0 (Received: 0)
    Data-In: 0 (Received: 0), 0 bytes
    Response: 0 (Received: 0), with sense 0
...
```

The following command displays detailed statistics for the specified iSCSI interface:

```
switch# show iscsi stats iscsi 8/1
iscsi8/1
    5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    iSCSI statistics
      0 packets input, 0 bytes
        0 Command pdus, 0 Data-out pdus, 0 Data-out bytes, 0 fragments
      0 packets output, 0 bytes
```

```
0 Response pdus (with sense 0), 0 R2T pdus
0 Data-in pdus, 0 Data-in bytes
```

show iscsi virtual-target

To display all the iSCSI nodes that are local to the switch, use the **show iscsi virtual-target** command.

show iscsi virtual-target [configured] [*name*]

Syntax Description

configured	(optional) Displays the information for all iSCSI ports.
name	(Optional) Displays iSCSI information for the specified virtual-target.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

If no parameter is provided the command lists all the active iSCSI virtual targets. If the iSCSI node name is provided then the command lists the details of that iSCSI virtual target.

Examples

The following example displays information on all the iSCSI virtual targets:

```
switch# show iscsi virtual-target
target: abc1
    Port WWN 21:00:00:20:37:a6:b0:bf
    Configured node
target: iqn.com.domainname.172.22.93.143.08-03.gw.22000020374b5247
    Port WWN 22:00:00:20:37:4b:52:47 , VSAN 1
    Auto-created node
...
target: iqn.com.domainname.172.22.93.143.08-03.gw.210000203739aa39
    Port WWN 21:00:00:20:37:39:aa:39 , VSAN 1
    Auto-created node
```

The following example displays a specified iSCSI virtual target:

```
switch# show iscsi virtual-target iqn.com.domainname.172.22.93.143.08-03.gw.210000203739a95b
target: iqn.com.domainname.172.22.93.143.08-03.gw.210000203739a95b
    Port WWN 21:00:00:20:37:39:a9:5b , VSAN 1
    Auto-created node
```

The following example displays the trespass status for a virtual target:

```
switch# show iscsi virtual-target iqn.abc
target: abc
    Port WWN 00:00:00:00:00:00:00:00
    Configured node
    all initiator permit is disabled
    trespass support is  enabled S
```

show islb cfs-session status

To display iSCSI server load balancing (iSLB) Cisco Fabric Services information, use the **show islb cfs-session status** command.

show islb cfs-session status

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays iSLB session informations.

```
ips-hac2# show islb cfs-session status
last action               : fabric distribute disable
last action result        : success
last action failure cause : success
```

Related Commands

Command	Description
show islb initiator	Displays iSLB initiator information.
show islb merge status	Displays iSLB merge status information.
show islb pending	Displays iSLB pending configurations.
show islb pending-diff	Displays iSLB pending configuration differences.
show islb session	Displays iSLB session information.
show islb status	Displays iSLB CFS status information.
show islb virtual-target	Displays iSLB virtual target information.
show islb vrrp	Displays iSLB VRRP load balancing information.

show islb initiator

To display iSCSI server load balancing (iSLB) Cisco Fabric Services information, use the **show islb initiator** command.

show islb initiator [{**name node-name** [{**detail**|**fcp-session [detail]**|**iscsi-session [detail]**}]|**configured** [**name initiator-name**]|**detail**|**fcp-session [detail]**|**iscsi-session [detail]**|**summary [name]**}]

Syntax Description

name *node-name*	Displays the initiator node name. The maximum size is 80.
detail	Displays more detailed information.
fcp-session	Displays Fibre Channel session details.
iscsi-session	Displays iSLB session details.
configured	Displays iSLB initiator configured information.
name *initiator-name*	Displays the configured initiator name. The maximum size is 223.
summary	Displays iSLB initiator summary information.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows iSLB initiator configuration information:

```
switch# show islb initiator configured
iSCSI Node name is 1.1.1.1
    No. of PWWN: 2
      Port WWN is 23:01:00:0c:85:90:3e:82
      Port WWN is 23:02:00:0c:85:90:3e:82
    Load Balance Metric: 1000
    Number of Initiator Targets: 0
iSCSI Node name is 2.2.2.2
    Load Balance Metric: 1000
    Number of Initiator Targets: 0
```

Related Commands

Command	Description
show islb cfs-session status	Displays iSLB session status and status information.

Command	Description
show islb merge status	Displays iSLB merge status information.
show islb pending	Displays iSLB pending configurations.
show islb pending-diff	Displays iSLB pending configuration differences.
show islb session	Displays iSLB session information.
show islb status	Displays iSLB CFS status information.
show islb virtual-target	Displays iSLB virtual target information.
show islb vrrp	Displays iSLB VRRP load balancing information.

show islb merge status

To display iSCSI server load balancing (iSLB) merge status information, use the **show islb merge status** command.

show islb merge status

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows iSLB merge status information:

```
switch# show islb merge status
Merge Status: SUCCESS
```

Related Commands

Command	Description
show islb cfs-session status	Displays iSLB session information.
show islb initiator	Displays iSLB initiator information.
show islb pending	Displays iSLB pending configurations.
show islb pending-diff	Displays iSLB pending configuration differences.
show islb session	Displays iSLB session information.
show islb status	Displays iSLB CFS status information.
show islb virtual-target	Displays iSLB virtual target information.
show islb vrrp	Displays iSLB VRRP load balancing information.

show islb pending

To display iSCSI server load balancing (iSLB) pending configurations, use the **show islb pending** command.

show islb pending

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows iSLB pending configuration information:

```
switch# show islb pending
iscsi initiator idle-timeout 10
```

islb initiator ip-address 10.1.1.1static pWWN 23:01:00:0c:85:90:3e:82static pWWN 23:06:00:0c:85:90:3e:82username test1

```
islb initiator ip-address 10.1.1.2static nWWN 23:02:00:0c:85:90:3e:82
```

Related Commands

Command	Description
show islb initiator	Displays iSLB initiator information.
show islb cfs-session status	Displays iSLB session information.
show islb merge status	Displays iSLB merge status information.
show islb pending-diff	Displays iSLB pending configuration differences.
show islb session	Displays iSLB session information.
show islb status	Displays iSLB CFS status information.
show islb virtual-target	Displays iSLB virtual target information.
show islb vrrp	Displays iSLB VRRP load balancing information.

show islb pending-diff

To display iSCSI server load balancing (iSLB) pending configuration differences, use the **show islb pending-diff** command.

show islb pending-diff

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows iSLB pending configuration differences:

```
switch# show islb pending-diff
+iscsi initiator idle-timeout 10islb initiator ip-address 10.1.1.1+ static pWWN
23:06:00:0c:85:90:3e:82+islb initiator ip-address 10.1.1.2+ static nWWN
23:02:00:0c:85:90:3e:82
```

Related Commands

Command	Description
show islb cfs-session status	Displays iSLB session information.
show islb initiator	Displays iSLB initiator information.
show islb merge status	Displays iSLB merge status information.
show islb pending	Displays iSLB pending configurations.
show islb session	Displays iSLB session information.
show islb status	Displays iSLB CFS status information.
show islb virtual-target	Displays iSLB virtual target information.
show islb vrrp	Displays iSLB VRRP load balancing information.

show islb session

To display iSLB session information, use the **show islb session** command.

show islb session [{**detail**|**incoming**|**initiator initiator-node-name**|**iscsi slot-number**|**outgoing**|**target target-node-name**}]

Syntax Description

detail	(Optional) Displays detailed iSLB session information.
incoming	(Optional) Displays incoming iSLB sessions.
initiator *initiator-node-name*	(Optional) Displays session information for a specific iSLB initiator. The maximum size for the initiator node name is 80.
iscsi *slot-port*	(Optional) Specifies the iSCSI interface.
outgoing	(Optional) Displays outgoing iSLB sessions.
target	(Optional) Displays session information for a specific iSLB target. The maximum size for the target node name is 80.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows iSLB session information:

```
switch# show islb session
Initiator iqn.1987-05.com.cisco.01.15cee6e7925087abc82ed96377653c8
  Session #1
      Target iqn.com.domainname.172.22.93.143.08-03.gw.22000020374b5247
      VSAN 1, ISID 000000000000, Status active, no reservation

  Session #2
      Target iqn.com.domainname.172.22.93.143.08-03.gw.220000203738e77d
      VSAN 1, ISID 000000000000, Status active, no reservation
Initiator iqn.1987-05.com.cisco:02.91b0ee2e8aa1.iscsi16-w2k
  Session #1
     Discovery session, ISID 00023d00022f, Status active

  Session #2
      Target iqn.com.domainname.172.22.93.143.08-03.gw.2200002037388bc2
     VSAN 1, ISID 00023d000230, Status active, no reservation
```

Related Commands

Command	Description
show islb cfs-session status	Displays iSLB session information.
show islb initiator	Displays iSLB initiator information.
show islb merge status	Displays iSLB merge status information.
show islb pending	Displays iSLB pending configurations.
show islb pending-diff	Displays iSLB CFS pending configuration differences.
show islb status	Displys iSLB CFS status information.
show islb virtual-target	Displays iSLB virtual target information.
show islb vrrp	Displays iSLB VRRP load-balancing information.

show islb status

To display iSCSI server load balancing (iSLB) Cisco Fabric Services status, use the **show islb status** command.

show islb status

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows iSLB CFS status:

```
switch# show islb status
iSLB Distribute is enabled
iSLB CFS Session does not exist
```

Related Commands

Command	Description
show islb cfs-session status	Displays iSLB session information.
show islb initiator	Displays iSLB initiator information.
show islb merge status	Displays iSLB merge status information.
show islb pending	Displays iSLB pending configurations.
show islb pending-diff	Displays iSLB CFS pending configuration differences.
show islb session	Displays iSLB session information.
show islb virtual-target	Displays iSLB virtual target information.
show islb vrrp	Displays iSLB VRRP load balancing information.

show islb virtual-target

To display information about iSLB virtual targets, use the **show islb virtual-target** command.

show islb virtual-target [{**name**|**configured name**}]

Syntax Description

name	(Optional) Specifies the iSLB virtual target name. The range is 16 bytes to 223 bytes.
configured	(Optional) Displays information about configured iSLB virtual targets.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows an iSLB target:

```
switch# show islb virtual-target newtarget0987654321
target: newtarget0987654321
    Configured node (iSLB)
    No. of initiators permitted: 1
      initiator fromtarget1234567890 is permitted
    All initiator permit is enabled
    Trespass support is  disabled
    Revert to primary support is  disabled
```

The following example shows all configured iSLB virtual targets:

```
switch# show islb virtual-target configured
target: testtarget1234567
    Configured node (iSLB)
    No. of initiators permitted: 1
      initiator trespass is permitted
    All initiator permit is disabled
    Trespass support is  disabled
    Revert to primary support is  disabled
target: testertarget987654321
    Port WWN 10:20:30:40:50:60:70:80
    Configured node (iSLB)
    No. of initiators permitted: 1
      initiator mytargetdevice is permitted
    All initiator permit is disabled
    Trespass support is  disabled
    Revert to primary support is  disabled
target: newtarget0987654321
    Configured node (iSLB)
    No. of initiators permitted: 1
```

```
      initiator fromtarget1234567890 is permitted
    All initiator permit is enabled
    Trespass support is  disabled
    Revert to primary support is  disabled
target: mytargetdevice123
    Configured node (iSLB)
    All initiator permit is disabled
    Trespass support is  enabled
    Revert to primary support is  disabled
```

Related Commands

Command	Description
show islb cfs-session status	Displays iSLB session information.
show islb initiator	Displays iSLB initiator information.
show islb merge status	Displays iSLB merge status information.
show islb pending	Displays iSLB pending configurations.
show islb pending-diff	Displays iSLB CFS pending configuration differences.
show islb session	Displays iSLB session information.
show islb status	Displays iSLB CFS status information.
show islb vrrp	Displays iSLB VRRP load-balancing information.

show islb vrrp

To display iSLB VRRP load balancing information, use the **show islb vrrp** command.

show islb vrrp [{**assignment** [{**initiator node-name** [**vr group-number**]|**vr group-number**}]|**interface** [{**switch WWN** [**vr group-number**]|**vr group-number**}]|**summary** [**vr group-number**]|**vr group-number**}]

Syntax Description

assignment	(Optional) Displays iSLB VRRP initiator to interface assignment.
initiator *node-name*	(Optional) Displays a specific iSLB initiator's interface assignment. The maximum is 80.
vr *group-number*	(Optional) Displays information for a specific VR group. The range is 1 to 255.
interface	(Optional) Displays iSLB VRRP interface information.
switch *WWN*	(Optional) Displays a interface information for a specific switch. The format of WWN is *hh:hh:hh:hh:hh:hh:hh:hh* .
summary	(Optional) Displays iSLB VRRP load-balancing summary information.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows iSLB VRRP interface information:

```
switch# show islb vrrp interface vr 41
-- Interfaces For Load Balance --
    Interface GigabitEthernet1/1.441
        Switch wwn: 20:00:00:0d:ec:02:cb:00
        VRRP group id: 41, VRRP IP address: 209.165.200.226
            Interface VRRP state: backup
            Interface load: 3000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 209.165.200.226
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None
    Interface GigabitEthernet1/2.441
        Switch wwn: 20:00:00:0d:ec:02:cb:00
```

```
        VRRP group id: 41, VRRP IP address: 209.165.200.226
            Interface VRRP state: backup
            Interface load: 2000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.122.114
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None
    Interface GigabitEthernet2/1.441
        Switch wwn: 20:00:00:0d:ec:0c:6b:c0
        VRRP group id: 41, VRRP IP address: 209.165.200.226
            Interface VRRP state: backup
            Interface load: 2000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.122.111
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None
    Interface GigabitEthernet2/2.441
        Switch wwn: 20:00:00:0d:ec:0c:6b:c0
        VRRP group id: 41, VRRP IP address: 209.165.200.226
            Interface VRRP state: master
            Interface load: 1000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.122.112
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None
    Interface GigabitEthernet2/3.441
        Switch wwn: 20:00:00:0d:ec:0c:6b:c0
        VRRP group id: 41, VRRP IP address: 209.165.200.226
            Interface VRRP state: backup
            Interface load: 2000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.122.113
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None
```

The following example shows iSLB VRRP summary information:

```
switch# show islb vrrp summary
                        -- Groups For Load Balance --
-------------------------------------------------------------------------------
              VR Id             VRRP Address Type             Configured Status
-------------------------------------------------------------------------------
                 41                           IPv4                       Enabled
                 42                           IPv4                       Enabled
                      -- Interfaces For Load Balance --
-------------------------------------------------------------------------------
 VR Id         VRRP IP              Switch WWN                  Ifindex      Load
-------------------------------------------------------------------------------
```

```
    41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/1.441      3000
    41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/2.441      2000
    41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/1.441      2000
M   41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/2.441      1000
    41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/3.441      2000
M   42   10.10.142.111 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/1.442      2000
    42   10.10.142.111 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/2.442      1000
    42   10.10.142.111 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/3.442      2000
                  -- Initiator To Interface Assignment --
--------------------------------------------------------------------------------
Initiator  VR Id         VRRP IP              Switch WWN                  Ifindex
--------------------------------------------------------------------------------
iqn.1987-05.com.cisco:01.09ea2e99c97
             41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/1.441
iqn.1987-05.com.cisco:01.5ef81885f8d
             41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/3.441
iqn.1987-05.com.cisco:01.8fbdb3fdf8
             41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/1.441
iqn.1987-05.com.cisco:01.99eddd9b134
             41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/1.441
iqn.1987-05.com.cisco:01.a1398a8c6bc6
             41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/3.441
iqn.1987-05.com.cisco:01.e15c63d09d18
             41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/2.441
iqn.1987-05.com.cisco:01.e9aab57a51e0
             41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/1.441
iqn.1987-05.com.cisco:01.ecc2b77b6086
             41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/2.441
iqn.1987-05.com.cisco:01.f047da798a44
             41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/2.441
iqn.1987-05.com.cisco:01.f686f5cd11f
             41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/1.441
```

The following example shows iSLB VRRP summary information for vr 41:

```
switch# show islb vrrp summary vr 41
                       -- Groups For Load Balance --
--------------------------------------------------------------------------------
               VR Id             VRRP Address Type             Configured Status
--------------------------------------------------------------------------------
                  41                          IPv4                        Enabled
                       -- Interfaces For Load Balance --
--------------------------------------------------------------------------------
 VR Id         VRRP IP              Switch WWN                  Ifindex      Load
--------------------------------------------------------------------------------
    41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/1.441      3000
    41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/2.441      2000
    41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/1.441      2000
M   41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/2.441      1000
    41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/3.441      2000
                  -- Initiator To Interface Assignment --
--------------------------------------------------------------------------------
Initiator  VR Id         VRRP IP              Switch WWN                  Ifindex
--------------------------------------------------------------------------------
iqn.1987-05.com.cisco:01.09ea2e99c97
             41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/1.441
iqn.1987-05.com.cisco:01.5ef81885f8d
             41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/3.441
iqn.1987-05.com.cisco:01.8fbdb3fdf8
             41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/1.441
iqn.1987-05.com.cisco:01.99eddd9b134
             41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/1.441
iqn.1987-05.com.cisco:01.a1398a8c6bc6
             41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/3.441
```

```
iqn.1987-05.com.cisco:01.e15c63d09d18
              41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/2.441
iqn.1987-05.com.cisco:01.e9aab57a51e0
              41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/1.441
iqn.1987-05.com.cisco:01.ecc2b77b6086
              41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/2.441
iqn.1987-05.com.cisco:01.f047da798a44
              41   10.10.122.112 20:00:00:0d:ec:02:cb:00  GigabitEthernet1/2.441
iqn.1987-05.com.cisco:01.f686f5cd11f
              41   10.10.122.112 20:00:00:0d:ec:0c:6b:c0  GigabitEthernet2/1.441
```

The following example shows complete iSLB VRRP load balancing information.

```
switch# show islb vrrp

-- Groups For Load Balance --
    VRRP group id 41
        Address type: IPv4
        Configured status: Enabled
    VRRP group id 42
        Address type: IPv4
        Configured status: Enabled
-- Interfaces For Load Balance --
    Interface GigabitEthernet1/1.441
        Switch wwn: 20:00:00:0d:ec:02:cb:00
        VRRP group id: 41, VRRP IP address: 209.165.200.226
            Interface VRRP state: backup
            Interface load: 3000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.122.115
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None
    Interface GigabitEthernet1/2.441
        Switch wwn: 20:00:00:0d:ec:02:cb:00
        VRRP group id: 41, VRRP IP address: 209.165.200.226
            Interface VRRP state: backup
            Interface load: 2000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.122.114
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None
    Interface GigabitEthernet2/1.441
        Switch wwn: 20:00:00:0d:ec:0c:6b:c0
        VRRP group id: 41, VRRP IP address: 209.165.200.226
            Interface VRRP state: backup
            Interface load: 2000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.122.111
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None
    Interface GigabitEthernet2/2.441
        Switch wwn: 20:00:00:0d:ec:0c:6b:c0
```

```
        VRRP group id: 41, VRRP IP address: 209.165.200.226
            Interface VRRP state: master
            Interface load: 1000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.122.112
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None
    Interface GigabitEthernet2/3.441
        Switch wwn: 20:00:00:0d:ec:0c:6b:c0
        VRRP group id: 41, VRRP IP address: 209.165.200.226
            Interface VRRP state: backup
            Interface load: 2000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.122.113
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None
    Interface GigabitEthernet2/1.442
        Switch wwn: 20:00:00:0d:ec:0c:6b:c0
        VRRP group id: 42, VRRP IP address: 209.165.200.226
            Interface VRRP state: master
            Interface load: 2000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.142.111
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None
    Interface GigabitEthernet2/2.442
        Switch wwn: 20:00:00:0d:ec:0c:6b:c0
        VRRP group id: 42, VRRP IP address: 209.165.200.226
            Interface VRRP state: backup
            Interface load: 1000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.142.112
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None
    Interface GigabitEthernet2/3.442
        Switch wwn: 20:00:00:0d:ec:0c:6b:c0
        VRRP group id: 42, VRRP IP address: 209.165.200.226
            Interface VRRP state: backup
            Interface load: 2000
            Interface redirection: enabled
            Group redirection: enabled
        Number of physical IP address: 1
            (1) 10.10.142.113
        Port vsan: 1
        Forwarding mode: store-and-forward
        Proxy initiator mode: disabled
        iSCSI authentication: CHAP or None
-- Initiator To Interface Assignment --
```

```
Initiator iqn.1987-05.com.cisco:01.09ea2e99c97
    VRRP group id: 41, VRRP IP address: 209.165.200.226
    Assigned to switch wwn: 20:00:00:0d:ec:0c:6b:c0
        ifindex: GigabitEthernet2/1.441
    Waiting for the redirected session request: False
    Initiator weighted load: 1000
Initiator iqn.1987-05.com.cisco:01.5ef81885f8d
    VRRP group id: 41, VRRP IP address: 209.165.200.226
    Assigned to switch wwn: 20:00:00:0d:ec:0c:6b:c0
        ifindex: GigabitEthernet2/3.441
    Waiting for the redirected session request: False
    Initiator weighted load: 1000
Initiator iqn.1987-05.com.cisco:01.8fbdb3fdf8
    VRRP group id: 41, VRRP IP address: 209.165.200.226
    Assigned to switch wwn: 20:00:00:0d:ec:02:cb:00
        ifindex: GigabitEthernet1/1.441
    Waiting for the redirected session request: False
    Initiator weighted load: 1000
Initiator iqn.1987-05.com.cisco:01.99eddd9b134
    VRRP group id: 41, VRRP IP address: 209.165.200.226
    Assigned to switch wwn: 20:00:00:0d:ec:02:cb:00
        ifindex: GigabitEthernet1/1.441
    Waiting for the redirected session request: False
    Initiator weighted load: 1000
Initiator iqn.1987-05.com.cisco:01.a1398a8c6bc6
    VRRP group id: 41, VRRP IP address: 209.165.200.226
    Assigned to switch wwn: 20:00:00:0d:ec:0c:6b:c0
        ifindex: GigabitEthernet2/3.441
    Waiting for the redirected session request: False
    Initiator weighted load: 1000
Initiator iqn.1987-05.com.cisco:01.e15c63d09d18
    VRRP group id: 41, VRRP IP address: 209.165.200.226
    Assigned to switch wwn: 20:00:00:0d:ec:02:cb:00
        ifindex: GigabitEthernet1/2.441
    Waiting for the redirected session request: False
    Initiator weighted load: 1000
Initiator iqn.1987-05.com.cisco:01.e9aab57a51e0
    VRRP group id: 41, VRRP IP address: 209.165.200.226
    Assigned to switch wwn: 20:00:00:0d:ec:02:cb:00
        ifindex: GigabitEthernet1/1.441
    Waiting for the redirected session request: False
    Initiator weighted load: 1000
Initiator iqn.1987-05.com.cisco:01.ecc2b77b6086
    VRRP group id: 41, VRRP IP address: 209.165.200.226
    Assigned to switch wwn: 20:00:00:0d:ec:0c:6b:c0
        ifindex: GigabitEthernet2/2.441
    Waiting for the redirected session request: False
    Initiator weighted load: 1000
Initiator iqn.1987-05.com.cisco:01.f047da798a44
    VRRP group id: 41, VRRP IP address: 209.165.200.226
    Assigned to switch wwn: 20:00:00:0d:ec:02:cb:00
        ifindex: GigabitEthernet1/2.441
    Waiting for the redirected session request: False
    Initiator weighted load: 1000
Initiator iqn.1987-05.com.cisco:01.f686f5cd11f
    VRRP group id: 41, VRRP IP address: 209.165.200.226
    Assigned to switch wwn: 20:00:00:0d:ec:0c:6b:c0
        ifindex: GigabitEthernet2/1.441
    Waiting for the redirected session request: False
    Initiator weighted load: 1000
```

Related Commands

Command	Description
show islb cfs-session status	Displays iSLB session information.
show islb initiator	Displays iSLB initiator information.
show islb merge status	Displays iSLB merge status information.
show islb pending	Displays iSLB pending configurations.
show islb pending-diff	Displays iSLB CFS pending configuration differences.
show islb session	Displays iSLB session information.
show islb status	Displays iSLB CFS status information.
show islb virtual-target	Displays iSLB virtual target information.

show isns

To display Internet Storage Name Service (iSNS) information, use the **show isns** command.

show isns {**config**|**database** [{**full**|**virtual-targets** [{**local**|**switch** *switch-wwn*}]}]|**entity** [{**all [detail]**|**id** *entity-id*}]|**iscsi global config** [{**all**|**switch** *switch-wwn*}]|**node** [{**all [detail]**|**configured**|**detail**|**name** *node-name*|**virtual** [**switch** *switch-wwn* **[detail]**]}]|**portal** [{**all [detail]**|**detail**|**ipaddress** *ip-address* **port** *tcp-port*|**virtual** [**switch** *switch-wwn* **[detail]**]}]|**profile** [{*profile-name* **[counters]**|**counters**}]|**query** *profile-name* {**gigabitethernet** *slot* / *port*|**port-channel** *port*}|**stats**}

Syntax Description

config	Displays iSNS server configuration.
database	Displays the iSNS database contents.
full	(Optional) Specifies all virtual targets or registered nodes in database.
virtual-targets	(Optional) Specifies just virtual targets.
local	(Optional) Specifies only local virtual targets.
switch *switch-wwn*	(Optional) Specifies a specific switch WWN. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
entity	Displays entity attributes.
all	(Optional) Specifies all information.
detail	(Optional) Specifies detailed information.
id *entity-id*	(Optional) Specifies an entity ID. Maximum length is 255.
iscsi global config	Displays iSCSI global configuration for import of Fibre Channel targets.
node	Displays node attributes.
configured	Specifies configured nodes with detailed information.
name *node-name*	(Optional) Specifies the node name. Maximum length is 255.
virtual	Specifies virtual targets.
portal	Displays portal attributes.
ipaddress *ip-address*	Specifies the IP address for the portal.
port *tcp-port*	(Optional) Specifies the TCP port for the portal. The range is 1 to 66535.
profile	(Optional) Displays iSNS profile information.
profile-name	Specifies a profile name. Maximum length is 64 characters.
counters	(Optional) Specifies statistics for the interfaces.

query profile-name	Specifies a query to send to the iSNS server.
gigabitethernet *slot*/*port*	Specifies a Gigabit Ethernet interface.
port-channel *port*	Specifies a PortChannel interface. The range is 1 to 128.
stats	Displays iSNS server statistics.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(x)	Added **config**, **database**, **entity**, **iscsi**, **node**, **portal**, and **stats** options.

Usage Guidelines

To access all but the **profile** and **query** options for this command, you must perform the **isns-server enable** command.

Examples

The following example shows how to display the iSNS configuration:

```
switch# show isns config
Server Name: ips-hac1(Cisco Systems) Up since: Mon Apr 27 06:59:49 1981
    Index: 1    Version: 1     TCP Port: 3205
    fabric distribute (remote sync): ON
    ESI
       Non Response Threshold: 5 Interval(seconds): 60
   Database contents
       Number of Entities: 1
       Number of Portals: 0
       Number of ISCSI devices: 2
       Number of Portal Groups: 0
```

The following example displays a specified iSNS profile:

```
switch# show isns profile ABC
iSNS profile name ABC
tagged interface GigabitEthernet2/3
iSNS Server 10.10.100.204
```

The following example displays all iSNS profiles.

```
switch# show isns profile
iSNS profile name ABC
tagged interface GigabitEthernet2/3
iSNS Server 10.10.100.204
iSNS profile name NBV
tagged interface GigabitEthernet2/5
iSNS Server 10.10.100.201
```

The following example displays iSNS PDU statistics for a specified iSNS profile:

```
switch# show isns profile ABC counters
iSNS profile name ABC
tagged interface GigabitEthernet2/3
iSNS statistics
  Input 54 pdus (registration/deregistration pdus only)
    Reg pdus 37,  Dereg pdus 17
  Output 54 pdus (registration/deregistration pdus only)
    Reg pdus  37,  Dereg pdus 17
iSNS Server  10.10.100.204
```

The following example displays iSNS PDU statistics for all iSNS profiles:

```
switch# show isns profile counters
iSNS profile name ABC
tagged interface GigabitEthernet2/3
iSNS statistics
  Input 54 pdus (registration/deregistration pdus only)
    Reg pdus 37,  Dereg pdus 17
  Output 54 pdus (registration/deregistration pdus only)
    Reg pdus  37,  Dereg pdus 17
iSNS Server  10.10.100.204
iSNS profile name NBV
tagged interface GigabitEthernet2/5
iSNS statistics
  Input 54 pdus (registration/deregistration pdus only)
    Reg pdus 37,  Dereg pdus 17
  Output 54 pdus (registration/deregistration pdus only)
    Reg pdus  37,  Dereg pdus 17
iSNS Server  10.10.100.201
```

Related Commands

Command	Description
isns-server enable	Enables the iSNS server.

show ivr

To display various Inter-VSAN Routing (IVR) configurations, use the **show ivr** command.

show ivr [{**pending**|**pending-diff**|**session status**|**virtual-domains** [**vsan** *vsan-id*]|**virtual-fcdomain-add-status**|**vsan-topology** [{**active**|**configured**}]|**zone** [{**active**|**name** *name* **[active]**}]|**zoneset** [{**active**|**brief**|**fabric**|**name** *name*|**status**}]}]

Syntax Description

pending	(Optional) Displays the IVR pending configuration.
pending-diff	(Optional) Displays the IVR pending configuration differences with the active configuration.
session	(Optional) Displays the IVR session status.
status	(Optional) Displays the status of the configured IVR session.
virtual-domains	(Optional) Displays IVR virtual domains for all local VSANs.
vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is 1 to 4093.
virtual-fcdomain-add-status	(Optional) Displays IVR virtual fcdomain status.
vsan-topology	(Optional) Displays the IVR VSAN topology
active	(Optional) Displays the active IVR facilities.
configured	(Optional) Displays the configured IVR facilities
zone	(Optional) Displays the Inter-VSA Zone (IVZ) configurations.
name *name*	(Optional) Specifies the name as configured in the database.
zoneset	(Optional) Displays the Inter-VSA Zone Set (IVZS) configurations.
brief	(Optional) Displays configured information in brief format.
fabric	(Optional) Displays the status of active zone set in the fabric.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(1b)	Added the pending and pending-diff keywords.

Usage Guidelines

To access this command, you must perform the **ivr enable** command.

Examples

The following example displays the status of the IVR virtual domain configuration:

```
switch# show ivr virtual-fcdomain-add-status
IVR virtual domains are added to fcdomain list in VSANS: 1
(As well as to VSANs in interoperability mode 2 or 3)
```

The following example displays IVR-enabled switches for a specified VSAN:

```
switch# show ivr enabled-switches vsan 2
AFID    VSAN    DOMAIN      CAPABILITY  SWITCH WWN
-----------------------------------------------------------------
   1      2     0x62( 98)    00000001    20:00:00:05:30:01:1b:c2 *
Total:   1 ivr-enabled VSAN-Domain pair>
```

The following example displays the status of the IVR session:

```
switch# show ivr session status
Last Action               : None
Last Action Result        : None
Last Action Failure Reason : None
```

The following example displays the configured IVR VSAN topology:

```
switch# show ivr vsan-topology
AFID  SWITCH WWN                Active   Cfg. VSANS
-----------------------------------------------------------
   1  20:00:00:05:30:00:3c:5e     yes     yes  3,2000
   1  20:00:00:05:30:00:58:de     yes     yes  2,2000
   1  20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
   1  20:02:00:44:22:00:4a:05     yes     yes  1-2,6
   1  20:02:00:44:22:00:4a:07     yes     yes  2-5
Total:   5 entries in active and configured IVR VSAN-Topology
Current Status: Inter-VSAN topology is ACTIVE
Last activation time: Sat Mar 22 21:46:15 1980
```

The following example displays the active IVR VSAN topology:

```
switch# show ivr vsan-topology active
AFID  SWITCH WWN                Active   Cfg. VSANS
-----------------------------------------------------------
   1  20:00:00:05:30:00:3c:5e     yes     yes  3,2000
   1  20:00:00:05:30:00:58:de     yes     yes  2,2000
   1  20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
   1  20:02:00:44:22:00:4a:05     yes     yes  1-2,6
   1  20:02:00:44:22:00:4a:07     yes     yes  2-5
Total:   5 entries in active IVR VSAN-Topology
Current Status: Inter-VSAN topology is ACTIVE
Last activation time: Sat Mar 22 21:46:15
```

The following example displays the configured IVR VSAN topology:

```
switch# show ivr vsan-topology configured
AFID  SWITCH WWN                Active   Cfg. VSANS
-----------------------------------------------------------
   1  20:00:00:05:30:00:3c:5e     yes     yes  3,2000
   1  20:00:00:05:30:00:58:de     yes     yes  2,2000
   1  20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
   1  20:02:00:44:22:00:4a:05     yes     yes  1-2,6
   1  20:02:00:44:22:00:4a:07     yes     yes  2-5
Total:   5 entries in configured IVR VSAN-Topology
```

The following example displays the combined user-defined and the automatically discovered IVR VSAN topology database:

```
switch(config)# show ivr vsan-topology
AFID  SWITCH WWN                Active   Cfg. VSANS
--------------------------------------------------------------
   1  20:00:00:0d:ec:04:99:00     yes      no  1-4
   1  20:00:00:0d:ec:0e:9c:80 *   yes      no  2,6-7,9
   1  20:00:00:0d:ec:0e:b0:40     yes      no  1-3,5,8
   1  20:00:00:0d:ec:04:99:00      no     yes  1-4
   1  20:00:00:0d:ec:0e:9c:80 *    no     yes  2,6-7,9
   1  20:00:00:0d:ec:0e:b0:40      no     yes  1-3,5,8
Total:   6 entries in active and configured IVR VSAN-Topology
```

Table 10: show ivr vsan-topology Field Descriptions, on page 1449 describes the significant fields shown in the **show ivr vsan-topology** display.

Table 10: show ivr vsan-topology Field Descriptions

Field	Description
AFID	Autonomous fabric ID (AFID)
Switch WWN	Switch world wide number
Active	Automatically discovered
Cfg.	Manually configured
VSANS	VSANs configured

The following example displays the IVZ configuration:

```
switch# show ivr zone
zone name Ivz_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
zone name ivr_qa_z_all
    pwwn 21:00:00:e0:8b:06:d9:1d vsan 1
    pwwn 21:01:00:e0:8b:2e:80:93 vsan 4
    pwwn 10:00:00:00:c9:2d:5a:dd vsan 1
    pwwn 10:00:00:00:c9:2d:5a:de vsan 2
    pwwn 21:00:00:20:37:5b:ce:af vsan 6
    pwwn 21:00:00:20:37:39:6b:dd vsan 6
    pwwn 22:00:00:20:37:39:6b:dd vsan 3
    pwwn 22:00:00:20:37:5b:ce:af vsan 3
    pwwn 50:06:04:82:bc:01:c3:84 vsan 5
```

The following example displays the active IVZS configuration:

```
switch# show ivr zoneset active
zoneset name IVR_ZoneSet1
  zone name Ivz_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

The following example displays information for a specified IVZ:

```
switch# show ivr zone name Ivz_vsan2-3
```

```
zone name Ivz_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

The following example displays the specified zone in the active IVZS:

```
switch# show ivr zone name Ivz_vsan2-3 active
zone name Ivz_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

The following example displays the IVZS configuration:

```
switch# show ivr zoneset
zoneset name ivr_qa_zs_all
  zone name ivr_qa_z_all
    pwwn 21:00:00:e0:8b:06:d9:1d vsan 1
    pwwn 21:01:00:e0:8b:2e:80:93 vsan 4
    pwwn 10:00:00:00:c9:2d:5a:dd vsan 1
    pwwn 10:00:00:00:c9:2d:5a:de vsan 2
    pwwn 21:00:00:20:37:5b:ce:af vsan 6
    pwwn 21:00:00:20:37:39:6b:dd vsan 6
    pwwn 22:00:00:20:37:39:6b:dd vsan 3
    pwwn 22:00:00:20:37:5b:ce:af vsan 3
    pwwn 50:06:04:82:bc:01:c3:84 vsan 5
zoneset name IVR_ZoneSet1
  zone name Ivz_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

The following example displays brief information for an IVR VSAN topology:

```
switch# show ivr vsan-topology configured
AFID  SWITCH WWN                 Active   Cfg. VSANS
-----------------------------------------------------------
   1  20:00:00:05:30:00:3c:5e     yes     yes  3,2000
   1  20:00:00:05:30:00:58:de     yes     yes  2,2000
   1  20:00:00:05:30:01:1b:c2 *   yes     yes  1-2
   1  20:02:00:44:22:00:4a:05     yes     yes  1-2,6
   1  20:02:00:44:22:00:4a:07     yes     yes  2-5
Total:   5 entries in configured IVR VSAN-Topology
```

The following example displays brief information for the active IVZS:

```
switch# show ivr zoneset brief Active
zoneset name IVR_ZoneSet1
  zone name Ivz_vsan2-3
```

The following example displays the status information for the IVZ:

```
switch# show ivr zoneset brief status
Zoneset Status

_______________
    name               : IVR_ZoneSet1
    state              : activation success
    last activate time : Sat Mar 22 21:38:46 1980
    force option       : off
status per vsan:

__________________
     vsan     status

     ____     ______
     2        active
```

The following example displays the specified zone set:

```
switch# show ivr zoneset name IVR_ZoneSet1
zoneset name IVR_ZoneSet1
  zone name Ivz_vsan2-3
    pwwn 21:00:00:e0:8b:02:ca:4a vsan 3
    pwwn 21:00:00:20:37:c8:5c:6b vsan 2
```

Related Commands

Command	Description
ivr distribute	Enables IVR CFS distribution.
ivr enable	Enables IVR.

show ivr aam

To display IVR AAM status, use the **show ivr aam** command.

show ivr aam

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display IVR AAM status:

```
switch(config)# show ivr aam
AAM mode status
--------------------------
AAM is disabled
switch(config)#
```

Related Commands

Command	Description
show fc-redirect-active configs	Displays all active configurations on a switch.

show ivr aam pre-deregister-check

To display IVR pre de-register check status, use the show ivr amm pre-deregister-check command.

show ivr aam pre-deregister-check

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display IVR de-register with check entries:

```
switch(config)# show ivr aam pre-deregister-check
AAM pre-deregister check status
--------------------------
FAILURE
There are merged entries or AAM has not been enabled with the following switches:
switch swwn 20:00:00:05:30:00:15:de
User has two options:
1. User can go ahead to issue ivr commit, but the above switches in the fabric may fail to
 deregister.
2. User may also run "ivr abort", then resolve above switches and re-issue the ivr aam
deregister.
Warning: IVR AAM pre-deregister-check status may not be up-to-date. Please issue the command
 "ivr aam pre-deregi
ster-check" to get updated status.
switch(config)#
```

The following example shows how to display IVR deregister without check status entries:

```
switch(config)# ivr aam pre-deregister-check
switch(config)# show ivr aam pre-deregister-check
AAM pre-deregister check status
--------------------------
SUCCESS
Warning: IVR AAM pre-deregister-check status may not be up-to-date. Please issue the command
 "ivr aam pre-deregister
-check" to get updated status.
switch(config)#
```

Related Commands

Command	Description
ivr enable	Enables the inter-VSAN Routing (IVR) feature.

show ivr fcdomain database

To display the IVR fcdomain database that contains the persistent FC ID mapping, use the **show ivr fcdomain database** command.

show ivr fcdomain database [**autonomous-fabric-num** *afid-num* **vsan** *vsan-id*]

Syntax Description

autonomous-fabric-num *afid-num*	(Optional) Specifies the AFID. The range is 1 to 64.
vsan *vsan-id*	(Optional) Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays all IVR fcdomain database entries:

```
switch# show ivr fcdomain database
-------------------------------------------------
  AFID  Vsan  Native-AFID  Native-Vsan  Virtual-domain
-------------------------------------------------
    1     2        10          11         0xc(12)
   21    22        20          11         0xc(12)
Number of Virtual-domain entries: 2
-------------------------------------------------
  AFID  Vsan          Pwwn           Virtual-fcid
-------------------------------------------------
   21    22  11:22:33:44:55:66:77:88  0x114466
   21    22  21:22:33:44:55:66:77:88  0x0c4466
   21    22  21:22:33:44:55:66:78:88  0x0c4466
Number of Virtual-fcid entries: 3
```

The following example displays the IVR fcdomain database entries for a specific AFID and VSAN:

```
switch# show ivr fcdomain database autonomous-fabric-num 21 vsan 22
-------------------------------------------------
  AFID  Vsan  Native-AFID  Native-Vsan  Virtual-domain
-------------------------------------------------
   21    22        20          11         0xc(12)
Number of Virtual-domain entries: 1
-------------------------------------------------
  AFID  Vsan          Pwwn           Virtual-fcid
-------------------------------------------------
   21    22  11:22:33:44:55:66:77:88  0x114466
   21    22  21:22:33:44:55:66:77:88  0x0c4466
```

```
   21    22  21:22:33:44:55:66:78:88  0x0c4466
Number of Virtual-fcid entries: 3
```

Related Commands

Command	Description
ivr fcdomain database autonomous-fabric-num	Creates IVR persistent FC IDs.

show ivr service-group

To display an inter-VSAN routing (IVR) service groups, use the **show ivr service-group** command.

show ivr service-group [{**active**|**configured**}]

Syntax Description

active	(Optional) Displays active IVR service groups.
configured	(Optional) Displays configured IVR service groups.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can configure a maximum of 16 IVR service groups.

Examples

The following example displays IIVR service groups:

```
switch# show ivr service-group
IVR CONFIGURED Service Group
====================================
SG-ID SG-NAME AFID VSANS
--------------------------------------------------------------------------------
1 sg-100 1 200-201,250,270
2 sg-200 1 100-101,150,170
Total: 2 entries in configured service group table
IVR ACTIVE Service Group
====================================
SG-ID SG-NAME AFID VSANS
--------------------------------------------------------------------------------
1 sg-100 1 200-201,250,270
2 sg-200 1 100-101,150,170
Total: 2 entries in active service group table
```

Related Commands

Command	Description
clear ivr service-group database	Clears an IVR service group database.
ivr service-group name	Configures an IVR service group.

show ivr virtual-fcdomain-add-status2

To display the Request Domain ID (RDI) mode in a specific AFID and VSAN for all IVR-enabled switches, use the show ivr virtual-fcdomain-add-status2 command.

show ivr virtual-fcdomain-add-status2

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Exec mode

Command History

Release	Modification
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the RDI mode in the local switch:

```
switch# show ivr virtual-fcdomain-add-status2
IVR virtual domains are added to fcdomain list in VSANS: 2 for afid 1
```

Related Commands

Command	Description
ivr virtual-fcdomain-add2	Configures the RDI mode in a specific AFID and VSAN for all IVR-enabled switches.

show ivr virtual-switch-wwn

To display an inter-VSAN routing (IVR) virtual switch WWN, use the **show ivr virtual-switch-wwn** command.

show ivr virtual-switch-wwn native-switch-wwn switch-wwn native-vsan vsan-id

Syntax Description

native-switch-wwn *switch-wwn*	Specifies the sWWN of the native switch. The format is in dotted hex.
native-vsan *vsan-id*	Specifies the ID of the native VSAN. The range is 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The sWWN of the virtual switch must be present in the fabric binding database of all the VSANs where the virtual switch is in use. If the sWWN is not in the database, you must add it before attempting to implement FICON over IVR.

Examples

The following example displays an IVR virtual sWNN:

```
switch# show ivr virtual-switch-wwn native-switch-wwn
20:00:00:0d:ec:00:8c:c0 native-vsan 1
virtual switch wwn : 20:01:00:0d:ec:00:8c:c1
```

Related Commands

Command	Description
show ivr	Displays IVR information.

show kernel core

To display kernel core configuration information, use the **show kernel core** command.

show kernel core {**limit**|**module** *slot*|**target**}

Syntax Description

limit	Displays the configured line card limit.
module *slot*	Displays the kernel core configuration for a module in the specified slot.
target	Displays the configured target IP address.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following examples display kernel core settings:

```
switch# show kernel core limit
2
switch# show kernel core target
10.50.5.5
switch# show kernel core module 5
module 5 core is enabled
         level is header
         dst_ip is 10.50.5.5
         src_port is 6671
         dst_port is 6666
         dump_dev_name is eth1
         dst_mac_addr is 00:00:0C:07:AC:01
```

show ldap-search-map

To display LDAP configuration information, use the show ldap-search-map command.

show ldap-search-map

Syntax Description

This command has no argument or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

```
The following example shows how to display LDAP configuration information:
switch# show ldap-search-map
total number of search maps : 0
switch#
```

Related Commands

Command	Description
ldap-server host	Displays LDAP server Ip address.

show ldap-server

To display the configured parameters for all the LDAP servers, use the show ldap-server command.

show ldap-server

Syntax Description

This command has no argument or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

```
The following example shows how to display the configured parameters for all the LDAP
servers:
switch# show ldap-server
timeout : 3
        port : 65534
    deadtime : 5
total number of servers : 2
following LDAP servers are configured:
    a:
                idle time:0
                test user:test
                test password:********
        timeout: 3    port: 1    rootDN:
        enable-ssl: true
    ipaddress:
                idle time:0
                test user:test
                test password:********
        timeout: 3    port: 65534    rootDN:
        enable-ssl: false
switch#
```

Related Commands

Command	Description
ldap-server host	Displays LDAP server Ip address.

show ldap-server groups

To display the configured parameter for all the LDAP server groups, use the show ldap-server groups command.

show ldap-server groups

Syntax Description

This command has no argument or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

```
The following example shows how to display the configured parameters for all the LDAP server
 groups:
switch# show ldap-server groups
total number of groups: 3
following LDAP server groups are configured:
    group ldap:
Authentication: Search and Bind
        Authentication Mech: Default(PLAIN)
    group a:
Authentication: Bind and Search
        CERT-DN match enabled
        Group validation enabled
        Authentication Mech: PLAIN
    group name:
Authentication: Search and Bind
        Authentication Mech: Default(PLAIN)
switch#
```

Related Commands

Command	Description
ldap-server host	Displays LDAP server Ip address.

show license

To display license information, use the **show license** command.

show license [{**brief**|**default**|**file** *filename*|**host-id** *license-name*|**usage**}]

Syntax Description

brief	(Optional) Displays a list of license files installed on a switch.
default	Optional) Displays services using a default license.
file *filename*	Optional) Displays information for a specific license file.
host-id *license-name*	Optional) Displays host ID used to request node-locked license.
usage	Optional) Displays information about the current license usage.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(2)	This command was introduced.
3.1(2)	Added the **default** keyword.

Usage Guidelines

None.

Examples

The following example displays a specific license installed on a switch:

```
switch# show license file fcports.lic
fcports.lic:
SERVER this_host ANY
VENDOR cisco
FEATURE fcports cisco 1.000 permanent 30 HOSTID=VDH=4C0AF664 \
        SIGN=24B2B68AA676 <------------------------ fcport license
```

The following example displays a list of license files installed on a switch:

```
switch# show license brief
fcports.lic
ficon.lic
```

The following example displays all licenses installed on a switch:

```
switch# show license
fcports.lic:
SERVER this_host ANY
VENDOR cisco
FEATURE fcports cisco 1.000 permanent 30 HOSTID=VDH=4C0AF664 \
        SIGN=24B2B68AA676 <-------------------------fcport license
```

```
ficon.lic:
FEATURE ficon cisco 1.000 permanent uncounted HOSTID=VDH=4C0AF664 \
        SIGN=CB7872B23700 <----------------------------ficon license
```

The following example displays the host IDs, required to request node locked license:

```
switch# show license host-id
License hostid:VDH=4C0AF664
The following example displays information about current license usage.
switch# show license usage
Feature                 Installed   License Status  ExpiryDate   Comments
                                    Count
--------------------------------------------------------------------------------------------
FM_SERVER_PKG           Yes         -       Unused   never        license missing
MAINFRAME_PKG           No          -       Unused                Grace Period 57days15hrs
ENTERPRISE_PKG          Yes         -       InUse    never        -
SAN_EXTN_OVER_IP        No          0       Unused                -
SAN_EXTN_OVER_IP_IPS4   No          0       Unused
--------------------------------------------------------------------------------------------
```

The following example displays services using a default license:

```
switch# show license default
Feature                              Default License Count
-------------------------------------------------------------------------------
FM_SERVER_PKG                        -
ENTERPRISE_PKG                       -
PORT_ACTIVATION_PKG                  12
10G_PORT_ACTIVATION_PKG              0
-------------------------------------------------------------------------------
```

show line

To configure a virtual terminal line, use the **show line** command.

show line [{**com1** [**user-input-string**]|**console** [{**connected**|**user-input-string**}]}]

Syntax Description

com1	(Optional) Displays auxiliary line configuration.
user-input-string	(Optional) Displays the user-input initial string.
console	(Optional) Displays console line configuration.
connected	(Optional) Displays the physical connection status.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.
3.0(1)	Modified examples for Supervisor-1 and Supervisor-2 modules.

Usage Guidelines

None.

Examples

The following example displays output from an MDS switch with a Supervisor-1 module:

```
switch# show line console
line Console:
Speed: 9600 bauds
Databits: 8 bits per byte
Stopbits: 1 bit(s)
Parity: none
Modem In: Enable
Modem Init-String -
default : ATE0Q1&D2&C1S0=1\015
Statistics: tx:12842 rx:366 Register Bits:RTS|CTS|DTR|DSR|CD|RI
```

The following example displays output from an MDS switch with a Supervisor-2 module:

```
switch# show line console
line Console:
Speed: 9600 bauds
Databits: 8 bits per byte
Stopbits: 1 bit(s)
Parity: none
Modem In: Enable
Modem Init-String -
default :
ATE0Q0V1&D0&C0S0=1\015
Statistics: tx:12842 rx:366 Register Bits:RTS|CTS|DTR|DSR|CD|RI
```

The following example displays output from an MDS switch with a Supervisor-1 module:

```
switch# show line com1
line Aux:
Speed: 9600 bauds
Databits: 8 bits per byte
Stopbits: 1 bit(s)
Parity: none
Modem In: Enable
Modem Init-String -
default : ATE0Q1&D2&C1S0=1\015
Statistics: tx:17 rx:0 Register Bits:RTS|DTR
```

The following example displays output from an MDS switch with a Supervisor-2 module:

```
switch# show line com1
line Aux:
Speed: 9600 bauds
Databits: 8 bits per byte
Stopbits: 1 bit(s)
Parity: none
Modem In: Enable
Modem Init-String -
default :
ATE0Q0V1&D0&C0S0=1\015
Statistics: tx:17 rx:0 Register Bits:RTS|DTR
```

Related Commands

Command	Description
clear line	Deleted configured line sessions.
line aux	Configures the auxiliary COM 1 port.
line console	Configures primary terminal line.

show locator-led status

To show the status of locator LEDs on the system, use the **show locator-led status** command.

show locator-led status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

network-adminnetwork-operatorvdc-adminvdc-operator

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following example shows the locator LED status for the system:

```
switch# show locator-led status
```

Component	Locator LED Status

Chassis	off
Module 1	off
Module 2	off
Module 3	off
Module 4	off
Module 5	off
Module 6	off

Xbar 2	off
Xbar 3	off
Xbar 5	off
Xbar 6	off
PowerSupply 1	off
PowerSupply 2	off
PowerSupply 3	off
Fan 1	off
Fan 2	off
Fan 3	off

Related Commands

Command	Description
locator-led	Blinks an LED on the system.

show logging

To display the current message logging configuration, use the **show logging** command .

show logging [{**console**|**info**|**last lines**|**level** *facility*|**logfile**|**module**|**monitor**|**nvram** [**last lines**]|**onboard information**|**pending**|**pending-diff**|**server**|**status**}]

Syntax Description

console	(Optional) Displays console logging configuration.
info	(Optional) Displays logging configuration.
last lines	(Optional) Displays last few lines of the log file. The range is 1 to 9999.
level *facility*	(Optional) Displays facility logging configuration. Facility values include **aaa**, **acl**, **auth**, **authpriv**, **bootvar**, **callhome**, **cdp**, **cfs**, **cimserver**, **cron**, **daemon**, **device-alias**, **dstats**, **ethport**, **fc2d**, **fcc**, **fcd**, **fcdomain**, **fcns**, **fcsp-mgr**, **fdmi**, **ficon**, **flogi**, **fspf**, ftp, **ike**, **ipacl**, **ipconf**, **ipfc**, **ips**, **ipsec**, **isns**, kernel, **license**, localn, lpr, mail, **mcast**, **module**, **news**, **platform**, **port**, **port-security**, **qos**, **radius**, **rdl**, **rib**, **rlir**, **rscn**, **scsi-target**, **security**, **syslog**, **sysmgr**, **systemhealth**, **tacacs**, **tlport**, **user**, **uucp**, **vni**, **vrrp-cfg**, vsan, **vshd**, **wwm**, **xbar**, and **zone**.
logfile	(Optional) Displays contents of the log file.
module	(Optional) Displays module linecard logging configuration.
monitor	Displays monitor logging configuration.
nvram	Displays NVRAM log.
onboard *information*	(Optional) Displays onboard failure logging (OBFL) information. The types of information include **boot-uptime**, **cpu-hog**, **device-version**, **endtime**, **environmental-history**, **error-stats**, **exception-log**, **interrupt-stats**, **mem-leak**, **miscellaneous-error**, **module**, **obfl-history**, **obfl-logs**, **register-log**, **stack-trace**, **starttime**, **status**, and **system-health**.
pending	(Optional) Displays the server address pending configuration.
pending-diff	(Optional) Displays the server address pending configuration differences with the active configuration.
server	(Optional) Displays server logging configuration.
status	(Optional) Displays the status of the last operation.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
5.2(1)	Added a new comment.
1.3(1)	This command was introduced.
2.0(x)	Added the pending, pending-diff, and **status** keywords.
3.0(1)	Added the **onboard** keyword.

Usage Guidelines

None.

Examples

The following example displays module linecard logging configuration:

```
switch# show logging module
Logging linecard:                enabled (Severity: notifications)
switch#
```

The following example displays level for module linecard manager logging configuration:

```
switch# show logging level module
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
module                  5                       1
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
switch#
```

The following example displays current system message logging:

```
switch# show logging

Logging console:                enabled (Severity: notifications)
Logging monitor:                enabled (Severity: information)
Logging linecard:               enabled (Severity: debugging)
Logging server:                 enabled
{172.22.0.0}
        server severity:        debugging
        server facility:        local7
{172.22.0.0}
        server severity:        debugging
        server facility:        local7
Logging logfile:                enabled
        Name - external/sampleLogFile: Severity - notifications Size - 3000000
syslog_get_levels :: Error(-1) querying severity values for fcmpls at SAP 30
syslog_get_levels :: Error(-1) querying severity values for fcfwd at SAP 38
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
kern                    6                       4
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       0
syslog                  3                       3
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
```

```
authpriv                3                       3
ftp                     3                       3
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
zone                    2                       2
vni                     2                       2
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
acl                     2                       2
tlport                  2                       2
port                    5                       5
port_channel            5                       5
fcmpls                  0                       0
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
vrrp_cfg                2                       2
fcfwd                   0                       0
ntp                     2                       2
platform                5                       5
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rscn                    2                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
Nov  8 16:48:04 excal-113 %LOG_VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console
from pts/1 (171.71.58.56)
Nov  8 17:44:09 excal-113 %LOG_VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console
from pts/0 (171.71.58.72)
```

The following example displays console logging status:

```
switch# show logging
 console

Logging console:                enabled (Severity: notifications)
```

The following example displays logging facility status:

```
switch# show logging
 facility
syslog_get_levels :: Error(-1) querying severity values for fcmpls at SAP 30
syslog_get_levels :: Error(-1) querying severity values for fcfwd at SAP 38
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
```

```
kern                    6                       4
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       0
syslog                  3                       3
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
authpriv                3                       3
ftp                     3                       3
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
zone                    2                       2
vni                     2                       2
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
acl                     2                       2
tlport                  2                       2
port                    5                       5
port_channel            5                       5
fcmpls                  0                       0
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
vrrp_cfg                2                       2
fcfwd                   0                       0
ntp                     2                       2
platform                5                       5
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rscn                    2                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

The following example displays logging information:

```
switch# show logging
 info

Logging console:                enabled (Severity: notifications)
Logging monitor:                enabled (Severity: information)
Logging linecard:               enabled (Severity: debugging)
Logging server:                 enabled
{172.22.95.167}
```

```
        server severity:        debugging
        server facility:        local7
{172.22.92.58}
        server severity:        debugging
        server facility:        local7
Logging logfile:                enabled
        Name - external/sampleLogFile: Severity - notifications Size - 3000000
syslog_get_levels :: Error(-1) querying severity values for fcmpls at SAP 30
syslog_get_levels :: Error(-1) querying severity values for fcfwd at SAP 38
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
kern                    6                       4
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       0
syslog                  3                       3
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
authpriv                3                       3
ftp                     3                       3
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
zone                    2                       2
vni                     2                       2
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
acl                     2                       2
tlport                  2                       2
port                    5                       5
port_channel            5                       5
fcmpls                  0                       0
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
vrrp_cfg                2                       2
fcfwd                   0                       0
ntp                     2                       2
platform                5                       5
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rscn                    2                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

The following example displays last few lines of a log file:

```
switch# show logging
 last 2
Nov  8 16:48:04 excal-113 %LOG_VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console
from pts/1 (171.71.58.56)
Nov  8 17:44:09 excal-113 %LOG_VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console
from pts/0 (171.71.58.72)
```

The following example displays monitor logging status.

```
switch# show logging
 monitor

Logging monitor:                enabled (Severity: information)
```

The following example displays server information:

```
switch# show logging
 server

Logging server:                 enabled
{172.22.95.167}
        server severity:        debugging
        server facility:        local7
{172.22.92.58}
        server severity:        debugging
        server facility:        local7
```

The following example shows onboard failure logging for boot-uptime for module 2:

```
switch# show logging onboard module 2 boot-uptime
---------------------------
    Module:  2
---------------------------


Wed Nov  9 12:05:56 2005:  Boot Record
-------------------------------------------------------------------------------
Boot Time..........:  Wed Nov  9 12:05:56 2005
Slot Number........:  2
Serial Number......:  JAB0912026U
Bios Version.......:    v0.0.8(08/18/05)
Alt Bios Version...:    v0.0.8(08/18/05)
Firmware Version...:  3.0(1) [build 3.0(0.276)]


Wed Nov  9 11:58:04 2005:  Card Uptime Record
---------------------------------------------
Uptime: 273, 0 days 0 hour(s) 4 minute(s) 33 second(s)
Reset Reason: Reset Requested by CLI command reload (9)
Card Mode..........................:  Runtime




Wed Nov  9 12:05:56 2005:  Card Uptime Record
---------------------------------------------
Uptime: 32, 0 days 0 hour(s) 0 minute(s) 32 second(s)
Reset Reason: Unknown (0)
Card Mode..........................:  Runtime
```

The following example shows onboard failure logging for boot-uptime:

```
switch# show logging onboard boot-uptime
----------------------------
    Module:  2
----------------------------


Wed Nov  9 12:05:56 2005:  Boot Record
--------------------------------------------------------------------------------
Boot Time..........:  Wed Nov  9 12:05:56 2005
Slot Number........:  2
Serial Number......:  JAB0912026U
Bios Version.......:    v0.0.8(08/18/05)
Alt Bios Version...:    v0.0.8(08/18/05)
Firmware Version...:  3.0(1) [build 3.0(0.276)]


Wed Nov  9 11:58:04 2005:  Card Uptime Record
-----------------------------------------------
Uptime: 273, 0 days 0 hour(s) 4 minute(s) 33 second(s)
Reset Reason: Reset Requested by CLI command reload (9)
Card Mode..........................:  Runtime



Wed Nov  9 12:05:56 2005:  Card Uptime Record
-----------------------------------------------
Uptime: 32, 0 days 0 hour(s) 0 minute(s) 32 second(s)
Reset Reason: Unknown (0)
Card Mode..........................:  Runtime


----------------------------
    Module:  5
----------------------------


Wed Nov  9 12:05:05 2005:  Boot Record
--------------------------------------------------------------------------------
Boot Time..........:  Wed Nov  9 12:05:05 2005
Slot Number........:  5
Serial Number......:  JAB091100TS
Bios Version.......:  00.01.01 (Oct 25 2005 - 15:48:45)
Alt Bios Version...:  00.01.01 (Oct 25 2005 - 15:48:45)
Firmware Version...:  3.0(1) [build 3.0(0.274)]


Wed Nov  9 11:58:04 2005:  Card Uptime Record
-----------------------------------------------
Uptime: 503255, 5 days 19 hour(s) 47 minute(s) 35 second(s)
Reset Reason: Reset reason: Reset Requested by CLI command reload (9)
Card Mode..........................:  Runtime



Wed Nov  9 12:05:05 2005:  Card Uptime Record
-----------------------------------------------
Uptime: 172, 0 days 0 hour(s) 2 minute(s) 52 second(s)
Reset Reason: Reset reason: Unknown (0)
Card Mode..........................:  Runtime
```

The following example shows onboard failure logging for device-version:

```
switch# show logging onboard device-version
----------------------------
    Module:  2
----------------------------

Device Version Record
-------------------------------------------------------------------------
Timestamp                  Device Name      Instance Hardware Software
                                                 Num  Version  Version
-------------------------------------------------------------------------
Wed Nov  9 12:05:56 2005   Stratosphere           0        1        1
Wed Nov  9 12:05:56 2005   Stratosphere           1        1        1
Wed Nov  9 12:05:56 2005   Skyline-asic           0        1        1
Wed Nov  9 12:05:56 2005   Tuscany-asic           0        1        0
Wed Nov  9 12:05:56 2005   X-Bus IO               0        6        0
Wed Nov  9 12:05:56 2005   Power Mngmnt Epl       0        6        0
----------------------------
    Module:  5
----------------------------

Device Version Record
-------------------------------------------------------------------------
Timestamp                  Device Name      Instance Hardware Software
                                                 Num  Version  Version
-------------------------------------------------------------------------
Wed Nov  9 12:05:05 2005   Power Mngmnt Epl       0        7        0
Wed Nov  9 12:05:05 2005   IO FPGA Molakini       0        8        0
Wed Nov  9 12:05:05 2005   bellagio2              0        1        0
Wed Nov  9 12:05:05 2005   BabyCaesar             0        1        0
```

The following example show onboard failure logging for system health:

```
switch# show logging onboard system-health

Feature supported only on active-sup
----------------------------
    Module:  5
----------------------------
Wed Nov  9 12:04:58 2005@345463 (5/31/0x0): System health started with pid 2607
Wed Nov  9 12:05:05 2005@943388 (5/31/0xb): Module Supervisor 5, swid 31 came online
Wed Nov  9 12:05:05 2005@944275 (5/31/0xb): LC config removed for module 7
Wed Nov  9 12:05:05 2005@944454 (5/31/0xb): LC config removed for module 8
Wed Nov  9 12:05:05 2005@944592 (5/31/0xb): LC config removed for module 9
Wed Nov  9 12:05:05 2005@944717 (5/31/0xb): LC config removed for module 10
Wed Nov  9 12:05:05 2005@944846 (5/31/0xb): LC config removed for module 11
Wed Nov  9 12:05:05 2005@944969 (5/31/0xb): LC config removed for module 12
Wed Nov  9 12:05:05 2005@945094 (5/31/0xb): LC config removed for module 13
Wed Nov  9 12:05:05 2005@945222 (5/31/0xb): LC config removed for module 14
Wed Nov  9 12:05:05 2005@945343 (5/31/0xb): LC config removed for module 15
Wed Nov  9 12:05:05 2005@945470 (5/31/0xb): LC config removed for module 16
Wed Nov  9 12:05:50 2005@814217 (2/29/0x0): System health started with pid 397
Wed Nov  9 12:05:56 2005@904068 (5/31/0xb): LC inserted for module 2
Wed Nov  9 12:05:59 2005@167373 (5/31/0xb): Module Linecard 2, swid 29 came online
switch# show logging onboard
boot-uptime            exception-log          obfl-logs
cpu-hog                interrupt-stats        register-log
device-version         mem-leak               stack-trace
endtime                miscellaneous-error    starttime
environmental-history  module                 status
error-stats            obfl-history           system-health
```

The following example show onboard failure logging for obfl-logs:

```
switch# show logging onboard obfl-logs
Module:  1 not online.


OBFL: Status:

    Module:  2 OBFL Log:                                      Enabled
    cpu-hog                                                   Enabled
    environmental-history                                     Enabled
    error-stats                                               Enabled
    exception-log                                             Enabled
    interrupt-stats                                           Enabled
    mem-leak                                                  Enabled
    miscellaneous-error                                       Enabled
    obfl-log (boot-uptime/device-version/obfl-history)  Enabled
    register-log                                              Enabled
    stack-trace                                               Enabled


OBFL: Memory Leak:
----------------------------
    Module:  2
----------------------------


OBFL: Stack Trace:
----------------------------
    Module:  2
----------------------------
OBFL: Environment History:
----------------------------
    Module:  2
----------------------------

========== Sensor Temperature History Log ==========
-----------------------------------------------------
Wed Nov  9 12:05:50 2005 sensor 0 temperature 31
Wed Nov  9 12:05:50 2005 sensor 1 temperature 31
Wed Nov  9 12:05:50 2005 sensor 2 temperature 29
Wed Nov  9 12:06:20 2005 sensor 0 temperature 33
Wed Nov  9 12:06:20 2005 sensor 1 temperature 34
Wed Nov  9 12:06:50 2005 sensor 0 temperature 35
Wed Nov  9 12:06:50 2005 sensor 1 temperature 36
Wed Nov  9 12:07:20 2005 sensor 1 temperature 38
Wed Nov  9 12:08:50 2005 sensor 0 temperature 37
Wed Nov  9 12:08:50 2005 sensor 1 temperature 40

========== Sensor Temperature Error Log ==========
-------------------------------------------------
Wed Nov  9 12:05:50 2005 Start of Service: sensor 0 initial temperature 31
Wed Nov  9 12:05:50 2005 Start of Service: sensor 1 initial temperature 31
Wed Nov  9 12:05:50 2005 Start of Service: sensor 2 initial temperature 29


OBFL: Interrupt Statistics:
----------------------------
    Module:  2
----------------------------


--------------------------------------------------------------------------------
```

```
 INTERRUPT COUNTS INFORMATION FOR DEVICE ID 63 DEVICE: Stratosphere
-------------------------------------------------------------------------------
                                  |        |        |   Time Stamp    |In|Port
   Interrupt Counter Name         | Count  | Thresh |MM/DD/YY HH:MM:SS|st|Rang
                                  |        |        |                 |Id|e
-------------------------------------------------------------------------------
FCP_LAF_MISC_INT_DT_IN_OBUF       |7       |0       |11/09/05 12:06:00|00|1
FCP_MAC_SR1_LR_DETECTED           |1       |0       |11/09/05 12:06:00|00|1
FCP_MAC_SR1_LRR_DETECTED          |1       |0       |11/09/05 12:06:00|00|1
FCP_MAC_SR1_OLS_DETECTED          |1       |0       |11/09/05 12:06:00|00|1
FCP_MAC_SR2_LRR_IDLE_RECEIVED     |1       |0       |11/09/05 12:06:00|00|1
FCP_MAC_SR2_AL_NON_F8_LIP_RECEIVED|2       |0       |11/09/05 12:06:00|00|1
FCP_MAC_SR2_AL_LIP_RECEIVED       |1       |0       |11/09/05 12:06:00|00|1
FCP_MAC_SR2_AL_ARB_F0_RECEIVED    |1       |0       |11/09/05 12:06:00|00|1
FCP_LAF_MISC_INT_DT_IN_OBUF       |2       |0       |11/09/05 12:06:00|00|2
FCP_MAC_SR1_OLS_DETECTED          |1       |0       |11/09/05 12:06:00|00|2
FCP_MAC_SR2_AL_NON_F8_LIP_RECEIVED|2       |0       |11/09/05 12:06:00|00|2
FCP_MAC_SR2_AL_LIP_RECEIVED       |3       |0       |11/09/05 12:06:00|00|2
FCP_LAF_MISC_INT_DT_IN_OBUF       |b       |0       |11/09/05 12:06:00|00|3
FCP_MAC_SR1_LR_DETECTED           |3       |0       |11/09/05 12:06:00|00|3
FCP_MAC_SR1_LRR_DETECTED          |2       |0       |11/09/05 12:06:00|00|3
FCP_MAC_SR1_OLS_DETECTED          |2       |0       |11/09/05 12:06:00|00|3
FCP_MAC_SR2_LR_IDLE_RECEIVED      |1       |0       |11/09/05 12:06:00|00|3
FCP_MAC_SR2_LRR_IDLE_RECEIVED     |2       |0       |11/09/05 12:06:00|00|3
FCP_MAC_SR2_AL_NON_F8_LIP_RECEIVED|3       |0       |11/09/05 12:06:00|00|3
FCP_MAC_SR2_AL_LIP_RECEIVED       |1       |0       |11/09/05 12:06:00|00|3
FCP_MAC_SR2_AL_ARB_F0_RECEIVED    |2       |0       |11/09/05 12:06:00|00|3
FCP_LAF_MISC_INT_DT_IN_OBUF       |2       |0       |11/09/05 12:06:00|00|4
FCP_MAC_SR1_LRR_DETECTED          |1       |0       |11/09/05 12:06:00|00|4
FCP_MAC_SR1_OLS_DETECTED          |3       |0       |11/09/05 12:06:00|00|4
FCP_MAC_SR2_LRR_IDLE_RECEIVED     |1       |0       |11/09/05 12:06:00|00|4
FCP_MAC_SR2_AL_NON_F8_LIP_RECEIVED|3       |0       |11/09/05 12:06:00|00|4
FCP_MAC_SR2_AL_LIP_RECEIVED       |3       |0       |11/09/05 12:06:00|00|4
FCP_LAF_MISC_INT_DT_IN_OBUF       |d       |0       |11/09/05 12:06:05|00|1
FCP_MAC_SR1_LRR_DETECTED          |2       |0       |11/09/05 12:06:05|00|1
FCP_MAC_SR1_OLS_DETECTED          |2       |0       |11/09/05 12:06:05|00|1
FCP_MAC_SR2_LRR_IDLE_RECEIVED     |2       |0       |11/09/05 12:06:05|00|1
FCP_MAC_SR2_AL_LIP_RECEIVED       |2       |0       |11/09/05 12:06:05|00|1
FCP_MAC_SR2_AL_ARB_F0_RECEIVED    |2       |0       |11/09/05 12:06:05|00|1
FCP_LAF_MISC_INT_DT_IN_OBUF       |3       |0       |11/09/05 12:06:05|00|2
FCP_MAC_SR1_LR_DETECTED           |1       |0       |11/09/05 12:06:05|00|2
FCP_MAC_SR1_OLS_DETECTED          |3       |0       |11/09/05 12:06:05|00|2
FCP_MAC_SR2_LR_IDLE_RECEIVED      |1       |0       |11/09/05 12:06:05|00|2
FCP_MAC_SR2_AL_NON_F8_LIP_RECEIVED|4       |0       |11/09/05 12:06:05|00|2


OBFL: Error Statistics:
----------------------------
    Module:  2
----------------------------


OBFL: System Bootup Record:
----------------------------
    Module:  2
----------------------------


Wed Nov  9 12:05:56 2005:  Boot Record
-------------------------------------------------------------------------------
Boot Time..........:  Wed Nov  9 12:05:56 2005
Slot Number........:  2
Serial Number......:  JAB0912026U
Bios Version.......:    v0.0.8(08/18/05)
```

```
Alt Bios Version...:    v0.0.8(08/18/05)
Firmware Version...:  3.0(1) [build 3.0(0.276)]


Wed Nov  9 12:05:56 2005:  Card Uptime Record
-----------------------------------------------
Uptime: 32, 0 days 0 hour(s) 0 minute(s) 32 second(s)
Reset Reason: Unknown (0)
Card Mode.......................:  Runtime



OBFL: Device Versions in Switch:
----------------------------
    Module:  2
----------------------------

Device Version Record
-------------------------------------------------------------------------
Timestamp                  Device Name      Instance Hardware Software
                                                Num  Version  Version
-------------------------------------------------------------------------
Wed Nov  9 12:05:56 2005   Stratosphere            0        1        1
Wed Nov  9 12:05:56 2005   Stratosphere            1        1        1
Wed Nov  9 12:05:56 2005   Skyline-asic            0        1        1
Wed Nov  9 12:05:56 2005   Tuscany-asic            0        1        0
Wed Nov  9 12:05:56 2005   X-Bus IO                0        6        0
Wed Nov  9 12:05:56 2005   Power Mngmnt Epl        0        6        0


OBFL: Exception Log:
----------------------------
    Module:  2
----------------------------


OBFL: Register Log:
----------------------------
    Module:  2
----------------------------


OBFL: Miscellaneous Error Logs:
----------------------------
    Module:  2
----------------------------

LC Config Record: Wed Nov  9 12:05:40 2005@471600
lc_copy_from_sup_to_lc() failure for sdwrap: 121


OBFL: Status:

    Module:  5 OBFL Log:                                    Enabled
    error-stats                                             Enabled
    exception-log                                           Enabled
    miscellaneous-error                                     Enabled
    obfl-log (boot-uptime/device-version/obfl-history)  Enabled
    system-health                                           Enabled
    stack-trace                                             Enabled


OBFL: Memory Leak:
```

```
----------------------------
    Module:  5
----------------------------
mem-leak: This option not supported on SUP.


OBFL: Stack Trace:
----------------------------
    Module:  5
----------------------------
stack-trace: This option not supported on SUP.


OBFL: Environment History:
----------------------------
    Module:  5
----------------------------

========== Sensor Temperature History Log ==========
----------------------------------------------------
Wed Nov  9 12:05:06 2005 sensor 0 temperature 36
Wed Nov  9 12:05:06 2005 sensor 1 temperature 35
Wed Nov  9 12:05:06 2005 sensor 2 temperature 31


OBFL: Interrupt Statistics:
----------------------------
    Module:  5
----------------------------
interrupt-stats: This option not supported on SUP.


OBFL: Error Statistics:
----------------------------
    Module:  5
----------------------------

------------------------------------------------------------------
Date (mm/dd/yy)=11/09/05  Time (hs:mn:sec): 12:10:05
Baby Ceaser data

------------------------------------------------------------------
Date (mm/dd/yy)=11/09/05  Time (hs:mn:sec): 12:10:05
Arbiter Bellagio2 data
GROUP:4
bkt_tx_perr_drop_cnt           0
bkr_rx_req_fifo_drop_cnt       0
bkr_rx_req_fifo_perr_drop_cnt  0
bkr_rx_di_lut_perr_drop_cnt    0
fil_drop_cnt                   0
crm_gid_drop_cnt               0
ser_rxs_perr_cnt               0
top_ddr_rx_perr_cnt            0
Bucket Counters
 Bkt Cos  Gresend            Grant          Request  Rresend
-------------------------------------------------------------
   0   0        0                0                0        0
   0   1        0                0                0        0
   0   2        0                0                0        0
   0   3        0             1127             1127        0
  64   0        0                0                0        0
  64   1        0                0                0        0
  64   2        0                0                0        0
  64   3        0                0                0        0
```

```
 128   0         0                 0                 0         0
 128   1         0                 0                 0         0
 128   2         0                 0                 0         0
 128   3         0                 0                 0         0
 192   0         0                 0                 0         0
 192   1         0                 0                 0         0
 192   2         0                 0                 0         0
 192   3         0                73                73         0
 256   0         0                 0                 0         0
 256   1         0                 0                 0         0
 256   2         0                 0                 0         0
 256   3         0                 0                 0         0
 320   0         0                 0                 0         0
 320   1         0                 0                 0         0
 320   2         0                 0                 0         0
 320   3         0                 0                 0         0
 384   0         0                 0                 0         0
 384   1         0                 0                 0         0
 384   2         0                 0                 0         0
 384   3         0                 0                 0         0
 448   0         0                 0                 0         0
 448   1         0                 0                 0         0
 448   2         0                 0                 0         0
 448   3         0                 0                 0         0
 512   0         0                 0                 0         0
 512   1         0                 0                 0         0
 512   2         0                 0                 0         0
 512   3         0                 0                 0         0
 576   0         0                 0                 0         0
 576   1         0                 0                 0         0
 576   2         0                 0                 0         0
 576   3         0                 0                 0         0
 640   0         0                 0                 0         0
 640   1         0                 0                 0         0
 640   2         0                 0                 0         0
 640   3         0                 0                 0         0
 704   0         0                 0                 0         0
 704   1         0                 0                 0         0
 704   2         0                 0                 0         0
 704   3         0                 0                 0         0
 768   0         0                 0                 0         0
 768   1         0                 0                 0         0
 768   2         0                 0                 0         0
 768   3         0                 0                 0         0
 832   0         0                 0                 0         0
 832   1         0                 0                 0         0
 832   2         0                 0                 0         0
 832   3         0                 0                 0         0
 896   0         0                 0                 0         0
 896   1         0                 0                 0         0
 896   2         0                 0                 0         0
 896   3         0                 0                 0         0
 960   0         0                 0                 0         0
 960   1         0                 0                 0         0
 960   2         0                 0                 0         0
 960   3         0                 0                 0         0
LDI Counters
LDI COS  OUT_REQ   CREDIT CREDITNA
-----------------------------------
  0   0         0    14164        63
  0   1         0    41874        63
  0   2         0    41874        63
  0   3         0    41905        63
  1   0         0    14164        63
```

```
 1   1         0    41874       63
 1   2         0    41874       63
 1   3         0    41904       63
 2   0         0    14164       63
 2   1         0    41874       63
 2   2         0    41874       63
 2   3         0    41902       63
 3   0         0    14164       63
 3   1         0    41874       63
 3   2         0    41874       63
 3   3         0    41903       63
 4   0         0    14164       63
 4   1         0    41873       63
 4   2         0    41873       63
 4   3         0    41903       63
 5   0         0    14164       63
 5   1         0    41873       63
 5   2         0    41873       63
 5   3         0    41903       63
 6   0         0    14164       63
 6   1         0    41872       63
 6   2         0    41872       63
 6   3         0    41903       63
 7   0         0    14164       63
 7   1         0    41872       63
 7   2         0    41872       63
 7   3         0    41903       63
 8   0         0    14163       63
 8   1         0    41871       63
 8   2         0    41871       63
 8   3         0    41902       63
 9   0         0    14163       63
 9   1         0    41871       63
 9   2         0    41871       63
 9   3         0    41902       63
10   0         0    14163       63
10   1         0    41871       63
10   2         0    41871       63
10   3         0    41901       63
11   0         0    14163       63
11   1         0    41871       63
11   2         0    41871       63
11   3         0    41901       63
12   0         0    14163       63
12   1         0    41870       63
12   2         0    41870       63
12   3         0    41901       63
13   0         0    14163       63
13   1         0    41870       63
13   2         0    41870       63
13   3         0    41900       63
14   0         0    14163       63
14   1         0    41869       63
14   2         0    41869       63
14   3         0    41900       63
15   0         0    14163       63
15   1         0    41869       63
15   2         0    41869       63
15   3         0    41900       63
16   0         0    14163       63
16   1         0    41869       63
16   2         0    41869       63
16   3         0    41900       63
17   0         0    14162       63
```

```
17   1         0     41868        63
17   2         0     41868        63
17   3         0     41899        63
18   0         0     14162        63
18   1         0     41868        63
18   2         0     41868        63
18   3         0     41898        63
19   0         0     14162        63
19   1         0     41868        63
19   2         0     41868        63
19   3         0     41898        63
20   0         0     14162        63
20   1         0     41868        63
20   2         0     41868        63
20   3         0     41898        63
21   0         0     14162        63
21   1         0     41867        63
21   2         0     41867        63
21   3         0     41898        63
22   0         0     14162        63
22   1         0     41867        63
22   2         0     41867        63
22   3         0     41897        63
23   0         0     14162        63
23   1         0     41866        63
23   2         0     41866        63
23   3         0     41897        63
24   0         0         0         0
24   1         0         0         0
24   2         0         0         0
24   3         0         0         0
25   0         0         0         0
25   1         0         0         0
25   2         0         0         0
25   3         0         0         0
26   0         0         0         0
26   1         0         0         0
26   2         0         0         0
26   3         0         0         0
27   0         0         0         0
27   1         0         0         0
27   2         0         0         0
27   3         0         0         0
28   0         0         0         0
28   1         0         0         0
28   2         0         0         0
28   3         0         0         0
29   0         0         0         0
29   1         0         0         0
29   2         0         0         0
29   3         0         0         0
30   0         0         0         0
30   1         0         0         0
30   2         0         0         0
30   3         0         0         0
31   0         0         0         0
31   1         0         0         0
31   2         0         0         0
31   3         0         0         0
32   0         0         0         0
32   1         0         0         0
32   2         0         0         0
32   3         0         0         0
33   0         0         0         0
```

```
33   1          0          0          0
33   2          0          0          0
33   3          0          0          0
34   0          0          0          0
34   1          0          0          0
34   2          0          0          0
34   3          0          0          0
35   0          0          0          0
35   1          0          0          0
35   2          0          0          0
35   3          0          0          0
36   0          0          0          0
36   1          0          0          0
36   2          0          0          0
36   3          0          0          0
37   0          0          0          0
37   1          0          0          0
37   2          0          0          0
37   3          0          0          0
38   0          0          0          0
38   1          0          0          0
38   2          0          0          0
38   3          0          0          0
39   0          0          0          0
39   1          0          0          0
39   2          0          0          0
39   3          0          0          0
40   0          0          0          0
40   1          0          0          0
40   2          0          0          0
40   3          0          0          0
41   0          0          0          0
41   1          0          0          0
41   2          0          0          0
41   3          0          0          0
42   0          0          0          0
42   1          0          0          0
42   2          0          0          0
42   3          0          0          0
43   0          0          0          0
43   1          0          0          0
43   2          0          0          0
43   3          0          0          0
44   0          0          0          0
44   1          0          0          0
44   2          0          0          0
44   3          0          0          0
45   0          0          0          0
45   1          0          0          0
45   2          0          0          0
45   3          0          0          0
46   0          0          0          0
46   1          0          0          0
46   2          0          0          0
46   3          0          0          0
47   0          0          0          0
47   1          0          0          0
47   2          0          0          0
47   3          0          0          0
48   0          0          0          0
48   1          0          0          0
48   2          0          0          0
48   3          0          0          0
49   0          0          0          0
```

```
 49   1         0         0         0
 49   2         0         0         0
 49   3         0         0         0
 50   0         0         0         0
 50   1         0         0         0
 50   2         0         0         0
 50   3         0         0         0
 51   0         0         0         0
 51   1         0         0         0
 51   2         0         0         0
 51   3         0         0         0
 52   0         0         0         0
 52   1         0         0         0
 52   2         0         0         0
 52   3         0         0         0
 53   0         0         0         0
 53   1         0         0         0
 53   2         0         0         0
 53   3         0         0         0
 54   0         0         0         0
 54   1         0         0         0
 54   2         0         0         0
 54   3         0         0         0
 55   0         0         0         0
 55   1         0         0         0
 55   2         0         0         0
 55   3         0         0         0
 56   0         0         0         0
 56   1         0         0         0
 56   2         0         0         0
 56   3         0         0         0
 57   0         0         0         0
 57   1         0         0         0
 57   2         0         0         0
 57   3         0         0         0
 58   0         0         0         0
 58   1         0         0         0
 58   2         0         0         0
 58   3         0         0         0
 59   0         0         0         0
 59   1         0         0         0
 59   2         0         0         0
 59   3         0         0         0
 60   0         0         0         0
 60   1         0         0         0
 60   2         0         0         0
 60   3         0         0         0
 61   0         0         0         0
 61   1         0         0         0
 61   2         0         0         0
 61   3         0         0         0
 62   0         0         0         0
 62   1         0         0         0
 62   2         0         0         0
 62   3         0         0         0
 63   0         0         0         0
 63   1         0         0         0
 63   2         0         0         0
 63   3         0         0         0

----------------------------------------------------------------
Date (mm/dd/yy)=11/09/05  Time (hs:mn:sec): 12:10:05
Arbiter Bellagio2 data
GROUP:10
```

```
bkt_tx_perr_drop_cnt           0
bkr_rx_req_fifo_drop_cnt       0
bkr_rx_req_fifo_perr_drop_cnt  0
bkr_rx_di_lut_perr_drop_cnt    0
fil_drop_cnt                   0
crm_gid_drop_cnt               0
ser_rxs_perr_cnt               0
top_ddr_rx_perr_cnt            0
Bucket Counters
 Bkt Cos  Gresend            Grant          Request  Rresend
-------------------------------------------------------------
   0   0        0                0                0        0
   0   1        0                0                0        0
   0   2        0                0                0        0
   0   3        0               73               73        0
  64   0        0                0                0        0
  64   1        0                0                0        0
  64   2        0                0                0        0
  64   3        0                0                0        0
 128   0        0                0                0        0
 128   1        0                0                0        0
 128   2        0                0                0        0
 128   3        0                0                0        0
 192   0        0                0                0        0
 192   1        0                0                0        0
 192   2        0                0                0        0
 192   3        0               59               59        0
 256   0        0                0                0        0
 256   1        0                0                0        0
 256   2        0                0                0        0
 256   3        0                0                0        0
 320   0        0                0                0        0
 320   1        0                0                0        0
 320   2        0                0                0        0
 320   3        0                0                0        0
 384   0        0                0                0        0
 384   1        0                0                0        0
 384   2        0                0                0        0
 384   3        0                0                0        0
 448   0        0                0                0        0
 448   1        0                0                0        0
 448   2        0                0                0        0
 448   3        0                0                0        0
 512   0        0                0                0        0
 512   1        0                0                0        0
 512   2        0                0                0        0
 512   3        0                0                0        0
 576   0        0                0                0        0
 576   1        0                0                0        0
 576   2        0                0                0        0
 576   3        0                0                0        0
 640   0        0                0                0        0
 640   1        0                0                0        0
 640   2        0                0                0        0
 640   3        0                0                0        0
 704   0        0                0                0        0
 704   1        0                0                0        0
 704   2        0                0                0        0
 704   3        0                0                0        0
 768   0        0                0                0        0
 768   1        0                0                0        0
 768   2        0                0                0        0
 768   3        0                0                0        0
 832   0        0                0                0        0
```

```
 832   1         0                0                0         0
 832   2         0                0                0         0
 832   3         0                0                0         0
 896   0         0                0                0         0
 896   1         0                0                0         0
 896   2         0                0                0         0
 896   3         0                0                0         0
 960   0         0                0                0         0
 960   1         0                0                0         0
 960   2         0                0                0         0
 960   3         0                0                0         0
LDI Counters
LDI COS  OUT_REQ   CREDIT CREDITNA
-----------------------------------
  0   0         0     9471        63
  0   1         0        0         0
  0   2         0        0         0
  0   3         0     9548        63
  1   0         0     9471        63
  1   1         0        0         0
  1   2         0        0         0
  1   3         0     9487        63
  2   0         0        0         0
  2   1         0        0         0
  2   2         0        0         0
  2   3         0        0         0
  3   0         0        0         0
  3   1         0        0         0
  3   2         0        0         0
  3   3         0        0         0
  4   0         0        0         0
  4   1         0        0         0
  4   2         0        0         0
  4   3         0        0         0
  5   0         0        0         0
  5   1         0        0         0
  5   2         0        0         0
  5   3         0        0         0
  6   0         0        0         0
  6   1         0        0         0
  6   2         0        0         0
  6   3         0        0         0
  7   0         0        0         0
  7   1         0        0         0
  7   2         0        0         0
  7   3         0        0         0
  8   0         0        0         0
  8   1         0        0         0
  8   2         0        0         0
  8   3         0        0         0
  9   0         0        0         0
  9   1         0        0         0
  9   2         0        0         0
  9   3         0        0         0
 10   0         0        0         0
 10   1         0        0         0
 10   2         0        0         0
 10   3         0        0         0
 11   0         0        0         0
 11   1         0        0         0
 11   2         0        0         0
 11   3         0        0         0
 12   0         0        0         0
 12   1         0        0         0
```

```
12   2          0          0          0
12   3          0          0          0
13   0          0          0          0
13   1          0          0          0
13   2          0          0          0
13   3          0          0          0
14   0          0          0          0
14   1          0          0          0
14   2          0          0          0
14   3          0          0          0
15   0          0          0          0
15   1          0          0          0
15   2          0          0          0
15   3          0          0          0
16   0          0          0          0
16   1          0          0          0
16   2          0          0          0
16   3          0          0          0
17   0          0          0          0
17   1          0          0          0
17   2          0          0          0
17   3          0          0          0
18   0          0          0          0
18   1          0          0          0
18   2          0          0          0
18   3          0          0          0
19   0          0          0          0
19   1          0          0          0
19   2          0          0          0
19   3          0          0          0
20   0          0          0          0
20   1          0          0          0
20   2          0          0          0
20   3          0          0          0
21   0          0          0          0
21   1          0          0          0
21   2          0          0          0
21   3          0          0          0
22   0          0          0          0
22   1          0          0          0
22   2          0          0          0
22   3          0          0          0
23   0          0          0          0
23   1          0          0          0
23   2          0          0          0
23   3          0          0          0
24   0          0          0          0
24   1          0          0          0
24   2          0          0          0
24   3          0          0          0
25   0          0          0          0
25   1          0          0          0
25   2          0          0          0
25   3          0          0          0
26   0          0          0          0
26   1          0          0          0
26   2          0          0          0
26   3          0          0          0
27   0          0          0          0
27   1          0          0          0
27   2          0          0          0
27   3          0          0          0
28   0          0          0          0
28   1          0          0          0
```

```
28    2          0          0          0
28    3          0          0          0
29    0          0          0          0
29    1          0          0          0
29    2          0          0          0
29    3          0          0          0
30    0          0          0          0
30    1          0          0          0
30    2          0          0          0
30    3          0          0          0
31    0          0          0          0
31    1          0          0          0
31    2          0          0          0
31    3          0          0          0
32    0          0          0          0
32    1          0          0          0
32    2          0          0          0
32    3          0          0          0
33    0          0          0          0
33    1          0          0          0
33    2          0          0          0
33    3          0          0          0
34    0          0          0          0
34    1          0          0          0
34    2          0          0          0
34    3          0          0          0
35    0          0          0          0
35    1          0          0          0
35    2          0          0          0
35    3          0          0          0
36    0          0          0          0
36    1          0          0          0
36    2          0          0          0
36    3          0          0          0
37    0          0          0          0
37    1          0          0          0
37    2          0          0          0
37    3          0          0          0
38    0          0          0          0
38    1          0          0          0
38    2          0          0          0
38    3          0          0          0
39    0          0          0          0
39    1          0          0          0
39    2          0          0          0
39    3          0          0          0
40    0          0          0          0
40    1          0          0          0
40    2          0          0          0
40    3          0          0          0
41    0          0          0          0
41    1          0          0          0
41    2          0          0          0
41    3          0          0          0
42    0          0          0          0
42    1          0          0          0
42    2          0          0          0
42    3          0          0          0
43    0          0          0          0
43    1          0          0          0
43    2          0          0          0
43    3          0          0          0
44    0          0          0          0
44    1          0          0          0
```

```
44   2          0          0          0
44   3          0          0          0
45   0          0          0          0
45   1          0          0          0
45   2          0          0          0
45   3          0          0          0
46   0          0          0          0
46   1          0          0          0
46   2          0          0          0
46   3          0          0          0
47   0          0          0          0
47   1          0          0          0
47   2          0          0          0
47   3          0          0          0
48   0          0          0          0
48   1          0          0          0
48   2          0          0          0
48   3          0          0          0
49   0          0          0          0
49   1          0          0          0
49   2          0          0          0
49   3          0          0          0
50   0          0          0          0
50   1          0          0          0
50   2          0          0          0
50   3          0          0          0
51   0          0          0          0
51   1          0          0          0
51   2          0          0          0
51   3          0          0          0
52   0          0          0          0
52   1          0          0          0
52   2          0          0          0
52   3          0          0          0
53   0          0          0          0
53   1          0          0          0
53   2          0          0          0
53   3          0          0          0
54   0          0          0          0
54   1          0          0          0
54   2          0          0          0
54   3          0          0          0
55   0          0          0          0
55   1          0          0          0
55   2          0          0          0
55   3          0          0          0
56   0          0          0          0
56   1          0          0          0
56   2          0          0          0
56   3          0          0          0
57   0          0          0          0
57   1          0          0          0
57   2          0          0          0
57   3          0          0          0
58   0          0          0          0
58   1          0          0          0
58   2          0          0          0
58   3          0          0          0
59   0          0          0          0
59   1          0          0          0
59   2          0          0          0
59   3          0          0          0
60   0          0          0          0
60   1          0          0          0
```

```
 60   2         0         0         0
 60   3         0         0         0
 61   0         0         0         0
 61   1         0         0         0
 61   2         0         0         0
 61   3         0         0         0
 62   0         0         0         0
 62   1         0         0         0
 62   2         0         0         0
 62   3         0         0         0
 63   0         0         0         0
 63   1         0         0         0
 63   2         0         0         0
 63   3         0         0         0

OBFL: System Bootup Record:
----------------------------
    Module:  5
----------------------------


OBFL: Device Versions in Switch:
----------------------------
    Module:  5
----------------------------


OBFL: Exception Log:
----------------------------
    Module:  5
----------------------------


OBFL: Register Log:
----------------------------
    Module:  5
----------------------------
register-log: This option not supported on SUP.


OBFL: Miscellaneous Error Logs:
----------------------------
    Module:  5
----------------------------.
```

Related Commands

Command	Description
logging	Configures logging parameters.

show logging onboard flow-control request-timeout

To display the Onboard Failure Logging (OBFL) request timeout for a source-destination pair per module with the timestamp information, use the **show logging onboard flow-control request-timeout** command.

show logging onboard flow-control request-timeout

Command Default

Displays the OBFL request timeout for a source-destination pair, per module, with the timestamp information.

Command Modes

EXEC mode.

Command History

Release	Modification
5.0(1a)	This command was introduced.

Examples

This example shows how to display the request timeout for a source-destination pair per module with the timestamp information for the supervisor CLI:

```
switch# show logging onboard flow-control request-timeout
----------------------------
    Module:  1
----------------------------
----------------------------
    Module:  2
----------------------------
-------------------------------------------------------------------------------------
|  Dest  |   Source   |Events|      Timestamp         |       Timestamp        |
|  Intf  |    Intf    | Count|       Earliest         |         Latest         |
-------------------------------------------------------------------------------------
|sup-fc0 |fc2/48,     |    24|Wed Oct 31 14:31:35 2012|Wed Oct 31 14:31:36 2012|
-------------------------------------------------------------------------------------
|sup-fc0 |fc2/9,      |  7158|Mon Feb  7 10:49:20 2011|Mon Feb  7 10:52:59 2011|
|        |fc2/23,     |      |                        |                        |
|        |fc2/24,     |      |                        |                        |
-------------------------------------------------------------------------------------
|sup-fc0 |fc2/9,      |  7907|Mon Feb  7 10:45:17 2011|Mon Feb  7 10:49:20 2011|
|        |fc2/23,     |      |                        |                        |
-------------------------------------------------------------------------------------
|sup-fc0 |fc2/23,     |     2|Mon Feb  7 10:45:17 2011|Mon Feb  7 10:45:17 2011|
-------------------------------------------------------------------------------------
```

Related Commands

Command	Description
logging	Configures logging parameters.

show mcast

To display multicast information, use the **show mcast** command.

show mcast [**vsan vsan-id**]

Syntax Description

vsan *vsan-id*	(Optional) Specifies the number of the VSAN. The range is 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays multicast information:

```
switch# show mcast

Multicast root for VSAN 1
        Configured root mode : Principal switch
        Operational root mode : Principal switch
        Root Domain ID : 0x15(21)
Multicast root for VSAN 73
        Configured root mode : Principal switch
        Operational root mode : Principal switch
        Root Domain ID : 0x65(101)
Multicast root for VSAN 99
        Configured root mode : Principal switch
        Operational root mode : Principal switch
        Root Domain ID : 0xe4(228)
Multicast root for VSAN 4001
        Configured root mode : Principal switch
        Operational root mode : Principal switch
        Root Domain ID : 0xe9(233)
Multicast root for VSAN 4002
        Configured root mode : Principal switch
        Operational root mode : Principal switch
        Root Domain ID : 0x78(120)
Multicast root for VSAN 4003
        Configured root mode : Principal switch
        Operational root mode : Principal switch
        Root Domain ID : 0xe0(224)
Multicast root for VSAN 4004
        Configured root mode : Principal switch
        Operational root mode : Lowest domain switch
        Root Domain ID : 0x01(1)
```

Related Commands

Command	Description
mcast root	Configures the multicast root VSAN.

show module

To display the module information including the online diagnostic test status, use the show module command.

show module

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the module information including the online diagnostic test status:

```
switch# show module
Mod  Ports  Module-Type                         Model              Status
---  -----  ---------------------------------- ------------------ ----------
1    48     2/4/8/10/16 Gbps Advanced FC Module DS-X9448-768K9     ok
5    0      Supervisor module-3                DS-X9700-SF3-K9    ha-standby
6    0      Supervisor module-3                DS-X9700-SF3-K9    active *
9    48     2/4/8/10/16 Gbps Advanced FC Module DS-X9448-768K9     powered-dn
Mod  Power-Status  Reason
---  ------------  --------------------------
9    powered-dn     Configured Power down
Mod  Sw              Hw
---  --------------  ------
1    6.2(1X)         0.301
5    6.2(1X)         0.103
6    6.2(1X)         0.103
Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    54-7f-ee-d7-bc-2c to 54-7f-ee-d7-bc-2f  JAE164302NU
5    d8-67-d9-0a-86-1d to d8-67-d9-0a-86-2f  JAF1629AMQA
6    d8-67-d9-0a-86-0a to d8-67-d9-0a-86-1c  JAF1629AMQF
9    00-00-00-00-00-00 to 00-00-00-00-00-00  JAE164302O4
Mod  Online Diag Status
---  ------------------
1    Pass
switch#
```

Related Commands

Commands	Description
debug sme	Debugs Cisco SME features.

show module

To verify the status of a module, use the **show module** command.

show module [{**slot** [**recovery-steps**]|**diag**|**uptime**|**xbar** **number**}]

Syntax Description

slot	(Optional) Specifies the slot number for the module.
recovery-steps	(Optional) Displays information about modules and the steps to recover a module.
diag	(Optional) Displays module-related information.
uptime	(Optional) Displays the length of time that the modules have been functional in the switch.
xbar *number*	(Optional) Displays information about the specified crossbar, either 1 or 2.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.
3.0(1)	Added the **recovery-steps and xbar** options.
NX-OS 4.1(1b)	Added the command output for a module resource on a 24-port line card with all ports in shared mode.
NX-OS 4.1(1b)	Added the command output for a module resource on a 24-port line card with few ports in shared mode and few port in dedicated mode.
NX-OS 4.1(1b)	Added the command output for a module resource on a 12-port line card with all ports in dedicated mode.
NX-OS 4.1(1b)	Added the command output for a module resource on a 12-port line card with all ports in dedicated mode and extended feature enabled.
NX-OS 4.1(1b)	Added the command output for show module xbar.

Usage Guidelines

If your chassis has more than one switching module, you will see the progress check if you enter the show module command several times and view the status column each time.

The switching module goes through a testing and an initializing stage before displaying an ok status.

Use the **uptime** option to display the time that a specified supervisor module, switching module, or services module is functional in the switch. This time is computed from the time a module goes online after a disruptive upgrade or reset.

You can use the **recovery-steps** option only for modules that are powered down because of problems with index allocation.

Before using the **recovery-steps** option, make sure that **debug module no-power-down** is not on.

Note You cannot use the **recovery-steps** option to recover a Supervisor module. Also, the Cisco MDS 9124 switch does not support the **recovery-steps** option.

For additional information about port indices, refer to the *Cisco MDS 9000 Family CLI Configuration Guide* and to the *Cisco MDS 9000 Family Troubleshooting Guide* .

Examples

The following example displays information about the modules on the switch:

```
switch# show module
Mod  Ports  Module-Type                       Model              Status
---  -----  -------------------------------- ------------------ ------------
2    32     Advanced Services Module         DS-X9032-SMV       powered-dn
4    32     Advanced Services Module         DS-X9032-SMV       powered-dn
5    0      Supervisor/Fabric-1              DS-X9530-SF1-K9    active *
6    0      Supervisor/Fabric-1              DS-X9530-SF1-K9    ha-standby
8    32     1/2 Gbps FC Module               DS-X9032           ok
Mod  Sw           Hw      World-Wide-Name(s) (WWN)
---  -----------  ------  --------------------------------------------------
5    1.2(2)       0.610   --
6    1.2(2)       0.610   --
8    1.2(2)       0.3     21:c1:00:0b:46:79:f1:40 to 21:e0:00:0b:46:79:f1:40
Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
5    00-d0-97-38-b4-01 to 00-d0-97-38-b4-05  JAB06350B0H
6    00-d0-97-38-b3-f9 to 00-d0-97-38-b3-fd  JAB06350B1R
8    00-05-30-00-2b-e2 to 00-05-30-00-2b-e6  jab062407x4
* this terminal session
```

The following example shows how to module resources on a 24-port line card with all ports in shared mode:

```
switch# show module 1 resources
                          BB_Credit   Bandwidth   Rate
                                      (Gbps)      Mode
------------------------------------------------------------------------------
Available Dedicated Buffers    5336
Port-Group 0
Total Bandwidth                       12
Allocated Dedicated Bandwidth         0
Shared Bandwidth in Use               12
      fc1/1                   16      4           shared
      fc1/2                   16      4           shared
      fc1/3                   16      4           shared
      fc1/4                   16      4           shared
      fc1/5                   16      4           shared
      fc1/6                   16      4           shared
```

The following example shows how to module resources on a 24-port line card with a few ports in shared mode and a few ports in dedicated mode:

```
switch# show module 1 resources
                          BB_Credit   Bandwidth   Rate
                                      (Gbps)      Mode
------------------------------------------------------------------------------
Available Dedicated Buffers    1776
```

```
Port-Group 0
Total Bandwidth                         12
Allocated Dedicated bandwidth           8
Shared Bandwidth in Use                 4
      fc1/1                   250       1             dedicated
      fc1/2                   16        4             shared
      fc1/3                   250       1             dedicated
      fc1/4                   250       2             dedicated
      fc1/5                   16        4             shared
      fc1/6                   250       4             dedicated
```

The following example shows how to module resources on a 12-port line card with all ports in dedicated mode:

```
switch# show module 1 resources
                          BB_Credit   Bandwidth   Rate
                                      (Gbps)      Mode
------------------------------------------------------------------------------
Available Dedicated Buffers    3000
Port-Group 0
Total Bandwidth                         12
Allocated Dedicated bandwidth           11
Shared Bandwidth in Use                 0

      fc1/1                   250       4             dedicated
      fc1/2                   250       1             dedicated
      fc1/3                   250       2             dedicated
      fc1/4                   250       1             dedicated
      fc1/5                   250       2             dedicated
      fc1/6                   250       1             dedicated
```

The following example shows module resources on a 12-port line card with all ports in dedicated mode and extended feature enabled:

```
switch# show module 1 resources
                          BB_Credit   Bandwidth   Rate
                                      (Gbps)      Mode
------------------------------------------------------------------------------
Available Dedicated Buffers    2700
Port-Group 0
Total Bandwidth                         12
Allocated Dedicated bandwidth           11
Shared Bandwidth in Use                 0
      fc1/1                   100       1             dedicated
      fc1/2                   250       1             dedicated
      fc1/3                   250       2             dedicated
      fc1/4                   150       1             dedicated
      fc1/5                   300       2             dedicated
      fc1/6                   600       4             dedicated
```

The following example displays diagnostic information about the modules on the switch:

```
switch# show module diag
Diag status for module 2 (. = PASS, F = FAIL, N = N/A)
CPU           .
SPROM         .
ASICS         .
Diag status for module 4 (. = PASS, F = FAIL, N = N/A)
CPU           .
SPROM         .
ASICS         .
```

The following example displays uptime information about the modules on the switch:

```
switch#  show module uptime
------ Module 1 -----
Module Start Time:   Wed Apr 14 18:12:48 2004
Up Time:             16 days, 5 hours, 59 minutes, 41 seconds
------ Module 6 -----
Module Start Time:   Wed Apr 14 18:11:57 2004
Up Time:             16 days, 6 hours, 0 minutes, 32 second
```

The following example displays information about the crossbar:

```
switch# show module xbar
Xbar Ports  Module-Type                       Model              Status
---  -----  -------------------------------- ------------------ ------------
1    0      Fabric Module 1                  DS-13SLT-FAB1      ok
2    0      Fabric Module 2                  DS-13SLT-FAB2      ok

Xbar Sw              Hw      World-Wide-Name(s) (WWN)
---  --------------  ------  --------------------------------------------------
1    NA              0.0     --
2    NA              0.111   --

Xbar MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    NA                                      JAF1207ARRS
2    NA                                      JAE1212BPR0

* this terminal session
```

The following example uses the **show module**, **show port index-allocation**, and **show module recovery-steps** commands to display a Generation 1 module that is powered down due to a lack of indices:

```
switch# show module
Mod  Ports  Module-Type                       Model          Status
---  -----  -------------------------------- ------------------ --
1    48     1/2/4 Gbps FC Module             DS-X9148           ok
2    48     1/2/4 Gbps FC Module             DS-X9148           ok
3    48     1/2/4 Gbps FC Module             DS-X9148           ok
4    48     1/2/4 Gbps FC Module             DS-X9148           ok
6    0      Supervisor/Fabric-1              DS-X9530-SF1-K9    active *
7    48     1/2/4 Gbps FC Module             DS-X9148           ok
9    16     1/2 Gbps FC Module               DS-X9016   powered-dn
Mod  Power-Status  Power Down Reason
---  ------------  --------------------------
9    powered-dn    Insufficient resources (dest Index)
switch# show port index-allocation
Module index distribution:
-----------------------------------------------------+
Slot | Allowed |      Alloted indices info            |
     |  range* | Total |          Index values        |
-----|---------|-------|------------------------------|
 1   |   0-  31|   48  | 160-187,192-207,220-223      | (Slot 2 shares 28-31)
     |         |       |(Slot 3 shares 16-27) (Slot 7 shares 0-15)|
 2   |  32-  63|   48  | 28-63,240-251                |
 3   |  64-  95|   48  | 16-27,64-95,188-191          |
 4   |  96- 127|   48  | 96-127,224-239               |
 7   | 128- 159|   48  | 0-15,128-159                 |
 8   | 160- 191|   -   | (None)                       | (Slot 1 shares 160-187
     |         |       |) (Slot 3 shares 188-191)     |
 9   | 192- 223|   -   | (None)                       | (Slot 1 shares 192-207
```

```
     |         |       |,220-223)                    |
SUP  | 253-255 |   3   | 253-255                     |
*Allowed range applicable only for Generation-1 modules
switch# show module 9 recovery-steps
Failure Reason:
Insufficient indices in range 0-255. Module cannot be powered up
```

The following example uses the show port index-allocation command on the Cisco MDS 9124 switch:

```
switch# show port index-allocation
Module index distribution:
-------------------------------------------------------+
Slot | Allowed |      Allotted indices info            |
     |  range* | Total |          Index values         |
-----|---------|-------|-------------------------------|
 1   |   0- 255|   24  | 0-23                          |
SUP  |  -----  |   -   | (None)                        |
*Allowed range applicable only for Generation-1 modules
```

The following example uses the **show module**, **show port index-allocation**, and **show module recovery-steps** commands to display a Generation 1 module that is powered down because indices are not available in its slot. Specifically, indices 28 through 31 are taken by a 48-port card in slot 2:

```
switch# show module
Mod  Ports  Module-Type                       Model
Status
---  -----  -------------------------------- ------------------ --
1    32     1/2 Gbps FC Module                           powered-dn
2    48     1/2/4 Gbps FC Module             DS-X9148           ok
4    48     1/2/4 Gbps FC Module             DS-X9148           ok
6    0      Supervisor/Fabric-1              DS-X9530-SF1-K9    active *
Mod  Power-Status  Power Down Reason
---  ------------  --------------------------
1    powered-dn    Insufficient resources (dest Index)
switch# show port index-allocation
Module index distribution:
-------------------------------------------------------+
Slot | Allowed |      Alloted indices info             |
     |  range* | Total |          Index values         |
-----|---------|-------|-------------------------------|
 1   |   0-  31|   -   | (None)                        | (Slot 2 shares 28-31)
 2   |  32-  63|   48  | 28-63,240-251                 |
 3   |  64-  95|   -   | (None)                        |
 4   |  96- 127|   48  | 96-127,224-239                |
 7   | 128- 159|   -   | (None)                        |
 8   | 160- 191|   -   | (None)                        |
 9   | 192- 223|   -   | (None)                        |
SUP  | 253-255 |   3   | 253-255                       |
*Allowed range applicable only for Generation-1 modules
switch# show module 1 recovery-steps
Failure Reason:
Indices in allowed range 0 - 31 unavailable
Check "show port index-allocation" for more details
Recovery Steps:
Insert failed module in any one of the slots: 3, 7, 8, 9
```

The following example uses the **show module**, **show port index-allocation**, and **show module recovery-steps** commands to display a Generation 1 module that is powered down because of a lack of indices between 0 and 255.

```
switch# show module
```

```
Mod  Ports  Module-Type                       Model          Status
---  -----  -------------------------------- ------------------ ------------
1    48     1/2/4 Gbps FC Module             DS-X9148           ok
2    48     1/2/4 Gbps FC Module             DS-X9148           ok
3    48     1/2/4 Gbps FC Module             DS-X9148           ok
4    48     1/2/4 Gbps FC Module             DS-X9148           ok
5    0      Supervisor/Fabric-2              DS-X9530-SF2-K9    active *
6    0      Supervisor/Fabric-2              DS-X9530-SF2-K9    ha-standby
7    48     1/2/4 Gbps FC Module             DS-X9148           ok
8    24     1/2/4 Gbps FC Module             DS-X9124           ok
9    32     1/2 Gbps FC Module                                  powered-dn
Mod  Power-Status  Power Down Reason
---  ------------  --------------------------
9    powered-dn    Insufficient resources (dest Index)
switch# show port index-allocation
Module index distribution:
-------------------------------------------------------+
Slot | Allowed |      Alloted indices info            |
     |  range  | Total |          Index values        |
-----|---------|-------|------------------------------|
 1   |   0-1023|   48  | 160-207                      |
 2   |   0-1023|   48  | 3-50                         |
 3   |   0-1023|   48  | 0-2,208-252                  |
 4   |   0-1023|   48  | 51-98                        |
 7   |   0-1023|   48  | 99-146                       |
 8   |   0-1023|   24  | 147-159,256-266              |
 9   |  -----  |   -   | (None)                       |
SUP  | 253-255 |   3   | 253-255                      |
switch# show module 9 recovery-steps
Failure Reason:
Insufficient indices in range 0-255. Module cannot be powered up
```

The following example uses the **show module**, **show port index-allocation**, and **show module recovery-steps** commands to display a Generation 1 module that is powered down due to non-availability of contiguous indices.

```
switch# show module
Mod  Ports  Module-Type                       Model          Status
---  -----  -------------------------------- ------------------ --
1    48     1/2/4 Gbps FC Module                                powered-dn
3    12     1/2/4 Gbps FC Module             DS-X9112           ok
4    8      IP Storage Services Module                          powered-dn
5    48     1/2/4 Gbps FC Module             DS-X9148           ok
6    48     1/2/4 Gbps FC Module             DS-X9148           ok
7    0      Supervisor/Fabric-2              DS-X9530-SF2-K9    active *
8    0      Supervisor/Fabric-2              DS-X9530-SF2-K9    ha-standby
9    24     1/2/4 Gbps FC Module             DS-X9124           ok
11   4      10 Gbps FC Module                DS-X9704           ok
12   48     1/2/4 Gbps FC Module             DS-X9148           ok
13   16     1/2 Gbps FC Module               DS-X9016           ok

Mod  Power-Status  Power Down Reason
---  ------------  --------------------------
1    powered-dn    Config down
4    powered-dn    Insufficient resources (dest Index)

Mod  Sw           Hw      World-Wide-Name(s) (WWN)
---  -----------  ------  --------------------------------------------------
3    3.0(0.322)   0.222   20:81:00:05:30:01:9c:02 to 20:8c:00:05:30:01:9c:02
switch# show port index-allocation

Module index distribution:
-------------------------------------------------------+
```

```
Slot | Allowed |      Alloted indices info            |
     |  range  | Total |          Index values        |
-----|---------|-------|------------------------------|
 1   |  -----  |   -   | (None)                       |
 2   |  -----  |   -   | (None)                       |
 3   |   0- 255|   12  | 219-230                      |
 4   |  -----  |   -   | (None)                       |
 5   |   0- 255|   48  | 0-13,74-79,96-123            |
 6   |   0- 255|   48  | 124-150,232-252              |
 9   |   0- 255|   24  | 154-177                      |
10   |  -----  |   -   | (None)                       |
11   |   0- 255|    4  | 151-153,231                  |
12   |   0- 255|   48  | 32-73,178-183                |
13   |   0- 255|   16  | 80-95                        |
SUP  | 253-255 |   3   | 253-255                      |
switch# show module 4 recovery-steps
Failure Reason:
Contiguous and aligned indices unavailable for Generation-1 modules
Check "show port index-allocation" for more details
Please follow the steps below:
1. Power-off module in one of the following slots: 12
2. Power-on module in slot 4 and wait till it comes online
3. Power-on the module powered-off in step 1
4. Do "copy running-config startup-config" to save this setting
```

The following example uses the **show module**, **show port index-allocation**, and **show module recovery-steps** commands to display a Generation 1 module that is powered down because of alignment, even though contiguous indices 208 through 252 are available.

```
switch# show module
Mod  Ports  Module-Type                       Model           Status
---  -----  -------------------------------- ------------------ ------------
1    48     1/2/4 Gbps FC Module             DS-X9148           ok
2    48     1/2/4 Gbps FC Module             DS-X9148           ok
4    48     1/2/4 Gbps FC Module             DS-X9148           ok
5    0      Supervisor/Fabric-2              DS-X9530-SF2-K9    active *
6    0      Supervisor/Fabric-2              DS-X9530-SF2-K9    ha-standby
7    48     1/2/4 Gbps FC Module             DS-X9148           ok
9    32     1/2 Gbps FC Module               DS-X9032   powered-dn
Mod  Power-Status  Power Down Reason
---  ------------  --------------------------
9    powered-dn    Insufficient resources (dest Index)
switch# show port index-allocation

Module index distribution:
-------------------------------------------------------+
Slot | Allowed |      Alloted indices info            |
     |  range  | Total |          Index values        |
-----|---------|-------|------------------------------|
 1   |   0-1023|   48  | 160-207                      |
 2   |   0-1023|   48  | 3-50                         |
 3   |  -----  |   -   | (None)                       |
 4   |   0-1023|   48  | 51-98                        |
 7   |   0-1023|   48  | 99-146                       |
 8   |  -----  |   -   | (None)                       |
 9   |  -----  |   -   | (None)                       |
SUP  | 253-255 |   3   | 253-255                      |
switch# show module 9 recovery-steps
Failure Reason:
Contiguous and aligned indices unavailable for Generation-1 modules
Check "show port index-allocation" for more details
Recovery Steps:
Please follow the steps below:
```

```
1. Power off module in ANY ONE of the slots: 1, 4
2. Power on failed module in slot 9 and wait till it comes online
3. Power on the module that was powered off in step 1 and wait till it comes
   online
4. Do "copy running-config startup-config" to save this setting
```

show monitor session

To display specific information about a SPAN session, use the **show monitor session** command.

show monitor session [{**session-id**|**all**|**range session-id**}]

Syntax Description

session-id	(Optional) Specifies the SPAN session ID. The range is 1 to 48.
all	(Optional) Displays the SPAN session configuration for all sessions.
range	(Optional) Displays the SPAN session configuration for a range of sessions.

Command Default

None.

Command Modes

Any mode

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays local span session for all created sessions:

```
switch(config-monitor)# show monitor session all
   session 1
---------------
mode              : extended
ssn direction     : both
state             : up
source intf       :
    rx            : fc1/38
    tx            : fc1/38
    both          : fc1/38
source VLANs      :
    rx            :
    tx            :
    both          :
source exception  :
filter VLANs      : filter not specified
destination ports : fc1/1
Feature       Enabled   Value   Modules Supported       Modules Not-Supported
-------------------------------------------------------------------------------
rate-limiter  Yes       100%     5                       -
MTU-Trunc     No
Sampling      No
Legend:
  MCBE  = Multicast Best Effort
  L3-TX = L3 Multicast Egress SPAN
  Ex-SP = Module(s) with Exception SPAN source allocated in the session
```

The following example displays local span session in the both mode (bi-directional):

```
switch(config-monitor)# show monitor session 1
   session 1
---------------
mode              : extended
ssn direction     : both
state             : up
source intf       :
    rx            : fc1/38
    tx            : fc1/38
    both          : fc1/38
source VLANs      :
    rx            :
    tx            :
    both          :
source exception  :
filter VLANs      : filter not specified
destination ports : fc1/1
Feature       Enabled   Value   Modules Supported       Modules Not-Supported
-------------------------------------------------------------------------------
rate-limiter  Yes       100%     5                       -
MTU-Trunc     No
Sampling      No
Legend:
  MCBE  = Multicast Best Effort
  L3-TX = L3 Multicast Egress SPAN
  Ex-SP = Module(s) with Exception SPAN source allocated in the session
```

The following example displays local span session in rx mode(uni-directional):

```
switch(config-monitor)# show monitor session 1
   session 1
---------------
ssn direction     : rx
state             : up
source intf       :
    rx            : fc1/38
    tx            :
    both          :
source VLANs      :
    rx            :
    tx            :
    both          :
source exception  :
filter VLANs      : filter not specified
destination ports : fc1/1
Feature       Enabled   Value   Modules Supported       Modules Not-Supported
-------------------------------------------------------------------------------
rate-limiter  Yes       100%     5                       -
MTU-Trunc     No
Sampling      No
Legend:
  MCBE  = Multicast Best Effort
  L3-TX = L3 Multicast Egress SPAN
  Ex-SP = Module(s) with Exception SPAN source allocated in the session
```

The following example displays local span session in tx mode(uni-directional):

```
switch(config)# monitor session 1 tx
switch(config-monitor)# source interface fc1/38 tx
switch(config-monitor)# destination interface fc1/1
switch(config-monitor)# no shut
switch(config-monitor)# show monitor session 1
```

```
   session 1
---------------
ssn direction     : tx
state             : up
source intf       :
    rx            :
    tx            : fc1/38
    both          :
source VLANs      :
    rx            :
    tx            :
    both          :
source exception  :
filter VLANs      : filter not specified
destination ports : fc1/1
Feature       Enabled   Value   Modules Supported       Modules Not-Supported
-------------------------------------------------------------------------------
rate-limiter  Yes       100%     5                       -
MTU-Trunc     No
Sampling      No
Legend:
  MCBE  = Multicast Best Effort
  L3-TX = L3 Multicast Egress SPAN
  Ex-SP = Module(s) with Exception SPAN source allocated in the session
```

The following example displays the rspan session in both direction or both mode:

```
switch(config-monitor)# show monitor session 1
   session 1
---------------
mode              : extended
ssn direction     : both
state             : up
source intf       :
    rx            : fc1/38
    tx            : fc1/38
    both          : fc1/38
source VLANs      :
    rx            :
    tx            :
    both          :
source exception  :
filter VLANs      : filter not specified
destination ports : fc1/1
Feature       Enabled   Value   Modules Supported       Modules Not-Supported
-------------------------------------------------------------------------------
rate-limiter  Yes       100%     5                       -
MTU-Trunc     No
Sampling      No
Legend:
  MCBE  = Multicast Best Effort
  L3-TX = L3 Multicast Egress SPAN
  Ex-SP = Module(s) with Exception SPAN source allocated in the session
```

The following example displays the remote rspan session in tx direction or tx mode(uni-directional):

```
switch(config)# monitor session 1 tx
switch(config-monitor)# source interface fc1/38
switch(config-monitor)# destination interface fc1/1
switch(config-monitor)# no shut
switch(config-monitor)# show monitor session 1
   session 1
---------------
```

```
ssn direction     : tx
state             : up
source intf       :
    rx            :
    tx            : fc1/38
    both          :
source VLANs      :
    rx            :
    tx            :
    both          :
source exception  :
filter VLANs      : filter not specified
destination ports : fc1/1
Feature       Enabled   Value   Modules Supported       Modules Not-Supported
-------------------------------------------------------------------------------
rate-limiter  Yes       100%     5                       -
MTU-Trunc     No
Sampling      No
Legend:
  MCBE  = Multicast Best Effort
  L3-TX = L3 Multicast Egress SPAN
  Ex-SP = Module(s) with Exception SPAN source allocated in the session
```

The following example displays the local span session with port-channel as source in rx mode:

```
switch(config)# monitor session 1 rx
switch(config-monitor)# source interface port-channel 1
switch(config-monitor)# destination
description   destination
switch(config-monitor)# destination interface fc1/1
switch(config-monitor)# no shut
switch(config-monitor)# show monitor session 1
   session 1
---------------
mode              : extended
ssn direction     : both
state             : up
source intf       :
    rx            : Po1
    tx            : Po1
    both          : Po1
source VLANs      :
    rx            :
    tx            :
    both          :
source exception  :
filter VLANs      : filter not specified
destination ports : fc1/1
Feature       Enabled   Value   Modules Supported       Modules Not-Supported
-------------------------------------------------------------------------------
rate-limiter  Yes       100%     5                       -
MTU-Trunc     No
Sampling      No
Legend:
  MCBE  = Multicast Best Effort
  L3-TX = L3 Multicast Egress SPAN
  Ex-SP = Module(s) with Exception SPAN source allocated in the session
```

The following example displays the local span session with port-channel as source in rx mode:

```
switch(config)# monitor session 1 rx
switch(config-monitor)# source interface port-channel 1
switch(config-monitor)# destination
```

```
switch(config-monitor)# destination interface fc1/1
switch(config-monitor)# no shut
switch(config-monitor)# show monitor session 1
   session 1
---------------
ssn direction     : rx
state             : up
source intf       :
    rx            : Po1
    tx            :
    both          :
source VLANs      :
    rx            :
    tx            :
    both          :
source exception  :
filter VLANs      : filter not specified
destination ports : fc1/1
Feature       Enabled   Value   Modules Supported       Modules Not-Supported
------------------------------------------------------------------------------
rate-limiter  Yes       100%     5                       -
MTU-Trunc     No
Sampling      No
Legend:
  MCBE  = Multicast Best Effort
  L3-TX = L3 Multicast Egress SPAN
  Ex-SP = Module(s) with Exception SPAN source allocated in the session
The following example displays the local span session with port-channel as source in tx
mode:
switch(config)# monitor session 1 tx
switch(config-monitor)# source interface port-channel 1
switch(config-monitor)# destination interface fc1/1
switch(config-monitor)# no shut
switch(config-monitor)# show monitor session 1
   session 1
---------------
ssn direction     : tx
state             : up
source intf       :
    rx            :
    tx            : Po1
    both          :
source VLANs      :
    rx            :
    tx            :
    both          :
source exception  :
filter VLANs      : filter not specified
destination ports : fc1/1
Feature       Enabled   Value   Modules Supported       Modules Not-Supported
------------------------------------------------------------------------------
rate-limiter  Yes       100%     5                       -
MTU-Trunc     No
Sampling      No
Legend:
  MCBE  = Multicast Best Effort
  L3-TX = L3 Multicast Egress SPAN
  Ex-SP = Module(s) with Exception SPAN source allocated in the session
The following example displays the local span session with VSAN as source:
switch(config)# monitor session 1
switch(config-monitor)# source vsan 1
switch(config-monitor)# destination interface fc1/1
switch(config-monitor)# no shut
switch(config-monitor)#
```

```
sw-luke(config-monitor)# show monitor session 1
   session 1
---------------
mode              : extended
ssn direction     : both
state             : up
source intf       :
    rx            :
    tx            :
    both          :
source VLANs      :
    rx            :
    tx            :
    both          :
source VSANs      :
    rx            : 1
source exception  :
filter VLANs      : filter not specified
destination ports : fc1/1
Feature       Enabled   Value   Modules Supported       Modules Not-Supported
-------------------------------------------------------------------------------
rate-limiter  Yes       100%     5                       -
MTU-Trunc     No
Sampling      No
Legend:
  MCBE  = Multicast Best Effort
  L3-TX = L3 Multicast Egress SPAN
  Ex-SP = Module(s) with Exception SPAN source allocated in the session
```

The following example displays the local span session with VSAN as source with VSAN filter option:

```
switch(config)# monitor session 1
switch(config-monitor)# source vsan 1
switch(config-monitor)# destination interface fc1/1
switch(config-monitor)# source filter vsan 1
switch(config-monitor)# no shut
sw-luke(config-monitor)# show monitor session 1
   session 1
---------------
mode              : extended
ssn direction     : both
state             : up
source intf       :
    rx            :
    tx            :
    both          :
source VLANs      :
    rx            :
    tx            :
    both          :
source VSANs      :
    rx            : 1
source exception  :
filter VLANs      : filter not specified
    VSANs         : 1
destination ports : fc1/1
Feature       Enabled   Value   Modules Supported       Modules Not-Supported
-------------------------------------------------------------------------------
rate-limiter  Yes       100%     5                       -
MTU-Trunc     No
Sampling      No
Legend:
  MCBE  = Multicast Best Effort
```

```
L3-TX = L3 Multicast Egress SPAN
Ex-SP = Module(s) with Exception SPAN source allocated in the session
```

Related Commands

Command	Description
monitor session source interface	Configures the SPAN traffic in both ingress (rx) and egress (tx) directions.

show npv flogi-table

To display the information about N Port Virtualization (NPV) FLOGI session, use the show npv flogi-table command.

show npv flogi-table

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the information on NPV FLOGI session:

```
switch# show npv flogi-table
--------------------------------------------------------------------------------
SERVER EXTERNAL
INTERFACE VSAN FCID PORT NAME NODE NAME INTERFACE
--------------------------------------------------------------------------------
fc1/13 1 0x330100 2f:ff:00:06:2b:10:c1:14 2f:ff:00:06:2b:10:c1:14 fc1/4
fc1/13 1 0x333500 2f:bf:00:06:2b:10:c1:14 2f:bf:00:06:2b:10:c1:14 fc1/4
fc1/13 1 0x333600 2f:9f:00:06:2b:10:c1:14 2f:9f:00:06:2b:10:c1:14 fc1/3
fc1/13 1 0x333800 2f:7f:00:06:2b:10:c1:14 2f:7f:00:06:2b:10:c1:14 fc1/2
fc1/13 1 0x333e00 2f:3f:00:06:2b:10:c1:14 2f:3f:00:06:2b:10:c1:14 fc1/4
fc1/13 1 0x334a00 2e:bf:00:06:2b:10:c1:14 2e:bf:00:06:2b:10:c1:14 fc1/3
fc1/13 1 0x335400 2e:7f:00:06:2b:10:c1:14 2e:7f:00:06:2b:10:c1:14 fc1/4
fc1/13 1 0x336200 2d:ff:00:06:2b:10:c1:14 2d:ff:00:06:2b:10:c1:14 fc1/1
fc1/13 1 0x336f00 2d:9f:00:06:2b:10:c1:14 2d:9f:00:06:2b:10:c1:14 fc1/2
fc1/13 1 0x337300 2d:5f:00:06:2b:10:c1:14 2d:5f:00:06:2b:10:c1:14 fc1/2
fc1/13 1 0x337900 2c:ff:00:06:2b:10:c1:14 2c:ff:00:06:2b:10:c1:14 fc1/1
fc1/13 1 0x338500 2c:bf:00:06:2b:10:c1:14 2c:bf:00:06:2b:10:c1:14 fc1/2
fc1/13 1 0x338a00 2c:9f:00:06:2b:10:c1:14 2c:9f:00:06:2b:10:c1:14 fc1/1
```

Related Commands

Command	Description
show npv status	Displays the NPV current status.

show npv internal info

To display internal N Port Virtualization (NPV) information, use the show npv internal info command.

show npv internal info

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the NPV internal information:

```
switch# show npv internal info
NPV Globals:
============
NPV mode: ENABLED
Switch-Name: 209.165.200.226
Switch Mgmt IP Address: 209.165.200.226
proxy logo Retries: 1
Internal FLOGI max timeout Retries: -1
NS Registration max timeout Retries: 5
timer group handle: 0x30038fe0
Number of Active External Interfaces: 0
External Interface Info:
========================
Interface Information:
  ifindex: fc1/1, VSAN: 1, internal FLOGI fcid: 0x1e0000
  FSM current state: NPIVP_EXT_IF_ST_FLOGI_FAILED
  Internal FLOGI Fail Reason: Mismatch in VSAN for this upstream port
  fabric pwwn: 20:05:00:05:30:00:ca:16, fabric nwwn: 20:0a:00:05:30:00:ca:17
  my pwwn: 20:01:00:05:30:01:71:b8, my nwwn: 20:01:00:05:30:01:71:b9
Port Parameters:
  Rx B2B Credits: 16, Multiplier: 0, Buff Size: 2112
  Tx B2B Credits: 16, Multiplier: 0, Buff Size: 2112, bbscn: 0
  bbscn_capable: TRUE bbscn_max: 14, port_bbscn: 0
Timer & Retry Information:
  Busy Timer              (1), id: 21045, active: FALSE time remaining: 0
  Fail Retry Timer        (7), id: 4209, active: TRUE time remaining: 1
  FDISC Response Timer    (2), id: 00, active: FALSE time remaining: 0
  Error Clear Timer       (6), id: 71, active: TRUE time remaining: 433
Statistics:
  flogi retry count            : 113
  ns registration retry count  : 0
  number of flogis accepted: 0
  login failures out of ids: 0
  other login failures     : 0
```

```
  timed out login_failures : 0
  pending queue size       : 0
FLOGIs on this interface :
Interface Information:
  ifindex: fc1/5, VSAN: 1, internal FLOGI fcid: 0x000000
  FSM current state: NPIVP_EXT_IF_ST_PREINIT_DONE
  fabric pwwn: 00:00:00:00:00:00:00:00, fabric nwwn: 00:00:00:00:00:00:00:00
  my pwwn: 00:00:00:00:00:00:00:00, my nwwn: 00:00:00:00:00:00:00:00
Port Parameters:
  Rx B2B Credits: 0, Multiplier: 0, Buff Size: 0
  Tx B2B Credits: 0, Multiplier: 0, Buff Size: 0, bbscn: 0
  bbscn_capable: FALSE bbscn_max: 0, port_bbscn: 0
Timer & Retry Information:
  Busy Timer              (1), id: 00, active: FALSE time remaining: 0
  Fail Retry Timer        (7), id: 00, active: FALSE time remaining: 0
  FDISC Response Timer    (2), id: 00, active: FALSE time remaining: 0
  Error Clear Timer       (6), id: 71, active: TRUE time remaining: 433
Statistics:
  flogi retry count            : 0
  ns registration retry count  : 0
  number of flogis accepted: 0
  login failures out of ids: 0
  other login failures     : 0
  timed out login_failures : 0
  pending queue size       : 0
FLOGIs on this interface :
Server Interface Info:
======================
Interface Information:
  ifindex: fc1/4,  VSAN: 1, NPIV enable: FALSE,  lcp init done: FALSE
  Selected External Interface:
  FSM current state: NPIVP_SVR_IF_ST_WAITING_EXTERNAL_INTERFACE
Port Parameters:
  rxbbcredit: 0 rxbufsize: 0
  txbbcredit: 0 txbufsize: 0 txbbscn: 0
  bbscn_capable: FALSE bbscn_max: 0,  port_bbscn: 0
Statistics:
  number of FLOGIs: 0
```

Related Commands

Command	Description
debug npv	Enables debugging NPV configurations.
show debug npv	Displays the NPV debug commands configured on the switch.

show npv internal info traffic-map

To display internal N port virtualization (NPV) information about a traffic map, use the show npv internal info traffic-map command.

show npv internal info traffic-map

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
4.1(1b)	Command output has been changed.
3. 3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays NPV internal information:

```
switch# show npv internal info traffic-map
NPV Traffic Map Information:
------------------------------------------------------
Server-If       Last Change Time        External-If(s)
------------------------------------------------------
fc1/10          2147469648.265604868    fc1/9,fc1/13
fc1/20          2147469648.265604868    fc1/9,fc1/13
------------------------------------------------------
switch#
```

Related Commands

Command	Description
show npv traffic-map	Displays NPV traffic map.

show npv status

To display the N Port Virtualization (NPV) current status, use the show npv status command.

show npv status

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the current status of NPV:

```
switch# show npv status
External Interfaces:
====================
Number of External Interfaces: 6
Interface: fc1/1, FCID: 0x330037, State: Up
Interface: fc1/2, FCID: 0x330038, State: Up
Interface: fc1/3, FCID: 0x330039, State: Up
Interface: fc1/4, FCID: 0x33003a, State: Up
Interface: fc1/23, FCID: 0x7d0007, State: Up
Interface: fc1/24, FCID: 0x7d0006, State: Up
Server Interfaces:
==================
Number of Server Interfaces: 4
Interface: fc1/13, NPIV: Yes, State: Up
Interface: fc1/14, NPIV: Yes, State: Up
Interface: fc1/15, NPIV: Yes, State: Up
```

Related Commands

Command	Description
show npv flogi-table	Displays the information about NPV FLOGI session.

show npv traffic-map

To display an N Port Virtualization (NPV) traffic map, use the show npv traffic-map command.

show npv traffic-map

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the NPV traffic map information:

```
switch# show npv traffic-map
NPV Traffic Map Information:
----------------------------------------
Server-If       External-If(s)
----------------------------------------
fc1/10          fc1/9,fc1/13
fc1/20          fc1/9,fc1/13
----------------------------------------
switch#
```

Related Commands

Command	Description
show npv flogi-table	Displays information about NPV FLOGI sessions.
show npv internal info traffic-map	Displays internal information about the traffic map.

show ntp

To display the configured Network Time Protocol (NTP) server and peer associations, use the **show ntp** command.

show ntp {**peers**|**pending peers**|**pending-diff**|**session-status**|**statistics** [{**io**|**local**|**memory**|**peer** {**ipaddr** *ip-address*|**name** *peer-name*}}]|**timestamp-status**}

Syntax Description

peers	Displays all the peers.
pending peers	Displays pending NTP configuration changes on all peers.
pending-diff	Displays the differences between the pending NTP configuration changes and the active NTP configuration.
session-status	Displays the Cisco Fabric Services (CFS) session status.
statistics	Displays the NTP statistics
io	(Optional) Displays the input/output statistics.
local	(Optional) Displays the counters maintained by the local NTP.
memory	(Optional) Displays the statistics counters related to memory code.
peer	(Optional) Displays the per-peer statistics counter of a peer.
ipaddr *ip-address*	(Optional) Displays the peer statistics for the specified IP address.
name *peer-name*	(Optional) Displays the peer statistics for the specified peer name.
timestamp-status	Displays if the timestamp check is enabled.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0(x)	Added the pending, pending-diff, and **session-status** keywords.

Usage Guidelines

None.

Examples

The following example displays the NTP peer information:

```
switch# show ntp peers
```

```
-----------------------------------------
  Peer IP Address               Serv/Peer
-----------------------------------------
  10.20.10.2                    Server
  10.20.10.0                    Peer
```

The following example displays the NTP I/O statistics:

```
switch# show ntp statistics io
time since reset:     11152
receive buffers:      9
free receive buffers: 9
used receive buffers: 9
low water refills:    0
dropped packets:      0
ignored packets:      0
received packets:     3
packets sent:         2
packets not sent:     0
interrupts handled:   3
received by int:      3
```

The following example displays the NTP local statistics:

```
switch# show ntp statistics local
system uptime:          11166
time since reset:       11166
bad stratum in packet:  0
old version packets:    4
new version packets:    0
unknown version number: 0
bad packet format:      0
packets processed:      0
bad authentication:     0
```

The following example displays the NTP memory statistics information:

```
switch# show ntp statistics memory
time since reset:     11475
total peer memory:    15
free peer memory:     15
calls to findpeer:    0
new peer allocations: 0
peer demobilizations: 0
hash table counts:      0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
                        0   0   0   0   0   0   0   0
```

The following example displays the NTP peer statistics information using the IP address of the peer:

```
switch# show ntp statistics peer ipaddr 10.1.1.1
```

The following example displays the NTP peer statistics information using the name of the peer:

```
switch# show ntp statistics peer name Peer1
```

The following example displays the NTP timestamp status information:

```
switch# show ntp timestamp-status
Linecard 9 does not support Timestamp check.
```

Related Commands

Command	Description
ntp	Configures NTP parameters.

show nxapi

To display the status of NX-API and its elements, use the **show nxapi** command.

show nxapi

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Example

The following example shows how to display the status of NX-API and its elements.

```
switch# show nxapi

NX-API:       Enabled         Sandbox:      Enabled
HTTP Port:    8080            HTTPS Port:   Disabled
```

Related Commands

Command	Description
feature nxapi	Enables the NX-API feature.
nxapi sandbox	Enables the NX-API Developer Sandbox.
nxapi http port *port-number*	Configures an HTTP port to access the NX-API Developer Sandbox.
nxapi https port *port-number*	Configures an HTTPS port to access the NX-API Developer Sandbox.

show port index-allocation

To display port index allocation information, use the **show port index-allocation** command.

show port {**index-allocation startup**|**naming**}

Syntax Description

index-allocation	Displays port index allocation information.
startup	Displays port index allocation information at startup.
naming	Displays port naming information.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.
3.1(2)	Added the naming keyword.

Usage Guidelines

All software releases prior to Cisco SAN-OS Release 3.0(1) support Generation 1 hardware. Cisco SAN-OS Release 3.0(1) and later support Generation 2 hardware. You can combine Generation 1 and Generation 2 switching modules, with either Supervisor-1 modules or Supervisor-2 modules. However, combining switching modules and supervisor modules has the following limitations:

- Supervisor-1 modules only support a maximum of 256 port indexes, regardless of type of switching modules.
- Supervisor-2 modules support a maximum of 1024 port indexes when all switching modules in the chassis are Generation 2.
- Supervisor-2 modules only support a maximum of 256 port indexes when both Generation 1 and Generation 2 switching modules are installed in the chassis.

Note The Cisco MDS 9124 switch does not support the show port index-allocation startup command; however, it does support the show port index-allocation command.

Note On a switch where the maximum number of port indexes is 256, any module that exceeds that limit does not power up.

Examples

The following example displays port index allocation information at startup on a Cisco MDS switch with only Generation 1 switching modules installed:

```
switch# show port index-allocation startup
Startup module index distribution:
-----------------------------------------------------+
Slot | Allowed |      Alloted indices info            |
     |  range  | Total |          Index values        |
-----|---------|-------|------------------------------|
 1   |   0-  31|   32  | 0-31                         |
 2   |  32-  63|   32  | 32-63                        |
 3   |  64-  95|   32  | 64-95                        |
SUP  |  -----  |    3  | 253-255                      |
```

The following example displays current port index allocation on a Cisco MDS switch with only Generation 1 switching modules installed:

```
switch# show port index-allocation
Module index distribution:
-----------------------------------------------------+
Slot | Allowed |      Alloted indices info            |
     |  range  | Total |          Index values        |
-----|---------|-------|------------------------------|
 1   |   0-  31|   32  | 0-31                         |
 2   |  32-  63|   32  | 32-63                        |
 3   |  64-  95|   32  | 64-95                        |
 4   |  96- 127|   -   | (None)                       |
SUP  |  -----  |    3  | 253-255                      |
```

The following example displays port index allocation information at startup on a Cisco MDS switch with Generation 1 and Generation 2 switching modules installed:

```
switch# show port index-allocation startup
Startup module index distribution:
-----------------------------------------------------+
Slot | Allowed |      Alloted indices info            |
     |  range  | Total |          Index values        |
-----|---------|-------|------------------------------|
 4   |   0- 255|   32  | 0-31                         |
 5   |   0- 255|   32  | 32-63                        |
 6   |   0- 255|   32  | 96-127                       |
 9   |   0- 255|   24  | 64-87                        |
SUP  |  -----  |    3  | 253-255                      |
```

The following example shows the current port index allocation on a Cisco MDS switch with Generation 1 and Generation 2 switching modules installed:

```
switch# show port index-allocation
Module index distribution:
-----------------------------------------------------+
Slot | Allowed |      Alloted indices info            |
     |  range  | Total |          Index values        |
-----|---------|-------|------------------------------|
 1   |   0- 255|   -   | (None)                       |
 2   |   0- 255|   -   | (None)                       |
 3   |   0- 255|   -   | (None)                       |
 4   |   0- 255|   32  | 0-31                         |
 5   |   0- 255|   32  | 32-63                        |
 6   |   0- 255|   32  | 96-127                       |
 9   |   0- 255|   24  | 64-87                        |
10   |   0- 255|   -   | (None)                       |
11   |   0- 255|   -   | (None)                       |
12   |   0- 255|   -   | (None)                       |
13   |   0- 255|   -   | (None)                       |
```

show port-channel

Use the **show port-channel** command to view information about existing PortChannel configurations.

show port-channel {**compatibility-parameters**|**consistency [detail]**|**database** [**interface port-channel** *port-channel-number*]|**summary**|**usage**}

Syntax Description

compatibility-parameters	Displays compatibility parameters.
consistency	Displays the database consistency information of all modules.
detail	Displays detailed database consistency information.
database	Displays PortChannel database information.
interface port-channel port-channel-number	Specifies the PortChannel number. The range is 1 to 256.
summary	Displays PortChannel summary.
usage	Displays PortChannel number usage.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	• Increased the **interface port-channel** range to 256. • Modified the output of the **compatibility-parameters** option.

Usage Guidelines

None.

Examples

The following example displays the PortChannel summary:

```
switch# show port-channel summary
 NEW
```

The following example displays the PortChannel compatibility parameters:

```
switch# show port-channel compatibility-parameters
Parameters that have to be consistent across all members in a port-channel.
1. physical port layer
Members must have the same interface type, such as fibre channel, ethernet
or fcip.
2. port mode
Members must have the same port mode configured, either E or AUTO. If they
```

```
are configured in AUTO port mode, they have to negotiate E mode when they
come up. If a member negotiates a different mode, it will be suspended.
3. trunk mode
Members must have the same trunk mode configured. If they are configured in
AUTO trunking mode, they have to negotiate the same trunking mode when they
come up. If a member negotiates a different mode, it will be suspended.
4. speed
Members must have the same speed configured. If they are configured in AUTO
speed, they have to negotiate the same speed when they come up. If a member
negotiates a different speed, it will be suspended.
5. MTU
Members have to have the same MTU configured. This only applies to ethernet
port-channel.
6. ethernet port index
This only applies to ethernet port-channel. Each ethernet port-channel
could only have two ethernet ports. They must be in the same slot, their
port indices must be adjacent and the lower number must be odd. Example:
Gigabitethernet 8/5 - 6.
7. rate mode
Members must have the same rate mode configured. Rate Mode applies only to
isola FC ports
8. Maximum Speed Mismatch
Members must be configured to auto-negotiate to the same maximum speed.
9. Resources Unavailable
Members must be able to acquire resources required to maintain
compatibility. Check shared resources like speed, rate-mode and port mode.
10. Out of Service
Members must be in-service.
11. port VSAN
Members must have the same port VSAN.
12. port allowed VSAN list
Members must have the same port allowed VSAN list.
13. IP address
Members must not have IP address configured. This only applies to ethernet
port-channel.
14. IPv6 configuration
Members must not have any IPv6 configuration. This only applies to ethernet
port-channel.
15. port-security active bindings
Members must all be permitted by the activated port-security bindings and
fabric-bindings in all the allowed VSANs.
16. FC receive buffer size
Members must have the same fc receive buffer size. If the configured
receive buffer size is not compatible with the port capability then the
port will be error disabled
17. IP ACLs
Members must not have IP ACLs configured individually on them. This only
applies to ethernet port-channel.
18. sub interfaces
Members must not have sub-interfaces.
19. Access VLAN
Members must have same Access VLAN configured.
20. Native VLAN
Members must have same Native VLAN configured.
21. Duplex Mode
Members must have same Duplex Mode configured.
22. Ethernet Layer
Members must have same Ethernet Layer (switchport/no-switchport) configured.
23. Span Port
Members cannot be SPAN ports.
```

The following example displays the PortChannel database:

```
switch# show port-channel database
```

```
 port-channel 2
    Administrative channel mode is on
    Operational channel mode is on
    Last membership update succeeded
    First operational port is fc2/2
    1 port in total, 1 port up
    Ports:   fc2/2    [up]
```

The **show port-channel consistency** command has two options: without details **and with details**.

Command without details:

```
switch# show port-channel consistency
 Database is consistentswitch#
```

Command with details:

```
switch# show port-channel consistency detail
Authoritative port-channel database:
============================================
totally 1 port-channels
port-channel 2:
    1 ports, first operational port is fc2/2
    fc2/2    [up]
============================================
database 1: from module 5
============================================
totally 1 port-channels
port-channel 2:
    1 ports, first operational port is fc2/2
    fc2/2    [up]
============================================
database 2: from module 2
============================================
totally 1 port-channels
port-channel 2:
    1 ports, first operational port is fc2/2
    fc2/2    [up]
============================================
```

The **show port-channel usage** command displays details of the used and unused PortChannel numbers.

```
switch# show port-channel usage
Totally 2 port-channel numbers used=================================Used  :   3, 9Unused:
   1-2, 4-8, 10-256
```

show port-channel compatibility-parameters

To display the PortChannel compatibility parameters, use the show port-channel compatibility-parameters command.

show port-channel compatibility-parameters

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the PortChannel compatibility parameters:

```
switch# show port-channel compatibility-parameters
Parameters that have to be consistent across all members in a port-channel.
1. physical port layer
Members must have the same interface type, such as fibre channel, ethernet
or fcip.
2. port mode
Members must have the same port mode configured, either E or AUTO. If they
are configured in AUTO port mode, they have to negotiate E mode when they
come up. If a member negotiates a different mode, it will be suspended.
3. trunk mode
Members must have the same trunk mode configured. If they are configured in
AUTO trunking mode, they have to negotiate the same trunking mode when they
come up. If a member negotiates a different mode, it will be suspended.
4. speed
Members must have the same speed configured. If they are configured in AUTO
speed, they have to negotiate the same speed when they come up. If a member
negotiates a different speed, it will be suspended.
5. MTU
Members have to have the same MTU configured. This only applies to ethernet
port-channel.
6. ethernet port index
This only applies to ethernet port-channel. Each ethernet port-channel
could only have two ethernet ports. They must be in the same slot, their
port indeces must be adjacent and the lower number must be odd. Example:
Gigabitethernet 8/5 - 6.
7. rate mode
Members must have the same rate mode configured. Rate Mode applies only to
isola FC ports
8. Maximum Speed Mismatch
Members must be configured to auto-negotiate to the same maximum speed.
9. Resources Unavailable
Members must be able to acquire resources required to maintain
compatibility. Check shared resources like speed, rate-mode and port mode.
```

```
10. Out of Service
Members must be in-service.
11. MEDIUM
Members have to have the same medium type configured. This only applies to
ethernet port-channel.
12. Span mode
Members must have the same span mode.
13. admin channel mode
Port Channel admin channel mode must be active.
14. port VSAN
Members must have the same port VSAN.
15. port allowed VSAN list
Members must have the same port allowed VSAN list.
16. IP address
Members must not have IP address configured. This only applies to ethernet
port-channel.
17. IPv6 configuration
Members must not have any IPv6 configuration. This only applies to ethernet
port-channel.
18. port-security active bindings
Members must all be permitted by the activated port-security bindings and
fabric-bindings in all the allowed VSANs.
19. FC receive buffer size
Members must have the same fc receive buffer size. If the configured
receive buffer size is not compatible with the port capability then the
port will be error disabled
20. IP ACLs
Members must not have IP ACLs configured individually on them. This only
applies to ethernet port-channel.
21. sub interfaces
Members must not have sub-interfaces.
22. Duplex Mode
Members must have same Duplex Mode configured.
23. Ethernet Layer
Members must have same Ethernet Layer (switchport/no-switchport) configured.
24. Span Port
Members cannot be SPAN ports.
25. Storm Control
Members must have same storm-control configured.
26. Flow Control
Members must have same flowctrl configured.
27. Capabilities
Members must have common capabilities.
28. port
Members port VLAN info.
29. port
Members port does not exist.
30. switching port
Members must be switching port, Layer 2.
31. port access VLAN
Members must have the same port access VLAN.
--More--
```

Related Commands

Command	Description
show port-channel summary	Displays PortChannel summary.

show port-channel consistency

To display the PortChannel distributed database consistency, use the show port-channel consistency command.

show port-channel consistency detail

Syntax Description

detail	Specifies the PortChannel distributed database in all modules.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the Port Channel distributed database consistency:

```
switch# show port-channel consistency detail
Authoritative port-channel database:
============================================
total 1 port-channels
port-channel 1:
    1 ports, first operational port is none
    fc1/1    [down]
============================================
database 1: from module 1
============================================
total 1 port-channels
port-channel 1:
    1 ports, first operational port is none
    fc1/1    [down]
============================================
switch#
```

Related Commands

Command	Description
show port-channel compatibity-parameters	Displays PortChannel compatibility parameters.

show port-channel database

To display the PortChannel database, use the show port-channel database command.

show port-channel database interface port-channel *number*

Syntax Description

interface	Specifies the PortChannel interface.
port-channel *number*	Specifies the PortChannel number. The range is from 1 to 256.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.1(2)	This command was introduced.

Examples

The following example shows how to display the PortChannel database:

```
switch# show port-channel database interface port-channel 1
port-channel 1
    Administrative channel mode is on
    Operational channel mode is on
    Last membership update succeeded
    1 port in total, 0 ports up
    Ports:   fc1/1    [down]
switch#
```

Related Commands

Command	Description
show port-channel consistency	Displays PortChannel distributed database consistency.

show port-channel internal

To display the PortChannel internal status, use the show port-channel internal command.

show port-channel internal event-history {**all**|**debugs**|**errors**|**interface** {**fa**|**fc**|**gigabitethernet slot number port-channel port-channel number**|**lock**|**msgs**|**pcp**} **info** {**all**|**interface**} **mem-stats detail**}

Syntax Description

event-history	Specifies a PortChannel.
all	Specifies interface event transition for all interfaces.
debugs	Specifies debug logs for a PortChannel.
errors	Specifies error logs for a PortChannel.
interface	Specifies interface event transitions.
fa	Specifies the FA port interface.
fc	Specifies the Fiber Channel interface.
gigabitethernet	Specifies the Ethernet interface.
slot number	Specifies the slot number.
port-channel	Specifies the PortChannel interface.
port-channel number	Specifies the PortChannel number. The range is from 1 to 256.
lock	Specifies lock log of the PortChannel.
msgs	Specifies message logs of the PortChannel.
pcp	Specifies interface PCP event transition.
info	Specifies internal information.
all	Specifies PortChannel global information.
interface	Specifies PortChannel interface information.
mem-stats	Specifies memory allocation statistics of the PortChannel.
detail	Specifies detail memory statistics for the PortChannel.

Command Default

None.

Command Modes

EXEC 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 error logs for the PortChannel:

```
switch# show port-channel internal event-history errors
1) Event:E_DEBUG, length:99, at 268834 usecs after Thu Nov  6 12:44:17 2008
    [102] pcm_port_ac_add_eval(1420): pc: port-channel 2 last port 1000000 for t
his msg. send hw_config
2) Event:E_DEBUG, length:158, at 268821 usecs after Thu Nov  6 12:44:17 2008
    [102] pcm_port_ac_add_eval(1384): Added pc: port-channel 2 pinfo->nports=0x1
,port 1000000 for this msg. pinfo->bundle=0x1,mbr->bundle=0xfffe,ports_to_add=0x
1
3) Event:E_DEBUG, length:99, at 444720 usecs after Thu Nov  6 12:24:11 2008
    [102] pcm_port_ac_rem_eval(1655): pc: port-channel 1 last port 1000000 for t
his msg. send hw_config
4) Event:E_DEBUG, length:143, at 444702 usecs after Thu Nov  6 12:24:11 2008
    [102] pcm_port_ac_rem_eval(1645): removed pc: port-channel 1 pinfo->nports=0
x1,port 1000000 for this msg. pinfo->bundle=0x0,mbr->bundle=0xfffe
5) Event:E_DEBUG, length:72, at 462673 usecs after Thu Nov  6 12:23:59 2008
    [102] abort_members(1235): port-channel 2: reverting newly changed ports
6) Event:E_DEBUG, length:86, at 462660 usecs after Thu Nov  6 12:23:59 2008
    [102] split_members(1319): port-channel 2: fc1/1 is already in another port-
channel [1]
7) Event:E_DEBUG, length:68, at 293493 usecs after Thu Nov  6 12:19:05 2008
    [102] pcm_pc_ac_get_wwn(244): wwn request setting pinfo->bundle=0x1f
8) Event:E_DEBUG, length:65, at 292875 usecs after Thu Nov  6 12:19:05 2008
    [102] pcm_alloc_pc(494): pcallocpc setting pinfo->bundle to 0xFFFF
9) Event:E_DEBUG, length:73, at 535797 usecs after Thu Nov  6 12:02:03 2008
    [102] abort_members(1235): port-channel 20: reverting newly changed ports
10) Event:E_DEBUG, length:87, at 535784 usecs after Thu Nov  6 12:02:03 2008
    [102] split_members(1319): port-channel 20: fc1/1 is already in another port
-channel [1]
11) Event:E_DEBUG, length:68, at 533069 usecs after Thu Nov  6 12:02:03 2008
    [102] pcm_pc_ac_get_wwn(244): wwn request setting pinfo->bundle=0x13
12) Event:E_DEBUG, length:65, at 532434 usecs after Thu Nov  6 12:02:03 2008
    [102] pcm_alloc_pc(494): pcallocpc setting pinfo->bundle to 0xFFFF
13) Event:E_DEBUG, length:72, at 425969 usecs after Thu Nov  6 12:01:33 2008
    [102] abort_members(1235): port-channel 5: reverting newly changed ports
14) Event:E_DEBUG, length:86, at 425955 usecs after Thu Nov  6 12:01:33 2008
    [102] split_members(1319): port-channel 5: fc1/1 is already in another port-
channel [1]
15) Event:E_DEBUG, length:67, at 423106 usecs after Thu Nov  6 12:01:33 2008
    [102] pcm_pc_ac_get_wwn(244): wwn request setting pinfo->bundle=0x4
16) Event:E_DEBUG, length:65, at 422473 usecs after Thu Nov  6 12:01:33 2008
    [102] pcm_alloc_pc(494): pcallocpc setting pinfo->bundle to 0xFFFF
17) Event:E_DEBUG, length:72, at 612546 usecs after Thu Nov  6 12:01:22 2008
    [102] abort_members(1235): port-channel 2: reverting newly changed ports
18) Event:E_DEBUG, length:86, at 612534 usecs after Thu Nov  6 12:01:22 2008
    [102] split_members(1319): port-channel 2: fc1/1 is already in another port-
channel [1]
19) Event:E_DEBUG, length:67, at 56546 usecs after Thu Nov  6 12:00:16 2008
    [102] pcm_pc_ac_get_wwn(244): wwn request setting pinfo->bundle=0x1
20) Event:E_DEBUG, length:65, at 55927 usecs after Thu Nov  6 12:00:16 2008
    [102] pcm_alloc_pc(494): pcallocpc setting pinfo->bundle to 0xFFFF
21) Event:E_DEBUG, length:72, at 65985 usecs after Thu Nov  6 11:53:31 2008
    [102] abort_members(1235): port-channel 2: reverting newly changed ports
```

```
22) Event:E_DEBUG, length:86, at 65972 usecs after Thu Nov  6 11:53:31 2008
    [102] split_members(1319): port-channel 2: fc1/1 is already in another port-
channel [1]
23) Event:E_DEBUG, length:67, at 63276 usecs after Thu Nov  6 11:53:31 2008
    [102] pcm_pc_ac_get_wwn(244): wwn request setting pinfo->bundle=0x1
24) Event:E_DEBUG, length:65, at 62639 usecs after Thu Nov  6 11:53:31 2008
    [102] pcm_alloc_pc(494): pcallocpc setting pinfo->bundle to 0xFFFF
25) Event:E_DEBUG, length:90, at 942691 usecs after Thu Nov  6 11:48:04 2008
    [102] pcm_pc_create(923): port-channel interface <250> out of existing suppo
rted range 129
26) Event:E_DEBUG, length:40, at 942678 usecs after Thu Nov  6 11:48:04 2008
    [102] pcm_search_pc(733): invalid id 249


27) Event:E_DEBUG, length:40, at 175505 usecs after Mon Nov  3 13:25:07 2008
    [102] pcm_search_pc(733): invalid id 249
28) Event:E_DEBUG, length:40, at 346351 usecs after Mon Nov  3 13:23:58 2008
    [102] pcm_search_pc(733): invalid id 255
29) Event:E_DEBUG, length:40, at 634271 usecs after Mon Nov  3 13:17:10 2008
    [102] pcm_search_pc(733): invalid id 249
30) Event:E_DEBUG, length:73, at 1815 usecs after Thu Oct 30 17:16:05 2008
    [102] abort_members(1235): port-channel 20: reverting newly changed ports
31) Event:E_DEBUG, length:87, at 1802 usecs after Thu Oct 30 17:16:05 2008
    [102] split_members(1319): port-channel 20: fc1/1 is already in another port
-channel [1]
32) Event:E_DEBUG, length:68, at 999046 usecs after Thu Oct 30 17:16:04 2008
    [102] pcm_pc_ac_get_wwn(244): wwn request setting pinfo->bundle=0x13
33) Event:E_DEBUG, length:65, at 998412 usecs after Thu Oct 30 17:16:04 2008
    [102] pcm_alloc_pc(494): pcallocpc setting pinfo->bundle to 0xFFFF
34) Event:E_DEBUG, length:73, at 841236 usecs after Thu Oct 30 17:15:58 2008
    [102] abort_members(1235): port-channel 20: reverting newly changed ports
```

The following example shows how to display interface event transition for all interfaces:

```
switch# show port-channel internal event-history all
Low Priority Pending queue: len(0), max len(1) [Fri Nov  7 16:53:01 2008]
High Priority Pending queue: len(0), max len(14) [Fri Nov  7 16:53:01 2008]
PCM Control Block info:
pcm_max_channels        : 128
pcm_max_channel_in_use  : 32
pcm_max_eports          : 256
pcm_max_eports_inuse    : 0
bsup_dit_address : 0, rc=0x802b003e
has Generation-1 Line Card
Total of 1 Generation-1 Line cards
PCM total_vlans info: 0x0
g_pcm_cb.path.num_ports: 0
==================================================
PORT CHANNELS:
port-channel 1
channel     : 1
bundle      : 0
ifindex     : 0x4000000
pcport mode : NONE
admin mode  : on
oper mode   : on
nports      : 0
--More--
```

The following example shows how to display PortChannel global information:

```
switch# show port-channel internal info all
Low Priority Pending queue: len(0), max len(1) [Sun Nov  9 10:03:32 2008]
High Priority Pending queue: len(0), max len(14) [Sun Nov  9 10:03:32 2008]
```

```
PCM Control Block info:
pcm_max_channels        : 128
pcm_max_channel_in_use  : 32
pcm_max_eports          : 256
pcm_max_eports_inuse    : 0
bsup_dit_address : 0, rc=0x802b003e
has Generation-1 Line Card
Total of 1 Generation-1 Line cards
PCM total_vlans info: 0x0
g_pcm_cb.path.num_ports: 0
==================================================
PORT CHANNELS:
port-channel 1
channel     : 1
bundle      : 0
ifindex     : 0x4000000
pcport mode : NONE
admin mode  : on
oper mode   : on
nports      : 0
```

The following example shows how to display detail memstats for the PortChannel:

```
switch# show port-channel internal mem-stats detail
Private Mem stats for UUID : Malloc track Library(103) Max types: 5
-------------------------------------------------------------------------------
TYPE NAME                                          ALLOCS                  BYTES
                                                 CURR    MAX       CURR        MAX
   0 MT_MEM_other                                   0      0          0          0
   1 MT_MEM_mtrack_default                          0      0          0          0
   2 MT_MEM_mtrack_hdl                             30     31      13848      15484
   3 MT_MEM_mtrack_info                           390    518       6240       8288
   4 MT_MEM_mtrack_lib_name                       585    713      20466      24956
-------------------------------------------------------------------------------
Total bytes: 40554 (39k)
-------------------------------------------------------------------------------
Private Mem stats for UUID : Non mtrack users(0) Max types: 67
-------------------------------------------------------------------------------
TYPE NAME                                          ALLOCS                  BYTES
                                                 CURR    MAX       CURR        MAX
   0 [r-xp]/isan/bin/pcm                            0      0          0          0
   1 [r-xp]/isan/lib/convert/libsysstr.so           0      0          0          0
   2 [r-xp]/isan/lib/convert/libvdb.so              0      0          0          0
   3 [r-xp]/isan/lib/libaccounting.so.0.0.0         0      1          0         65
   4 [r-xp]/isan/lib/libacfg.so.0.0.0               0      8          0      51684
--More--
```

Related Commands

Command	Description
show port-channel database	Displays PortChannel database.

show port-channel summary

To display the PortChannel summary, use the show port-channel summary command.

show port-channel summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the PortChannel summary:

```
switch# show port-channel summary
--------------------------------------------------------------------------------
Interface                 Total Ports        Oper Ports        First Oper Port
--------------------------------------------------------------------------------
port-channel 1                 1                 0                  --
switch#
```

Related Commands

Command	Description
show port-channel internal	Displays the PortChannel internal status.

show port-channel usage

To display the PortChannel usage, use the show port-channel usage command.

show port-channel usage

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the PortChannel usage:

```
switch# show port-channel usage
Totally 1 port-channel number used
==================================
Used  :   1
Unused:   2 - 256
switch#
```

Related Commands

Command	Description
show port-channel summary	Displays the PortChannel usage.

show port-group-monitor

To display the the details about the Port Group Monitor (PGM) policy specified by [NAME] along with the counters information, use the show port-group-monitor command.

show port-group-monitor name

Syntax Description

name	Displays a policy name.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display Port Group Monitor policy name:

```
switch# show port-group-monitor pgmon
Policy Name  : pgmon
Admin status : Not Active
Oper status  : Not Active
Port type    : All Port Groups
-------------------------------------------------------------------------------------------Counter
 Threshold Interval %ge Rising Threshold %ge Falling Threshold In Use------- ---------
-------- -------------------- ---------------------- ------RX Performance Delta 60 80 20
YesTX Performance Delta 60 80 20
Yes-------------------------------------------------------------------------------------------switch#
```

The following example shows how to display Port Group Monitor:

```
switch# show port-group-monitor
-------------------------------------------------------------------------------------------
Port Group Monitor : enabled
-------------------------------------------------------------------------------------------
Policy Name  : pgm1
Admin status : Not Active
Oper status  : Not Active
Port type    : All Port Groups
-------------------------------------------------------------------------------------------
Counter Threshold Interval %ge Rising Threshold %ge Falling Threshold In Use
------- --------- -------- -------------------- ---------------------- ------
RX Performance Delta 60 50 10 Yes
TX Performance Delta 60 50 10 Yes
-------------------------------------------------------------------------------------------
Policy Name  : pgm2
Admin status : Not Active
Oper status  : Not Active
```

```
Port type    : All Port Groups
------------------------------------------------------------------------------------------------
Counter Threshold Interval %ge Rising Threshold %ge Falling Threshold In Use
------- --------- -------- -------------------- ---------------------- ------
RX Performance Delta 60 80 10 Yes
TX Performance Delta 60 80 10 Yes
------------------------------------------------------------------------------------------------
Policy Name  : default
Admin status : Not Active
Oper status  : Not Active
Port type    : All Port Groups
------------------------------------------------------------------------------------------------
Counter Threshold Interval %ge Rising Threshold %ge Falling Threshold In Use
------- --------- -------- -------------------- ---------------------- ------
RX Performance Delta 60 80 20 Yes
TX Performance Delta 60 80 20 Yes
------------------------------------------------------------------------------------------------
```

Related Commands

Command	Description
show port-group-monitor status	Displays Port Group Monitor status.

show port-group-monitor active

To display Port Group Monitor active policies along with the counters information, use the show port-group-monitor active command.

show port-group-monitor active

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display Port Group Monitor active policies:

```
Policy Name  : pgmon
Admin status : Active
Oper status  : Active
Port type    : All Port Groups
-------------------------------------------------------------------------------------------Counter
 Threshold Interval %ge Rising Threshold %ge Falling Threshold In Use------- ---------
-------- ------------------- ---------------------- ------RX Performance Delta 60 80 20
YesTX Performance Delta 60 80 20
Yes-------------------------------------------------------------------------------------------
```

Related Commands

Command	Description
show port-group-monitor status	Displays Port Group Monitor status.

show port-group-monitor status

To display Port Group Monitor (PGM) status, use the show port-group-monitor status command.

show port-group-monitor status

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display Port Group Monitor status:

```
switch# show port-group-monitor status
Port Group Monitor : EnabledActive Policies : pgmonLast 10 logs
switch#
```

Related Commands

Command	Description
show port-group-monitor	Displays Port Group Monitor information.

show port-license

To display the licensing usage on a Cisco MDS 9124, use the show port-license command.

show port-license

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the default port activation license configuration for the Cisco MDS 9124 switch:

```
switch# show port-license
 Available port activation licenses are 0
-----------------------------------------
  Interface    Port Activation License
-----------------------------------------
  fc1/1             acquire
  fc1/2             acquire
  fc1/3             acquire
  fc1/4             acquire
  fc1/5             acquire
  fc1/6             acquire
  fc1/7             acquire
  fc1/8             acquire
  fc1/9             eligible
  fc1/10            eligible
  fc1/11            eligible
  ...
  fc1/24            eligible
```

Related Commands

Command	Description
port-license	Makes a port eligible or ineligible to receive a license. Also used to acquire a license for a port.

show port-monitor

To configure the counter details of the policy, use the show port-monitor command.

show port-monitor [name]

Syntax Description

name	Displays a policy name.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
4.1(1b)	This command was introduced.

Usage Guidelines

The show port-monitor command can also take a string name of policy and displays the details of that policy only.

Examples

The following example shows how to display the counter details of the policy:

```
switch# show port-monitor
--------------------------------------------------------------------------------
-----------
Port Monitor : enabled
--------------------------------------------------------------------------------
-----------
Policy Name  : pgmon
Admin status : Active
Oper status  : Active
Port type    : All Access Ports
--------------------------------------------------------------------------------
-------------------------
Counter                  Threshold  Interval Rising Threshold event Falling Thre
shold  event Portguard
-------                  ---------  -------- ---------------- ----- ------------
------ ----- --------------
Link Loss                Delta      60       5                4     1
       4     Not enabled
Sync Loss                Delta      60       5                4     1
       4     Not enabled
ASIC Error Pkt from Port Delta      300      5                4     0
       4     Not enabled
ASIC Error Pkt to xbar   Delta      60       3                4     0
       4     Not enabled
ASIC Error Pkt from xbar Delta      300      5                4     0
--More--
switch#
```

Related Commands

Command	Description
show port-monitor	Shows port monitor policies.

show port-monitor active

To display the details of all operationally active policies, use the show port-monitor active command.

show port-monitor active

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
4.2.6	Changed the command output.
NX-OS 4.1(1b)	This command was introduced.

Usage Guidelines

Policies can be either operationally active or administratively active as shown by the show port-monitor active command. An administratively active policy is not active on the line card and can be activated operationally by enabling the port monitor.

Examples

The following example shows how to display the details of all operationally active policies:

```
switch(config)# show port-monitor active
Policy Name  : pgmon
Admin status : Active
Oper status  : Active
Port type    : All Access Ports
------------------------------------------------------------------------------
-------------------------
Counter                   Threshold  Interval Rising Threshold event Falling Thre
shold  event Portguard
-------                   ---------  -------- ---------------- ----- ------------
------ ----- --------------
Link Loss                 Delta      60       5                4     1
       4     Not enabled
Sync Loss                 Delta      60       5                4     1
       4     Not enabled
ASIC Error Pkt from Port Delta      300      5                4     0
       4     Not enabled
ASIC Error Pkt to xbar   Delta      60       3                4     0
       4     Not enabled
ASIC Error Pkt from xbar Delta      300      5                4     0
       4     Not enabled
------------------------------------------------------------------------------
-------------------------
--More--
switch(config)#
```

Related Commands

Command	Description
show port-monitor status	Shows the current status of the port monitor.

show port-monitor status

To display the current status of the port monitor feature along with the last 10 alarms or logs generated by port monitor, use the show port-monitor status command.

show port-monitor status

Syntax Description

This command has no argument or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows the current status of the port monitor feature:

```
switch# show port-monitor status
Port Monitor    : Enabled
Active Policies : pgm2
Last 10 logs :
switch#
```

Related Commands

Command	Description
show call home	Displays configured Call Home information.

show port-resources module

To display information about port resources in a Generation 2 module, use the **show port-resources** command.

show port-resources module *slot*

Syntax Description

slot	Specifies the module number. The range is 1 to 6.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the Generation 2 module shared resources configuration:

```
switch(config-if)# show port-resources module 1
Module 1
  Available dedicated buffers for global buffer #0 [port-group 1] are 2150
  Available dedicated buffers for global buffer #1 [port-group 2] are 2150
  Available dedicated buffers for global buffer #2 [port-group 3] are 2150
  Available dedicated buffers for global buffer #3 [port-group 4] are 2148
  Available dedicated buffers for global buffer #4 [port-group 5] are 2150
  Available dedicated buffers for global buffer #5 [port-group 6] are 2150
  Available dedicated buffers for global buffer #6 [port-group 7] are 2150
  Available dedicated buffers for global buffer #7 [port-group 8] are 650
  Available dedicated buffers for global buffer #8 [port-group 9] are 2150
  Available dedicated buffers for global buffer #9 [port-group 10] are 2150
  Available dedicated buffers for global buffer #10 [port-group 11] are 2150
  Available dedicated buffers for global buffer #11 [port-group 12] are 2150

 Port-Group 1
  Total bandwidth is 64.0 Gbps
  Allocated dedicated bandwidth is 64.0 Gbps
  --------------------------------------------------------------------
  Interfaces in the Port-Group       B2B Credit  Bandwidth  Rate Mode
                                        Buffers     (Gbps)
  --------------------------------------------------------------------
  fc1/1                                   500       16.0  dedicated
  fc1/2                                   500       16.0  dedicated
  fc1/3                                   500       16.0  dedicated
  fc1/4                                   500       16.0  dedicated

Port-Group 6
  Total bandwidth is 64.0 Gbps
  Allocated dedicated bandwidth is 64.0 Gbps
  --------------------------------------------------------------------
  Interfaces in the Port-Group       B2B Credit  Bandwidth  Rate Mode
                                        Buffers     (Gbps)
```

```
  ------------------------------------------------------------------------
  fc4/21                                  4090       16.0  dedicated
  fc4/22                                    10       16.0  dedicated
  fc4/23                                    10       16.0  dedicated
  fc4/24                                    10       16.0  dedicated

switch# show port-resources module 2
Module 2
Available dedicated buffers are 5164
Port-Group 1
 Total bandwidth is 12.8 Gbps
 Total shared bandwidth is 4.8 Gbps
 Allocated dedicated bandwidth is 8.0 Gbps
------------------------------------------------------------------------
Interfaces in the Port-Group B2B Credit Bandwidth Rate Mode
                               Buffers (Gbps)
------------------------------------------------------------------------
fc2/1                                16       4.0 shared
fc2/2                                16       4.0 shared
fc2/3                                16       4.0 shared
fc2/4                                16       4.0 shared
fc2/5                                16       4.0 dedicated
fc2/6                                16       4.0 dedicated
Port-Group 2
 Total bandwidth is 12.8 Gbps
 Total shared bandwidth is 4.8 Gbps
 Allocated dedicated bandwidth is 8.0 Gbps
------------------------------------------------------------------------
Interfaces in the Port-Group B2B Credit Bandwidth Rate Mode
                               Buffers (Gbps)
------------------------------------------------------------------------
fc2/7                                16       4.0 shared
fc2/8                                16       4.0 shared
fc2/9                                16       4.0 shared
fc2/10                               16       4.0 shared
fc2/11                               16       4.0 dedicated
fc2/12                               16       4.0 dedicated
Port-Group 3
 Total bandwidth is 12.8 Gbps
 Total shared bandwidth is 4.8 Gbps
 Allocated dedicated bandwidth is 8.0 Gbps
------------------------------------------------------------------------
Interfaces in the Port-Group B2B Credit Bandwidth Rate Mode
                               Buffers (Gbps)
------------------------------------------------------------------------
fc2/13                               16       4.0 shared
fc2/14                               16       4.0 shared
fc2/15                               16       4.0 shared
fc2/16                              250       4.0 dedicated
fc2/17                               16       2.0 dedicated
fc2/18                               16       2.0 dedicated
Port-Group 4
 Total bandwidth is 12.8 Gbps
 Total shared bandwidth is 0.8 Gbps
 Allocated dedicated bandwidth is 12.0 Gbps
------------------------------------------------------------------------
Interfaces in the Port-Group B2B Credit Bandwidth Rate Mode
                               Buffers (Gbps)
------------------------------------------------------------------------
fc2/19                               16       1.0 shared
fc2/20                               16       1.0 shared
fc2/21                               16       1.0 shared
fc2/22                               16       4.0 dedicated
```

```
fc2/23                                16       4.0 dedicated
fc2/24                                16       4.0 dedicated
```

Related Commands

Command	Description
show module	Verifies the status of a module.

show port-security

To display configured port security feature information, use the **show port-security database** command.

show port-security {**database** [**active** [**vsan** *vsan-id*]]|**fwwn** *fwwn-id* **vsan** *vsan-id*|**interface** {**fc** *slot/port*|**port-channel** *port*} **vsan** *vsan-id*|**vsan** *vsan-id*|**pending** [**vsan** *vsan-id*]|**pending-diff** [**vsan** *vsan-id*]|**statistics** [**vsan** *vsan-id*]|**status** [**vsan** *vsan-id*]|**violations** [{**last** *count*|**vsan** *vsan-id*}]}

Syntax Description

database	Displays database-related port security information.
active	(Optional) Displays the activated database information.
vsan *vsan-id*	(Optional) Displays information for the specified database.
fwwn *fwwn-id*	(Optional) Displays information for the specified fabric WWN.
interface	(Optional) Displays information for an interface.
fc *slot/port*	Displays information for the specified Fibre Channel interface.
port-channel *port*	Displays information for the specified PortChannel interface. The range is 1 to 128.
pending	Displays the server address pending configuration.
pending-diff	Displays the server address pending configuration differences with the active configuration.
statistics	Displays port security statistics.
status	Displays the port security status on a per VSAN basis.
violations	Displays violations in the port security database.
last count	(Optional) Displays the last number of lines in the database. The range is 1 to 100.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.
2.0(x)	Added the pending and pending-diff keywords.

Usage Guidelines

The access information for each port can be individually displayed. If you specify the FWWN or interface options, all devices that are paired in the active database (at that point) with the given FWWN or the interface are displayed.

The **show port-security** command issued with the **last** *number* option displays only the specified number of entries that appear first.

Examples

The following example displays the contents of the port security database:

```
switch# show port-security database
-------------------------------------------------------------------------------------
VSAN   Logging-in Entity             Logging-in Point  (          Interface)
-------------------------------------------------------------------------------------
1      21:00:00:e0:8b:06:d9:1d(pwwn)  20:0d:00:05:30:00:95:de(fc1/13)
1      50:06:04:82:bc:01:c3:84(pwwn)  20:0c:00:05:30:00:95:de(fc1/12)
2      20:00:00:05:30:00:95:df(swwn)  20:0c:00:05:30:00:95:de(port-channel 128)
3     20:00:00:05:30:00:95:de(swwn)  20:01:00:05:30:00:95:de(fc1/1)
[Total 4 entries]
```

The following example displays the output of the active port security database in VSAN 1:

```
switch# show port-security database vsan 1
-------------------------------------------------------------------------------
Vsan   Logging-in Entity             Logging-in Point        (Interface)
-------------------------------------------------------------------------------
1                 *                  20:85:00:44:22:00:4a:9e (fc3/5)
1      20:11:00:33:11:00:2a:4a(pwwn)  20:81:00:44:22:00:4a:9e (fc3/1)
[Total 2 entries]
```

The following example displays the active database.

```
switch# show port-security database active
-------------------------------------------------------------------------------------
VSAN   Logging-in Entity             Logging-in Point  (          Interface)    Learnt
-------------------------------------------------------------------------------------
1      21:00:00:e0:8b:06:d9:1d(pwwn)  20:0d:00:05:30:00:95:de(fc1/13)                 Yes
1      50:06:04:82:bc:01:c3:84(pwwn)  20:0c:00:05:30:00:95:de(fc1/12)                 Yes
2      20:00:00:05:30:00:95:df(swwn)  20:0c:00:05:30:00:95:de(port-channel 128)
       Yes
3     20:00:00:05:30:00:95:de(swwn)  20:01:00:05:30:00:95:de(fc1/1)
[Total 4 entries]
```

The following example displays the wildcard fwwn port security in VSAN 1:

```
switch# show port-security database fwwn 20:85:00:44:22:00:4a:9e vsan 1
Any port can login thru' this fwwn
```

The following example displays the configured FWWN port security in VSAN 1:

```
switch# show port-security database fwwn 20:01:00:05:30:00:95:de vsan 1
20:00:00:0c:88:00:4a:e2(swwn)
```

The following example displays the interface port information in VSAN 2:

```
switch# show port-security database interface fc 1/1 vsan 2
20:00:00:0c:88:00:4a:e2(swwn)
```

The following example displays the port security statistics:

```
switch# show port-security statistics
Statistics For VSAN: 1
-----------------------
Number of pWWN permit: 2
```

```
Number of nWWN permit: 2
Number of sWWN permit: 2
Number of pWWN deny  : 0
Number of nWWN deny  : 0
Number of sWWN deny  : 0
Total Logins permitted  : 4
Total Logins denied     : 0
Statistics For VSAN: 2
------------------------
Number of pWWN permit: 0
Number of nWWN permit: 0
Number of sWWN permit: 2
Number of pWWN deny  : 0
Number of nWWN deny  : 0
Number of sWWN deny  : 0
...
```

The following example displays the status of the active database and the autolearn configuration:

```
switch# show port-security status
VSAN 1 :Activated database, auto-learning is enabled
VSAN 2 :No Active database, auto-learning is disabled
...
```

The following example displays the previous 100 violations:

```
switch# show port-security violations
-------------------------------------------------------------------------------------------
VSAN  Interface    Logging-in Entity        Last-Time       [Repeat count]
-------------------------------------------------------------------------------------------
1  fc1/13    21:00:00:e0:8b:06:d9:1d(pwwn)        Jul  9 08:32:20 2003       [20]
      20:00:00:e0:8b:06:d9:1d(nwwn)
1  fc1/12    50:06:04:82:bc:01:c3:84(pwwn)        Jul  9 08:32:20 2003       [1]
      50:06:04:82:bc:01:c3:84(nwwn)
2  port-channel 1  20:00:00:05:30:00:95:de(swwn)  Jul  9 08:32:40 2003                [1]
[Total 2 entries]
```

Related Commands

Command	Description
port-security	Configures port security parameters.

show process creditmon credit-loss-event-history

To display the credit loss event history, use the **show processes creditmon credit-loss-event-history** command.

show process creditmon credit-loss-event-history module module-number

Syntax Description

module	Displays credit loss event history for a module.
module-number	Displays the module number.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(1)	This command is not supported for new MDS NG products but no changes made for the old MDS.
NX-OS 5.x	This command was introduced.

Usage Guidelines

None.

Examples

The following examples displays the credit loss event history for a module:

```
switch# show process creditmon credit-loss-event-history module 1
switch#
```

The following examples displays the credit loss event history:

```
switch# show process creditmon credit-loss-event-history
Module: 01
Module: 02
Module: 03
Module: 04
CLI is not supported on module 5
Module: 06
Module: 07
```

Related Commands

Command	Description
show process creditmon credit-loss-events	Displays the credit loss information.

show process creditmon credit-loss-events

To display the credit loss events information, use the **show processes creditmon credit-loss-events** command.

show process creditmon credit-loss-events module module-number

Syntax Description

module	Displays credit loss events information for a module.
module-number	Displays the module number.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(9)	This command is supported in MDS NG products but no changes made for the old MDS.
6.2(1)	This command is not supported for new MDS NG products but no changes made for the old MDS.
NX-OS 5.x	This command was introduced.

Usage Guidelines

In Cisco MDS 9710, 9706, 9250i and 9148S Series Switches, this command can be executed from configuration terminal mode itself. There are no changes in the old MDS, attach the module and execute the command.

Examples

The following examples displays the credit loss events information for a module:

```
switch# show process creditmon credit-loss-events module 9
Module: 09      Credit Loss Events: NO
switch#
```

The following examples displays the credit loss events information for a module:

Related Commands

Command	Description
show process creditmon credit-loss-event-history	Displays the credit monitor event history information.

show process creditmon event-history

To display the credit monitor event history information, use the **show processes creditmon event-history** command.

show process creditmon event-history

Syntax Description

This command has no argument or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(9)	This command is supported for new MDS NG products but no changes made for the old MDS.
6.2(1)	This command is not supported for new MDS NG products but no changes made for the old MDS.
NX-OS 5.x	This command was introduced.

Usage Guidelines

None.

Examples

The following examples displays the credit monitor event history information:

switch# attach module 2

```
switch# show process creditmon credit event-history
1) Event:CREDITMON_EVENT_MONITOR_OFF, length:4, at 10202 usec
s after Tue Apr 16 00:06:05 2013
interface =
2) Event:CREDITMON_EVENT_MONITOR_OFF, length:4, at 10199 usec
s after Tue Apr 16 00:06:05 2013
interface =
3) Event:CREDITMON_EVENT_MONITOR_OFF, length:4, at 10197 usec
s after Tue Apr 16 00:06:05 2013
interface =
4) Event:CREDITMON_EVENT_MONITOR_OFF, length:4, at 10194 usec
s after Tue Apr 16 00:06:05 2013
interface =
Module: 09      Credit Loss Events: NO
switch#
```

Related Commands

Command	Description
show process creditmon credit-loss-events	Displays the credit loss event information.

show process creditmon slowport-monitor-events

To display the credit monitor slow port statistics information, use the **show process** creditmon slowport-monitor-events command.

show process creditmon slowport-monitor-events module module-number

Syntax Description

module	Displays slowport monitor events for a module.
module-number	Displays the module number.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(9)	This command was introduced.

Usage Guidelines

None.

Examples

The following examples displays the creditmon slowport monitor statistics information for platform MDS 9710, 9706, 9250i and MDS 9148S:

```
switch# show process creditmon slowport-monitor-events
Module: 01 Slowport Detected: YES
================================================================================
Interface = fc1/37
----------------------------------------------------------------
| admin | slowport | oper | Timestamp |
| delay | detection | delay | |
| (ms) | count | (ms) | |
----------------------------------------------------------------
| 1 | 2 | 4 | 1. Mon Jun 30 16:19:06.068 2014 |
----------------------------------------------------------------
================================================================================
Interface = fc1/39
----------------------------------------------------------------
| admin | slowport | oper | Timestamp |
| delay | detection | delay | |
| (ms) | count | (ms) | |
----------------------------------------------------------------
| 1 | 2 | 4 | 1. Thu Jul 3 11:26:15.876 2014 |
----------------------------------------------------------------
================================================================================
Interface = fc1/40
----------------------------------------------------------------
| admin | slowport | oper | Timestamp |
| delay | detection | delay | |
| (ms) | count | (ms) | |
----------------------------------------------------------------
```

```
| 1 | 2 | 2 | 1. Thu Jul 3 11:26:15.537 2014 |
-----------------------------------------------------------------
```

Related Commands

Command	Description
system timeout slowport-monitor	Configures the system timeout values for the hardware slow port monitoring.

show process creditmon txwait-history

To display the TxWait history information of a physical device hardware, use the **show process creditmon txwait-history** command.

show process creditmon txwait-history [**module** **number**[**port** **number**]]

Syntax Description

module *number*	(Optional) Species a module number.
port *number*	(Optional) Specifies a port number.

Command Default

Displays the TxWait history information of a physical device hardware.

Command Modes

Privileged EXEC (#)

Release	Modification
5.x	This command was introduced.

Usage Guidelines

Examples

This example displays the transmit-wait history graph for 16-Gbps modules:

```
switch# show process creditmon txwait-history module 1 port 19

TxWait history for port fc1/19:
==============================
     9999999999999999999999999999999999999999999999999999999999999999
     2222222212222222222221222222122222212222222222222222222222212
     4434444580444424445545544547445549434053544443431444443445 4
1000
 900 ############################################################
800 ############################################################
700 ############################################################
600 ############################################################
500 ############################################################
400 ############################################################
300 ############################################################
200 ############################################################
100 ############################################################
    0....5....1....1....2....2....3....3....4....4....5....5....6
              0    5    0    5    0    5    0    5    0    5    0

          Tx Credit Not Available per second (last 60 seconds)
                 # = TxWait (ms)

   55555554
   5552222200000000000000000000000000000000000000000000000000000
   ............................................................
   4302222900000000000000000000000000000000000000000000000000000
60
54 #######
48 #######
42 ########
```

```
36 ########
30 ########
24 ########
18 ########
12 ########
 6 ########
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0

          Tx Credit Not Available per minute (last 60 minutes)
                 # = TxWait (secs)
```

```
     000000000000000000000000000000000000000000000000000000000000000000000000000000000000
3600
3240
2880
2520
2160
1800
1440
1080
 720
 360
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7.7
              0    5    0    5    0    5    0    5    0    5    0    5    0 2

          Tx Credit Not Available per hour (last 72 hours)
                 # = TxWait (secs)
```

Command	Description
show hardware	Displays information of the physical device hardware.

show processes

To display general information about all the processes, use the **show processes** command.

show processes [{**cpu**|**log** [{**details**|**pid process-id**}]|**memory**}]

Syntax Description

cpu	(Optional) Displays processes CPU information.
log	(Optional) Displays information about process logs.
details	(Optional) Displays detailed process log information.
pid *process-id*	(Optional) Displays process information about a specific process ID. The range is 0 to 2147483647.
memory	(Optional) Displays processes memory information.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following examples display general information about system processes:

```
switch# show process
PID    State  PC        Start_cnt    TTY   Process
-----  -----  --------  -----------  ----  -------------
  868      S  2ae4f33e            1     -  snmpd
  869      S  2acee33e            1     -  rscn
  870      S  2ac36c24            1     -  qos
  871      S  2ac44c24            1     -  port-channel
  872      S  2ac7a33e            1     -  ntp
    -     ER         -            1     -  mdog
    -     NR         -            0     -  vbuilder
PID: process ID.
State: process state
        D   uninterruptible sleep (usually IO)
        R   runnable (on run queue)
        S   sleeping
        T   traced or stopped
        Z   a defunct ("zombie") process
 NR  not-running
 ER  should be running but currently not-running
PC: Current program counter in hex format
Start_cnt: how many times a process has been started.
TTY: Terminal that controls the process. A "-" usually means a daemon not
     running on any particular tty.
```

```
Process: name of the process.

=====================================================
2. show processes cpu (new output)
Description: show cpu utilization information about the processes.
switch# show processes cpu
PID    Runtime(ms)  Invoked   uSecs  1Sec   Process
-----  -----------  --------  -----  -----  -----------
  842         3807    137001     27    0.0  sysmgr
 1112         1220     67974     17    0.0  syslogd
 1269          220     13568     16    0.0  fcfwd
 1276         2901     15419    188    0.0  zone
 1277          738     21010     35    0.0  xbar_client
 1278         1159      6789    170    0.0  wwn
 1279          515     67617      7    0.0  vsan
Runtime(ms): cpu time the process has used, expressed in milliseconds
Invoked: Number of times the process has been invoked.
uSecs:   Microseconds of CPU time in average for each process invocation.
1Sec:    CPU utilization in percentage for the last 1 second.
=====================================================
3. show processes mem
Description: show memory information about the processes.
PID    MemAlloc  StackBase/Ptr      Process
-----  --------  -----------------  ----------------
 1277    120632  7ffffcd0/7fffefe4  xbar_client
 1278     56800  7ffffce0/7ffffb5c  wwn
 1279   1210220  7ffffce0/7ffffbac  vsan
 1293    386144  7fffcf0/7fffebd4  span
 1294   1396892  7ffffce0/7fffdff4  snmpd
 1295    214528  7fffcf0/7ffff904  rscn
 1296     42064  7ffffce0/7ffffb5c  qos
MemAlloc: total memory allocated by the process.
StackBase/Ptr: process stack base and current stack pointer in hex format
=====================================================
3. show processes log
Description: list all the process logs
switch# show processes log
Process           PID     Normal-exit  Stack-trace  Core     Log-create-time
----------------  ------  -----------  -----------  -------  ---------------
fspf              1339             N            Y        N  Jan  5 04:25
lichen               1559             N            Y        N  Jan  2 04:49
rib               1741             N            Y        N  Jan  1 06:05
Normal-exit: whether or not the process exited normally.
Stack-trace: whether or not there is a stack trace in the log.
Core: whether or not there exists a core file.
Log-create-time: when the log file got generated.
```

The following example displays the detail log information about a particular process:

```
switch# show processes log pid 1339
Service: fspf
Description: FSPF Routing Protocol Application
Started at Sat Jan  5 03:23:44 1980 (545631 us)
Stopped at Sat Jan  5 04:25:57 1980 (819598 us)
Uptime: 1 hours 2 minutes 2 seconds
Start type: SRV_OPTION_RESTART_STATELESS (23)
Death reason: SYSMGR_DEATH_REASON_FAILURE_SIGNAL (2)
Exit code: signal 9 (no core)
CWD: /var/sysmgr/work
Virtual Memory:
    CODE      08048000 - 0809A100
    DATA      0809B100 - 0809B65C
    BRK       0809D988 - 080CD000
    STACK     7FFFFD20
```

```
    TOTAL     23764 KB
Register Set:
    EBX 00000005         ECX 7FFFF8CC         EDX 00000000
    ESI 00000000         EDI 7FFFF6CC         EBP 7FFFF95C
    EAX FFFFFDFE         XDS 8010002B         XES 0000002B
    EAX 0000008E (orig)  EIP 2ACE133E         XCS 00000023
    EFL 00000207         ESP 7FFFF654         XSS 0000002B
Stack: 1740 bytes. ESP 7FFFF654, TOP 7FFFFD20
0x7FFFF654: 00000000 00000008 00000003 08051E95 ................
0x7FFFF664: 00000005 7FFFF8CC 00000000 00000000 ................
0x7FFFF674: 7FFFF6CC 00000001 7FFFF95C 080522CD ........\....".."
0x7FFFF684: 7FFFF9A4 00000008 7FFFFC34 2AC1F18C ........4......*
```

show qos

To display the current QoS settings along with a the number of frames marked high priority, use the **show qos** command.

show qos {**class-map** [**name** *class-name*]|**dwrr**|**policy-map** [**name** *policy-name*]|**service policy** [{**interface fc** *slot / port*|**vsan** *vsan-id*}]|**statistics**}

Syntax Description

class-map	Displays QoS class maps.
name *class-name*	(Optional) Specifies a class map name. The maximum length is 63 alphanumeric characters.
dwrr	Displays deficit weighted round robin queue weights.
policy-map	Displays QoS policy-maps.
name *policy-name*	(Optional) Specifies a policy map name. The maximum length is 63 alphanumeric characters.
service policy	Displays QoS service policy associations.
interface fc *slot*/*port*	(Optional) Specifies a Fibre Channel interface.
vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is 1 to 4093.
statistics	Displays QoS related statistics.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

To access all but the **statistics** option for this command, you must perform the **qos enable** command.

Examples

The following example displays the contents of all class maps:

```
switch# show qos class-map
qos class-map MyClass match-any
    match dest-wwn 20:01:00:05:30:00:28:df
    match src-wwn 23:15:00:05:30:00:2a:1f
    match src-intf fc2/1
qos class-map Class2 match-all
    match src-intf fc2/14
qos class-map Class3 match-all
    match src-wwn 20:01:00:05:30:00:2a:1f
```

The following example displays the contents of a specified class map:

```
switch# show qos class-map name MyClass
qos class-map MyClass match-any
    match dest-wwn 20:01:00:05:30:00:28:df
    match src-wwn 23:15:00:05:30:00:2a:1f
    match src-intf fc2/1
```

The following example displays all configured policy maps:

```
switch# show qos policy-map
qos policy-map MyPolicy
    class MyClass
    priority medium
qos policy-map Policy1
    class Class2
    priority low
```

The following example displays a specified policy map:

```
switch# show qos policy-map name MyPolicy
qos policy-map MyPolicy
    class MyClass
        priority medium
```

The following example displays scheduled DWRR configurations:

```
switch# show qos dwrr
qos dwrr-q high weight 50
qos dwrr-q medium weight 30
qos dwrr-q low weight 20
```

The following example displays all applied policy maps:

```
switch# show qos service policy
qos service policy MyPolicy vsan 1
qos service policy Policy1 vsan 4
```

The following example displays QoS statistics:

```
switch# show qos statistics
Total number of FC frames transmitted from the Supervisor= 301431
Number of highest-priority FC frames transmitted         = 137679
Current priority of FC control frames = 7    (0 = lowest; 7 = highest)
```

show radius

To display the RADIUS Cisco Fabric Services (CFS) distribution status and other details, use the **show radius** command.

show radius {**distribution status**|**pending**|**pending-diff**}

Syntax Description

distribution status	Displays the status of the RADIUS CFS distribution.
pending	Displays the pending configuration that is not yet applied.
pending-diff	Displays the difference between the active configuration and the pending configuration.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the RADIUS distribution status:

```
switch# show radius distribution status
session ongoing: no
session db: does not exist
merge protocol status: merge activation done
last operation: none
last operation status: none
```

Related Commands

Command	Description
radius distribute	Enables RADIUS CFS distribution.

show radius-server

To display all configured RADIUS server parameters, use the **show radius-server** command.

show radius-server [{*server-nameipv4-addressipv6-address*}] [{**directed-request**|**groups**|**sorted**|**statistics**}]

Syntax Description

server-name	(Optional) Specifies the RADIUS server DNS name. The maximum character size is 256.
ipv4-address	(Optional) Specifies the RADIUS server IP address in the format *A.B.C.D* .
ipv6-address	(Optional) Specifies the RADIUS server IP address in the format *X:X::X* .
directed-request	(Optional) Displays an enabled directed request RADIUS server configuration.
groups	(Optional) Displays configured RADIUS server group information.
sorted	(Optional) Displays RADIUS server information sorted by name.
statistics	(Optional) Displays RADIUS statistics for the specified RADIUS server.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	• Added the *server-name* , *ipv4-address* , and *ipv6-address* arguments. • Added the **directed-request** and **statistics** options.

Usage Guidelines

Only administrators can view the RADIUS preshared key.

Examples

The following example shows the output of the **show radius-server** command:

```
switch# show radius-server

Global RADIUS shared secret:Myxgqc
retransmission count:5
timeout value:10
following RADIUS servers are configured:
        myradius.cisco.users.com:
                available for authentication on port:1812
                available for accounting on port:1813
        172.22.91.37:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:23MHcUnD
        10.10.0.0:
                available for authentication on port:1812
```

```
            available for accounting on port:1813
RADIUS shared secret:hostkey----> for administrators only
```

show rlir

To display the information about Registered Link Incident Report (RLIR), Link Incident Record Registration (LIRR), and Distribute Registered Link Incident Record (DRLIR) frames, use the **show rlir** command.

show rlir {**erl** [**vsan** *vsan-id*]|**history**|**recent** [{**interface fc** *slot/port*|**portnumber** *port-number*}]|**statistics** [**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

erl	Displays Established Registration List (ERL) information.
vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is 1 to 4093.
history	Displays link incident history.
recent	Displays recent link incident.
interface	(Optional) Specifies an interface.
fc *slot/port*	(Optional) Specifies a Fibre Channel interface on a Cisco MDS 9000 Family Switch.
bay *port* | **ext** *port* }	Specifies a Fibre Channel interface on a Cisco MDS 9124 Fabric Switch, a Cisco Fabric Switch for HP c-Class BladeSystem, and a Cisco Fabric Switch for IBM BladeCenter.
portnumber *port-number*	(Optional) Specifies a port number for the link incidents. The range is 1 to 224.
statistics	Displays RLIR statistics.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(2)	This command was introduced.
3.0(3)	Modified the **show rlir erl** command.
3.1(2)	Added the **bay** *port* | **ext** *port* keywords and arguments.

Usage Guidelines

If available, the host timestamp (marked by the *) is printed along with the switch timestamp. If the host timestamp is not available, only the switch timestamp is printed.

Examples

The following example displays the RLIR statistics for all VSANs:

```
switch# show rlir statistics
Statistics for VSAN: 1
-----------------------
Number of LIRR received      = 0
Number of LIRR ACC sent      = 0
Number of LIRR RJT sent      = 0
Number of RLIR sent          = 0
Number of RLIR ACC received  = 0
Number of RLIR RJT received  = 0
Number of DRLIR received     = 0
Number of DRLIR ACC sent     = 0
Number of DRLIR RJT sent     = 0
Number of DRLIR sent         = 0
Number of DRLIR ACC received = 0
Number of DRLIR RJT received = 0
Statistics for VSAN: 4
-----------------------
Number of LIRR received      = 0
Number of LIRR ACC sent      = 0
Number of LIRR RJT sent      = 0
Number of RLIR sent          = 0
Number of RLIR ACC received  = 0
Number of RLIR RJT received  = 0
Number of DRLIR received     = 0
Number of DRLIR ACC sent     = 0
Number of DRLIR RJT sent     = 0
Number of DRLIR sent         = 0
Number of DRLIR ACC received = 0
Number of DRLIR RJT received = 0
Statistics for VSAN: 61
-----------------------
Number of LIRR received      = 0
Number of LIRR ACC sent      = 0
Number of LIRR RJT sent      = 0
Number of RLIR sent          = 0
Number of RLIR ACC received  = 0
Number of RLIR RJT received  = 0
Number of DRLIR received     = 0
Number of DRLIR ACC sent     = 0
Number of DRLIR RJT sent     = 0
Number of DRLIR sent         = 0
Number of DRLIR ACC received = 0
Number of DRLIR RJT received = 0
```

The following example displays the RLIR statistics for a specified VSAN:

```
switch# show rlir statistics vsan 4
Statistics for VSAN: 4
-----------------------
Number of LIRR received      = 0
Number of LIRR ACC sent      = 0
Number of LIRR RJT sent      = 0
Number of RLIR sent          = 0
Number of RLIR ACC received  = 0
Number of RLIR RJT received  = 0
Number of DRLIR received     = 0
Number of DRLIR ACC sent     = 0
Number of DRLIR RJT sent     = 0
Number of DRLIR sent         = 0
```

```
Number of DRLIR ACC received = 0
Number of DRLIR RJT received = 0
```

The following example displays the RLIR statistics for all ERLs:

```
switch# show rlir erl
Established Registration List for VSAN: 2
-------------------------------------------
FC-ID       LIRR FORMAT    REGISTERED FOR
-------------------------------------------
0x0b0200    0x18           always receive
Total number of entries = 1
Established Registration List for VSAN: 100
-------------------------------------------
FC-ID       LIRR FORMAT    REGISTERED FOR
-------------------------------------------
0x0b0500    0x18           conditional receive
0x0b0600    0x18           conditional receive
Total number of entries = 2
```

The following example displays the ERLs for the specified VSAN:

```
switch# show rlir erl vsan 100
Established Registration List for VSAN: 100
-------------------------------------------
FC-ID       LIRR FORMAT    REGISTERED FOR
-------------------------------------------
0x0b0500    0x18           conditional receive
0x0b0600    0x18           conditional receive
Total number of entries = 2
```

The following example displays the RLIR preferred host configuration:

```
switch# show rlir erl
Established Registration List for VSAN: 5
-------------------------------------------
FC-ID       LIRR FORMAT     REGISTERED FOR
-------------------------------------------
0x772c00    0x18            conditional receive(*)
0x779600    0x18            conditional receive
0x779700    0x18            conditional receive
0x779800    0x18            conditional receive
Total number of entries = 4
(*) - Denotes the preferred host
```

The following example displays the RLIR history.

```
switch# show rlir history
Link incident history
-----------------------------------------------------------------------------------------------
 Host Time Stamp         Switch Time Stamp       VSAN   Domain   Port    Intf        Link
Incident Loc/Rem
-----------------------------------------------------------------------------------------------
 Sep 20 12:42:44 2006    Sep 20 12:42:44 2006    ****    ****    0x0b    fc1/12      Loss
of sig/sync LOC
 Reported Successfully to: [0x640001] [0x640201]
 Sep 20 12:42:48 2006    Sep 20 12:42:48 2006    ****    ****    0x0b    fc1/12      Loss
of sig/sync LOC
 Reported Successfully to: [0x640001] [0x640201]
 *** ** **:**:** ****    Sep 20 12:42:51 2006    1001    230     0x12    ****        Loss
of sig/sync REM
 Reported Successfully to: [0x640001] [0x640201]
```

```
 Sep 20 12:42:55 2006    Sep 20 12:42:55 2006    ****    ****    0x0b    fc1/12      Loss
of sig/sync LOC
 Reported Successfully to: None [No Registrations]
 *** ** **:**:** ****    Sep 20 12:45:56 2006    1001    230     0x12    ****        Loss
of sig/sync REM
 Reported Successfully to: None [No Registrations]
 *** ** **:**:** ****    Sep 20 12:45:56 2006    1001    230     0x12    ****        Loss
of sig/sync REM
 Reported Successfully to: None [No Registrations]
 Sep 20 12:52:45 2006    Sep 20 12:52:45 2006    ****    ****    0x0b    fc1/12      Loss
of sig/sync LOC
 Reported Successfully to: None [No Registrations]
 **** - Info not required/unavailable
```

The following example displays recent RLIRs for a specified interface:

```
switch# show rlir recent interface fc1/1-4
Recent link incident records
-------------------------------------------------------------------------------
Host Time Stamp          Switch Time Stamp        Port Intf   Link Incident
-------------------------------------------------------------------------------
Thu Dec 4 05:02:29 2003  Wed Dec 3 21:02:56 2003   2   fc1/2  Implicit Incident
Thu Dec 4 05:02:54 2003  Wed Dec 3 21:03:21 2003   4   fc1/4  Implicit Incident
```

The following example displays the recent RLIRs for a specified port number.

```
switch# show rlir recent portnumber 1-4
Recent link incident records
-------------------------------------------------------------------------------
Host Time Stamp          Switch Time Stamp        Port Intf    Link Incident
-------------------------------------------------------------------------------
Thu Dec 4 05:02:29 2003  Wed Dec 3 21:02:56 2003   2   fc1/2   Implicit Incident
Thu Dec 4 05:02:54 2003  Wed Dec 3 21:03:21 2003   4   fc1/4   Implicit Incident
```

show rmon

To display the remote monitoring (RMON) configuration or onboard log, use the **show rmon** command.

show rmon {**alarms**|**events**|**hcalarms**|**logs**}

Syntax Description

alarms	Displays the configured 32-bit RMON alarms.
events	Displays the configured RMON events.
hcalarms	Displays the configured 64-bit high-capacity (HC) RMON alarms.
logs	Displays the RMON event logs.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
2.0(x)	This command was introduced.
2.1(2)	Added the **logs** option.
3.0(1)	Added the **hcalarms** option.

Usage Guidelines

None.

Examples

The following example displays the configured RMON alarms:

```
switch# show rmon alarms
Alarm 20 is active, owned by test
Monitors 1.3.6.1.2.1.2.2.1.16.30 every 30 second(s)
 Taking delta samples, last value was 17
 Rising threshold is 15, assigned to event 1
 Falling threshold is 0, assigned to event 0
 On startup enable rising or falling alarm
```

The following example displays the configured RMON events:

```
switch# show rmon events
Event 4 is active, owned by administrator@london_op_center
Description is WARNING(4)
Event firing causes log and trap to community public, last fired 03:32:43
```

The following example displays the configured high-capacity RMON alarms:

```
switch# show rmon hcalarms
High Capacity Alarm 1 is active, owned by cseSysCPUUtilization.0@test
 Monitors 1.3.6.1.4.1.9.9.305.1.1.1.0 every 10 second(s)
 Taking absolute samples, last value was 0
```

```
 Rising threshold is 60, assigned to event 4
 Falling threshold is 59, assigned to event 4
 On startup enable rising alarm
 Number of Failed Attempts is 0
The following example displays the RMON event log located on the switch:
switch# show rmon logs
Event 4
    1 WARNING(4)Falling alarm 1, fired at 0 days 0:02:23 uptime
      iso.3.6.1.4.1.9.9.305.1.1.1.0=17 <= 59
Event 5
    1 INFORMATION(5)Startup Falling alarm 1, fired at 0 days 0:02:23 uptime
      iso.3.6.1.4.1.9.9.305.1.1.1.0=17 <= 59
    2 INFORMATION(5)Falling alarm 1, fired at 0 days 0:02:33 uptime
      iso.3.6.1.4.1.9.9.305.1.1.1.0=17 <= 59
```

Related Commands

Command	Description
rmon alarm	Configures the 32-bit RMON alarm.
rmon event	Configures an RMON event.
rmon hcalarm	Configures the 64-bit RMON alarm.
show snmp host	Displays the SNMP trap destination information.

show rmon status

To display the count of currently configured and maximum RMON alarm and hcalarm, use the **show rmon status** command.

show rmon status

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the count of currently configured and maximum RMON alarms and hcalarms:

```
switch# show rmon status
Maximum allowed 32 bit or 64 bit alarms : 512
Number of 32 bit alarms configured : 0
Number of 64 bit hcalarms configured : 0
```

Related Commands

Command	Description
show rmon alarms	Displays the RMON alarm table.
show rmon hcalarms	Displays the RMON hcalarm table.
show rmon events	Displays the RMON event table.
show rmon logs	Displays the RMON event log table.

show role

To display the description about the various Cisco SME role configurations, use the show role command.

show role

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.3(1a)	This command was introduced.
NX-OS 4.1(1c)	Changed the command output.

Usage Guidelines

Execute the setup sme command to set up the Cisco SME administrator and Cisco SME recovery roles and then use the show role command to display the role details.

Examples

The following example displays the Cisco SME role configurations:

```
switch# setup sme
Set up four roles necessary for SME, sme-admin, sme-stg-admin, sme-kmc-admin and
sme-rec-officer? (yes/no) [no] yes
SME setup done

switch# show role


Role: sme-admin
  Description: new role
  Vsan policy: permit (default)
  ----------------------------------------------
  Rule    Type    Command-type    Feature
  ----------------------------------------------
  1       permit  show            sme
  2       permit  config          sme
  3       permit  debug           sme

Role: sme-storage
  Description: new role
  Vsan policy: permit (default)
  ----------------------------------------------
  Rule    Type    Command-type    Feature
  ----------------------------------------------
  1       permit  show            sme-stg-admin
  2       permit  config          sme-stg-admin
  3       permit  debug           sme-stg-admin

Role: sme-kmc
  Description: new role
  Vsan policy: permit (default)
```

```
  ------------------------------------------------
  Rule    Type    Command-type    Feature
  ------------------------------------------------
  1       permit  show            sme-kmc-admin
  2       permit  config          sme-kmc-admin
  3       permit  debug           sme-kmc-admin

Role: sme-recovery
  Description: new role
  Vsan policy: permit (default)
  ------------------------------------------------
  Rule    Type    Command-type    Feature
  ------------------------------------------------
```

1 permit config sme-recovery-officer

Related Commands

Command	Description
setup sme	Sets up the Cisco SME administrator and Cisco SME recovery roles.

show role

To display roles (and their associated rules) configured on the switch, including those roles that have not yet been committed to persistent storage, use the **show role** command.

show role [{**name string**|**pending**|**pending-diff**|**session status**|**status**}]

Syntax Description

name string	(Optional) Specifies a name of the role.
pending	(Optional) Displays uncommitted role configuration for fabric distribution.
pending-diff	(Optional) Displays the differences between the pending configuration and the active configuration.
session status	(Optional) Displays the session status for a role.
status	(Optional) Displays the status of the latest Cisco Fabric Services (CFS) operation.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0(x)	Added the **pending**, **pending-diff**, **session**, and **status** options.

Usage Guidelines

The rules are displayed by rule number and are based on each role. All roles are displayed even if role name is not specified.

Only network-admin role can access this command.

Examples

The following example shows how to display information for all roles:

```
switch# show role

Role: network-admin
Description: Predefined Network Admin group. This role cannot be modified
Access to all the switch commands
Role: network-operator
Description: Predefined Network Operator group. This role cannot be modified
Access to Show commands and selected Exec commands
Role: svc-admin
Description: Predefined SVC Admin group. This role cannot be modified
Access to all SAN Volume Controller commands
Role: svc-operator
Description: Predefined SVC Operator group. This role cannot be modified
Access to selected SAN Volume Controller commands
Role: default-role
  Description: This is a system defined role and applies to all users
```

```
  vsan policy: permit (default)
  ----------------------------------------------
  Rule    Type    Command-type      Feature
  ----------------------------------------------
    1.   permit      show              system
    2.   permit      show                snmp
    3.   permit      show              module
    4.   permit      show            hardware
    5.   permit      show         environment
Role: sangroup
Description: SAN management group
--------------------------------------
Rule   Type   Command-type   Feature
--------------------------------------
  1.   permit    config           *
  2.     deny    config        fspf
  3.   permit     debug        zone
  4.   permit      exec      fcping
```

The following example displays the role session status:

```
switch# show role session status
Last Action                : None
Last Action Result         : None
Last Action Failure Reason : None
```

Related Commands

Command	Description
role abort	Enables authorization role CFS distribution.
role commit	Enables authorization role CFS distribution.
role distribute	Enables authorization role CFS distribution.
role name	Configures authorization roles.

show rscn

To display Registered State Change Notification (RSCN) information, use the **show rscn** command.

show rscn {**event-tov vsan vsan-id**|**pending vsan vsan-id**|**pending-diff vsan vsan-id**|**scr-table** [**vsan vsan-id**]|**statistics** [**vsan vsan-id**]}

Syntax Description

event-tov	Displays the event timeout value.
vsan vsan-id	Specifies a VSAN ID. The range is 1 to 4093.
pending	Displays the pending configuration.
pending-diff	Displays the difference between the active and the pending configuration.
scr-table	Displays the State Change Registration table.
statistics	Displays RSCN statistics.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **event-tov**, **pending**, and **pending-diff** options.

Usage Guidelines

The SCR table cannot be configured. It is only populated if one or more Nx ports send SCR frames to register for RSCN information. If the **show rscn scr-table** command does not return any entries, no Nx port is interested in receiving RSCN information.

Examples

The following example displays RSCN information:

```
switch# show rscn scr-table vsan 1
SCR table for VSAN: 1
---------------------------------------------
FC-ID         REGISTERED FOR
---------------------------------------------
0x1b0300      fabric detected rscns
Total number of entries = 1
```

The following example displays RSCN statistics.

```
switch# show rscn statistics vsan 1
Statistics for VSAN: 1
-------------------------
Number of SCR received         = 0
Number of SCR ACC sent         = 0
```

```
Number of SCR RJT sent         = 0
Number of RSCN received        = 0
Number of RSCN sent            = 0
Number of RSCN ACC received    = 0
Number of RSCN ACC sent        = 0
Number of RSCN RJT received    = 0
Number of RSCN RJT sent        = 0
Number of SW-RSCN received     = 0
Number of SW-RSCN sent         = 0
Number of SW-RSCN ACC received = 0
Number of SW-RSCN ACC sent     = 0
Number of SW-RSCN RJT received = 0
Number of SW-RSCN RJT sent     = 0
```

The following example shows the RSCN event timeout value configured on VSAN 1:

```
switch# show rscn event-tov vsan 1
Event TOV : 2000 ms
switch#
```

The following example shows the difference between the active RSCN configuration and the pending RSCN configuration on VSAN 1:

```
switch# show rscn pending-diff vsan 1
-  rscn event-tov 2000
+  rscn event-tov 20
switch#
```

show running radius

To display the RADIUS configuration, use the **show running radius** command.

show running radius all

Syntax Description

all	Displays running config with defaults.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(3)	Changed the command output.
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the RADIUS configuration:

```
switch# show running radius
version 4.1(3)
radius distribute
radius-server key 7 "fewhg"
radius-server timeout 1
radius-server retransmit 0
radius-server deadtime 1
radius-server host 10.10.1.1 authentication accounting
radius commit
aaa group server radius radius
switch#
The following example shows how to display the running config with defaults:
switch# show running radius all
version 4.1(3)
radius distribute
radius-server key 7 "fewhg"
radius-server timeout 1
radius-server retransmit 0
radius-server deadtime 1
radius-server host 10.10.1.1 auth-port 1812 acct-port 1813 authentication accoun
ting
radius-server host 10.10.1.1 test username test password test idle-time 0
radius commit
aaa group server radius radius
    server 10.10.1.1
    deadtime 0
switch#
```

Related Commands

Command	Description
radius distribute	Enables RADIUS CFS distribution.

show running-config

To display the running configuration file, use the **show running-config** command.

show running-config [{**diff**|**interface** [{**cpp**|**fc**|**fc** *slot/port*|**fc-tunnel** *tunnel-id*|**fcip** *fcip-number*|**gigabitethernet** *slot/port*|**iscsi** *slot/port*|**mgmt 0**|**port-channel**|**svc**|**vsan** *vsan-id*}]|**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

diff	(Optional) Displays the difference between the running and startup configurations.
interface	(Optional) Displays running configuration information for a range of interfaces.
cpp	(Optional) Displays the virtualization interface.
fc *slot*/*port*	(Optional) Specifies a Fibre Channel interface on a Cisco MDS 9000 Family Switch.
bay *port* | **ext** *port*	Specifies a Fibre Channel interface on a Cisco MDS 9124 Fabric Switch, a Cisco Fabric Switch for HP c-Class BladeSystem, and a Cisco Fabric Switch for IBM BladeCenter.
fc-tunnel *tunnel-id*	(Optional) Displays description of the specified FC tunnel from 1 to 4095.
fcip *fcip-number*	Displays the description of the specified FCIP interface from 1 to 255.
gigabitethernet *slot*/*port*	Displays the description of the Gigabit Ethernet interface in the specified slot and port.
iscsi *slot*/*port*	Displays the description of the iSCSI interface in the specified slot and port.
mgmt 0	Displays the description of the management interface.
port-channel	Displays the description of the PortChannel interface.
sup-fc	Displays the inband interface details.
svc	Displays the virtualization interface specific to the CSM module.
vsan *vsan-id*	Displays VSAN-specific information. The ID ranges from 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If the running configuration is different from the startup configuration, issue the **show startup-config diff** command to view the differences.

Examples

The following example displays the configuration currently running on the switch:

```
switch# show running-config

Building Configuration ...
 interface fc1/1
 interface fc1/2
 interface fc1/3
 interface fc1/4
 interface mgmt0
ip address 209.165.200.226 209.165.200.227
no shutdown
vsan database
boot system bootflash:isan-237; sup-1
boot kickstart bootflash:boot-237 sup-1
callhome
ip default-gateway 209.165.200.226
switchname switch
trunk protocol enable
username admin password 5 /AFDAMD4B2xK2  role network-admin
```

The following example displays the difference between the running configuration and the startup configuration:

```
switch# show running-config
 diff
Building Configuration ...
*** Startup-config
--- Running-config
***************** 1,16 ****
  fcip enable
  ip default-gateway 209.165.200.226
  iscsi authentication none
  iscsi enable
! iscsi import target fc
  iscsi virtual-target name vt
    pWWN 21:00:00:04:cf:4c:52:c1
  all-initiator-permit
--- 1,20 ----
  fcip enable
+ aaa accounting logsize 500
+
+
+
  ip default-gateway 209.165.200.226
  iscsi authentication none
  iscsi enable
! iscsi initiator name junk
  iscsi virtual-target name vt
    pWWN 21:00:00:04:cf:4c:52:c1
  all-initiator-permit
```

The following example displays running configuration information for a span destination interface—in this case, the management interface:

```
switch(config)# show running-config interface fc1/16
!Time: Tue Mar 26 22:52:27 2013
version 6.2(1)
interface fc1/1
  switchport speed 4000
  switchport mode SD
  no shutdown
switch(config)#
```

The following example displays running configuration information for a specified feature—in this case, VSANS:

```
switch# show running-config
 feature vsan
vsan database
vsan 2 suspend
vsan 3
vsan 4
vsan database
vsan 3 interface fc1/1
```

show running-config callhome

To display the Call Home configuration, use the show running-config callhome command.

show running-config callhome

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the Call Home configuration:

```
switch# show running-config callhome
version 5.0(1a)
callhome
transport email from isola-77@cisco.com
transport email reply-to someone@cisco.com
transport email smtp-server 72.163.129.201 port 1
transport email mail-server 10.64.74.94 port 25 priority 4
transport email mail-server 192.168.1.10 port 25 priority 50
transport email mail-server mail-server-1.cisco.com port 25 priority 100
switch#
```

Related Commands

Command	Description
callhome	Configures the Call Home function.

show running-config fcsp

To display the detailed run time information relevent to FC-SP, use the show running-config fcsp command.

show running-config fcsp

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the FC-SP details:

```
switch# show running-config fcsp
feature fcsp
fcsp esp sa 300
  key 0x00000000000000000000000000123456
  salt 0x123456
interface fc8/48
  fcsp off
  fcsp esp manual
    ingress-sa 300
    egress-sa 300version 4.1(2)
feature fcsp
fcsp esp sa 300
```

Related Commands

Command	Description
fcsp enable	Enables FC-SP.

show san-ext-tuner

To display SAN extension tuner information, use the **show san-ext-tuner** command.

show san-ext-tuner {**interface gigabitethernet** *slot / port* [**nport pwwn** *pwwn-id* **vsan** *vsan-id* **counters**]|**nports**}

Syntax Description

interface	Displays SAN extension tuner information for a specific Gigabit Ethernet interface.
gigabitethernet *slot*/*port*	Specifies a Gigabit Ethernet interface.
nport	(Optional) Specifies an N port.
pwwn *pwwn-id*	(Optional) Specifies a pWWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
vsan *vsan-id*	(Optional) Specifies a VSAN ID. The range is 1 to 4093.
counters	(Optional) Specifies SAN extension tuner counters.
nports	Displays SAN extension tuner information for all nports.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display SAN extension tuner N port information:

```
switch# show san-ext-tuner nports
```

Related Commands

Command	Description
san-ext-tuner	Enters SAN extension tuner configuration mode.

show santap module

To display the SANTap configuration on the Storage Services Module (SSM), use the **show santap module** command in EXEC mode.

show santap module slot {**avt** [{**name**|**brief**}]|**avtlun**|**cvt** [{**cvt-id**|**brief**}]|**dvt** [{**name**|**brief**}]|**dvtlun**|**rvt** [{**name**|**brief**}]|**rvtlun**|**session** [{**session-id**|**brief**}]|**tech-support**}

Syntax Description

slot	Displays SANTap configuration for a module in the specified slot.
avt	Displays the appliance virtual target (AVT) configuration.
name	(Optional) Specifies the user name.
brief	(Optional) Displays a brief format version of the display.
avtlun	Displays the appliance AVT LUN configuration.
cvt	Displays the control virtual target (CVT) configuration.
cvt-id	(Optional) Specifies a user configured CVT ID. The range is 1 to 65536.
dvt	Displays the data virtual target (DVT) configuration.
dvtlun	Displays the DVT LUN configuration.
rvt	Displays the remote virtual target (AVT) configuration.
rvtlun	Displays the RVT LUN configuration.
session	Displays the SANTap session information.
session-id	(Optional) Specifies a user configured session ID. The range is 1 to 65536.
tech-support	Displays information for technical support.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.
3.1(2)	Added the **tech-support** option.

Usage Guidelines

None.

Examples

The following example displays the SANTap AVT configuration:

```
switch# show santap module 2 avt
 AVT Information :
        avt pwwn     = 2a:4b:00:05:30:00:22:25
        avt nwwn     = 2a:60:00:05:30:00:22:25
        avt id       = 12
        avt vsan     = 4
        avt if_index = 0x1080000
        hi pwwn      = 21:00:00:e0:8b:07:61:aa
        tgt pwwn     = 22:00:00:20:37:88:20:ef
        tgt vsan     = 1
```

The following example displays the SANTap AVT LUN configuration:

```
switch# show santap module 2 avtlun
 AVT LUN Information :
        avt pwwn     = 2a:4b:00:05:30:00:22:25
        avt lun      = 0x0
        xmap id      = 16
        avt id       = 12
        tgt lun      = 0x0
```

The following example displays the SANTap CVT configuration:

```
switch# show santap module 2 cvt
 CVT Information :
        cvt pwwn     = 25:3c:00:05:30:00:22:25
        cvt nwwn     = 25:3d:00:05:30:00:22:25
        cvt id       = 1
        cvt xmap_id  = 2
        cvt vsan     = 10
```

The following example displays the SANTap DVT configuration:

```
switch# show santap module 2 dvt
 DVT Information :
        dvt pwwn     = 22:00:00:20:37:88:20:ef
        dvt nwwn     = 20:00:00:20:37:88:20:ef
        dvt id       = 3
        dvt mode     = 3
        dvt vsan     = 3
        dvt fp_port  = 0
        dvt if_index = 0x1080000
        dvt name     = MYDVT
```

The following example displays the SANTap DVT LUN configuration:

```
switch# show santap module 2 dvtlun
 DVT LUN Information :
        dvt pwwn     = 22:00:00:20:37:88:20:ef
        dvt lun      = 0x0
        xmap id      = 8
        dvt id       = 3
        dvt mode     = 0
        dvt vsan     = 3
        tgt pwwn     = 22:00:00:20:37:88:20:ef
        tgt lun      = 0x0
        tgt vsan     = 1
```

The following example displays the SANTap configuration session:

```
switch# show santap module 2 session
 Session Information :
        session id    = 1
        host pwwn     = 21:00:00:e0:8b:07:61:aa
        dvt pwwn      = 22:00:00:20:37:88:20:ef
        dvt lun       = 0x0
        tgt pwwn      = 00:00:00:00:00:00:00:00
        tgt lun       = 0x0
        adt pwwn      = 77:77:77:77:77:77:77:77
        adt lun       = 0x0
        num ranges    = 0
        dvt id        = 0
        vdisk id      = 0
        session state = 0
        mrl requested = 1
        pwl requested = 1
        iol requested = 0
```

The following example displays the SANTap RVT configuration:

```
switch# show santap module 2 rvt
 RVT Information :
        rvt pwwn     = 2a:61:00:05:30:00:22:25
        rvt nwwn     = 2a:62:00:05:30:00:22:25
        rvt id       = 17
        rvt vsan     = 4
        rvt if_index = 0x1080000
```

The following example displays the SANTap RVT LUN configuration:

```
switch# show santap module 2 rvtlun
 RVT LUN Information :
        rvt pwwn     = 2a:61:00:05:30:00:22:25
        rvt lun      = 0x0
        xmap id      = 22
        rvt id       = 17
        app pwwn     = 22:00:00:20:37:39:b1:00
        app lun      = 0x0
        app vsan     = 1
```

The following example displays information for technical support:

```
switch# show santap module 4 tech-support
 DVT Information :
        dvt pwwn     = 22:00:00:20:37:39:b1:00
        dvt nwwn     = 20:00:00:20:37:39:b1:00
        dvt id       = 0x83fe924
        dvt mode     = 3
        dvt vsan     = 1
        dvt if_index = 0x1180000
        dvt fp_port  = 1
        dvt name     = MYDVT3
        dvt tgt-vsan = 2
        dvt io timeout            = 10 secs
        dvt lun size handling     = 1
        dvt app iofail behaviour  = 0
        dvt quiesce behavior      = 0
        dvt tgt iofail behavior   = 0
        dvt appio failover time   = 0 secs
        dvt inq data behavior     = 0
 DVT Information :
        dvt pwwn     = 22:00:00:20:37:88:20:ef
```

```
        dvt nwwn     = 20:00:00:20:37:88:20:ef
        dvt id       = 0x8405bbc
        dvt mode     = 3
        dvt vsan     = 1
        dvt if_index = 0x1186000
        dvt fp_port  = 7
        dvt name     = MYDVT3
        dvt tgt-vsan = 2
        dvt io timeout            = 10 secs
        dvt lun size handling     = 1
        dvt app iofail behaviour  = 0
        dvt quiesce behavior      = 0
        dvt tgt iofail behavior   = 0
        dvt appio failover time   = 0 secs
        dvt inq data behavior     = 0
 DVT Information :
        dvt pwwn     = 22:00:00:20:37:39:87:70
        dvt nwwn     = 20:00:00:20:37:39:87:70
        dvt id       = 0x8405b2c
        dvt mode     = 3
        dvt vsan     = 3
        dvt if_index = 0x118c000
        dvt fp_port  = 13
        dvt name     = MYDVT3
        dvt tgt-vsan = 2
        dvt io timeout            = 10 secs
        dvt lun size handling     = 1
        dvt app iofail behaviour  = 0
        dvt quiesce behavior      = 0
        dvt tgt iofail behavior   = 0
        dvt appio failover time   = 0 secs
        dvt inq data behavior     = 0
 CVT Information :
        cvt pwwn     = 29:5d:33:33:33:33:33:36
        cvt nwwn     = 29:5e:33:33:33:33:33:36
        cvt id       = 0x83b11e4
        cvt xmap_id  = 0x83b1204
        cvt vsan     = 2
        cvt name     =
--------------------------------------------------------------------------
VSAN                 USAGE COUNT
--------------------------------------------------------------------------
2                    4
switch#
```

Table 11: show santap Field Descriptions, on page 1591 describes the significant fields shown in the previous displays.

Table 11: show santap Field Descriptions

Field	Description
app lun	Displays the appliance LUN.
app pwwn	Displays the appliance port world wide name.
app vsan	Displays the appliance VSAN number.
avt id	Displays the AVT ID number.
avt if_index	Displays the AVT interface index number.

Field	Description
avt lun	Displays the AVT LUN.
avt nwwn	Displays the AVT Node port world wide name.
avt pwwn	Displays the AVT port world wide name.
avt vsan	Displays the AVT VSAN number.
cvt id	Displays the CVT ID number.
cvt nwwn	Displays the CVT Node port world wide name.
cvt pwwn	Displays the CVT port world wide name.
cvt vsan	Displays the CVT VSAN number.
cvt xmap_id	Displays the CVT Xmap ID number.
dvt fp_port	Displays the DVT fabric port number.
dvt id	Displays the DVT.
dvt if_index	Displays the DVT interface index number.
dvt lun	Displays the DVT LUN.
dvt mode	Displays the DVT mode.
dvt name	Displays the DVT name.
dvt nwwn	Displays the DVT Node port world wide name.
dvt pwwn	Displays the DVT port world wide name.
dvt vsan	Displays the DVT VSAN number.
hi pwwn	Displays the <TBD> port world-wide name.
host pwwn	Displays the host port world wide name.
iol requested	Displays the <TBD> requested.
mrl requested	Displays the <TBD> requested.
num ranges	Displays the number ranges.
pwl requested	Displays the <TBD> requested.
rvt id	Displays the RVT ID number.
rvt if_index	Displays the RVT interface index.
rvt lun	Displays the RVT LUN.
rvt nwwn	Displays the RVT Node port world wide name.

Field	Description
rvt pwwn	Displays the RVT port world wide name.
rvt vsan	Displays the RVT VSAN number.
session id	Displays the session ID number.
session state	Displays the session state.
tgt lun	Displays the target LUN.
tgt pwwn	Displays the target port world wide name.
tgt vsan	Displays the target VSAN number.
vdisk id	Displays the virtual disk ID number.
xmap id	Displays the Xmap ID number.

Related Commands

Command	Description
santap module	Configures the mapping between the SSM and the VSAN where the appliance is configured.

show santap module dvt

To display the SANTap DVT configuration on the Storage Service Module (SSM), use the show santap module dvt command in the EXEC mode.

show santap module slot dvt {**name**|**brief**}

Syntax Description

slot	Specifies the module number. The range is from 1 to 9.
name	Specifies the user name for DVT.
brief	Displays SANTap DVT configuration in a brief format.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the SANTap DVT configuration:

```
switch# show santap module 2 dvt
DVT Information :
        dvt pwwn     = 22:00:00:20:37:88:20:ef
        dvt nwwn     = 20:00:00:20:37:88:20:ef
        dvt id       = 3
        dvt mode     = 3
        dvt vsan     = 3
        dvt fp_port  = 0
        dvt if_index = 0x1080000
        dvt name     = MYDVT
```

Related Commands

Command	Description
show santap vttbl	Displays the SANTap VTTBL configuration.

show santap module dvt brief

To display the SANTap Data Virtual Target (DVT) configuration in a brief format on the Storage Service Module (SSM), use the show santap module dvt brief command in the EXEC mode.

show santap module dvt brief slot

Syntax Description

slot	Displays SANTap configuration for a module in the specified slot.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the SANTap module DVT brief infomation for slot 13:

```
switch# show santap module 13 dvt brief
--------------------------------------------------------------------------------
DVT WWN                 DVT ID               MD  DVT VSAN    DVTIFIDX
--------------------------------------------------------------------------------
50:06:0e:80:00:c3:e0:46 139639316            3   30          0x1604000
switch# attach  module 13
Attaching to module 13 ...
To exit type 'exit', to abort type '$.'
Bad terminal type: "xterm". Will assume vt100.
```

The following example displays the SANTap VTTBL DVT configuration:

```
switch# attach module 2
module-3# show santap vttbl dvt 50:00:1f:e1:50:0c:3b:09
DVT Entry  :
        Activated        : FALSE
        Number LUNs     : 16
        Possible Hosts  :
             hi_pwwn = 10:00:00:00:c9:3f:90:21 : 4 LUNs
             hi_pwwn = 10:00:00:00:c9:4c:c0:e5 : 2 LUNs
             hi_pwwn = 21:00:00:e0:8b:0c:7d:21 : 2 LUNs
             hi_pwwn = 10:00:00:00:c9:56:ed:f2 : 2 LUNs
             hi_pwwn = 50:06:0b:00:00:60:2a:a0 : 4 LUNs
             hi_pwwn = 21:00:00:e0:8b:92:62:92 : 2 LUNs
```

The following example displays the SANTap vttbl DVT host configuration:

```
switch# show santap vttbl dvt 50:00:1f:e1:50:0c:3b:09 host 10:00:00:00:c9:3f:90:21
HI-LIST Entry  :
        State               : PRLI
        UA Power On         : 1
```

```
        FIT Created         : 1
        NVP Index           : 0x10000000c93f9021

    HI-LUNS Entry  :
        Number of LUNs    : 4
        DVT ID              : 0x83f978c
        HI Index            : 0
        LUNs Installed      : TRUE
        Target Lun, DVT Lun pairs :

        (0, 0)(1, 1)(2, 2)(3, 3)
```

Related Commands

Command	Description
show santap vttbl	Displays the SANTap VTTBL configuration.

show santap module dvtlun

To display the SANTap DVT LUN configuration on the Storage Service Module (SSM), use the show santap module dvt lun command in the EXEC mode.

show santap module slot dvtlun {**brief**|**dvt-pwwn**}

Syntax Description

slot	Specifies the module number. The range is from 1 to 9.
brief	Displays SANTap DVT LUN configuration in a brief format.
dvt-pwwn	Displays the DVT port world wide name (pWWN).

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the SANTap DVT LUN configuration:

```
switch# show santap module 2 dvtlun
 DVT LUN Information :
        dvt pwwn     = 22:00:00:20:37:88:20:ef
        dvt lun      = 0x0
        xmap id      = 8
        dvt id       = 3
        dvt mode     = 0
        dvt vsan     = 3
        tgt pwwn     = 22:00:00:20:37:88:20:ef
        tgt lun      = 0x0
        tgt vsan     = 1
```

Related Commands

Command	Description
show santap vttbl	Displays the SANTap VTTBL configuration.

show santap vttbl dvt

To display the SANTap VTTBL DVT configuration on the Storage Service Module (SSM), use the show santap vttbl dvt command in the EXEC mode.

show santap vttbl dvt dvt-pwwn

Syntax Description

vttbl	Displays SANtap VTTBL configuration.
dvt	Displays SANtap DVT configuration.
dvt-pwwn	Displays the DVT port world wide name (pWWN).

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the SANTap VTTBL DVT configuration:

```
switch# show santap vttbl dvt 50:00:1f:e1:50:0c:3b:09
DVT Entry  :
        Activated        : FALSE
        Number LUNs     : 16
        Possible Hosts  :
             hi_pwwn = 10:00:00:00:c9:3f:90:21 : 4 LUNs
             hi_pwwn = 10:00:00:00:c9:4c:c0:e5 : 2 LUNs
             hi_pwwn = 21:00:00:e0:8b:0c:7d:21 : 2 LUNs
             hi_pwwn = 10:00:00:00:c9:56:ed:f2 : 2 LUNs
             hi_pwwn = 50:06:0b:00:00:60:2a:a0 : 4 LUNs
             hi_pwwn = 21:00:00:e0:8b:92:62:92 : 2 LUNs
```

Related Commands

Command	Description
show santap vttbl	Displays the SANTap VTTVL configuration.

show santap vttbl dvt host

To display the SANTap VTTBL DVT host configuration on the Storage Service Module (SSM), use the show santap vttbl dvt host command in the EXEC mode.

show santap vttbl dvt dvt-pwwn host host-pwwn

Syntax Description

dvt-pwwn	Displays the DVT port world wide name (pWWN).
host pwwn	Displays the host pWWN.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the SANTap VTTBL DVT host configuration:

```
switch# show santap vttbl dvt 50:00:1f:e1:50:0c:3b:09 host 10:00:00:00:c9:3f:90:21
HI-LIST Entry  :
        State               : PRLI
        UA Power On         : 1
        FIT Created         : 1
        NVP Index           : 0x10000000c93f9021

    HI-LUNS Entry  :
        Number of LUNs    : 4
        DVT ID              : 0x83f978c
        HI Index            : 0
        LUNs Installed      : TRUE
        Target Lun, DVT Lun pairs :

        (0, 0)(1, 1)(2, 2)(3, 3)
```

Related Commands

Command	Description
show santap vttbl	Displays the SANTap VTTBL configuration.

show scheduler

To display command scheduler information, use the **show scheduler** command.

show scheduler {**config**|**job** [**name** *jobname*]|**logfile**|**schedule** [**name** *schedulename*]}

Syntax Description

config	Displays command scheduler configuration information.
job	Displays job information.
name *jobname*	(Optional) Restricts the output to a specific job name. Maximum length is 31 characters.
logfile	Displays the log file.
schedule	Displays schedule information.
name *schedulename*	(Optional) Restricts the output to a specific schedule name. Maximum length is 31 characters.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, the command scheduler must be enabled using the **scheduler enable** command.

Examples

The following example shows how to configure the e-mail transport:

```
switch# config t
   Enter configuration commands, one per line. End with CNTL/Z.
   switch(config)# scheduler transport email from sw2@sjtac.cisco.com
   switch(config)# scheduler transport email reply-to sw2@sjtac.cisco.com
   switch(config)# scheduler transport email smtp-server  13.7.3.2
```

The following example shows how to display the job information:

```
switch# show scheduler job name test_1
Job Name: test_1
----------------
config t
.81@ptEFACadmiQSAp8config t c====================================
==========================
switch#
```

The following example displays the command scheduler configuration information:

```
switch# show scheduler config
config terminal
```

```
  scheduler enable
end
```

The following example displays the command scheduler schedule information:

```
switch# show scheduler schedule configureVsan99
Schedule Name : configureVsan99
----------------------------------
User Name : admin
Schedule Type : Run once on Tue Aug 10 09:48:00 2004
Last Execution Time: Tue Aug 10 09:48:00 2004
-----------------------------------------------
Job Name       Status
-----------------------------------------------
addMemVsan99   Success (0)
```

The following example displays the command scheduler log file information:

```
switch# show scheduler logfile
Job Name : addMemVsan99 Job Status: Success (0)
Schedule Name : configureVsan99 User Name : admin
Completion time: Tue Aug 10 09:48:00 2004
-------------------------- Job Output --------------------------
'config terminal'
'vsan database'
'vsan 99 interface fc1/1'
'vsan 99 interface fc1/2'
'vsan 99 interface fc1/3'
'vsan 99 interface fc1/4'
```

The following example displays the command scheduler configuration information:

```
switch# show scheduler config
config terminal
  feature scheduler
  scheduler logfile size 16
  scheduler transport email from sw2@sjtac.cisco.com
  scheduler transport email reply-to  sw2@sjtac.cisco.com
  scheduler transport email smtp-server 13.7.3.2
end
config terminal
 scheduler job name backup_config
copy running-config startup-config
 show interface mgmt0
 copy startup-config tftp://13.7.3.2/

end
config terminal
  scheduler schedule name test
    time daily 11:23
    job name backup_config
    email-addr zawoo@cisco.com
end
config terminal
  scheduler schedule name te
    end
```

Related Commands

Command	Description
scheduler enable	Enables the command scheduler.

Command	Description
scheduler job name	Configures command scheduler jobs.
scheduler schedule name	Configures command schedules.

show scsi-flow

To display SCSI flow information, use the **show scsi-flow** command.

{**show scsi-flow** [**flow-id** *flow-id*]|**statistics** [**flow-id** *flow-id* **lun** *lun-number*]}

Syntax Description

flow-id *flow-id*	(Optional) Displays a specific SCSI flow index.
statistics	Displays the statistics for the SCSI flow.
lun lun-number	(Optional) Displays statics for a specific LUN number.

Command Default

None

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(2)	This command was introduced.

Examples

The following example displays SCSI flow services configuration for all SCSI flow identifiers:

```
switch# show scsi-flow
Flow Id: 3
        Initiator VSAN: 101
        Initiator WWN: 21:00:00:e0:8b:05:76:28
        Target VSAN: 102
        Target WWN: 21:00:00:20:37:38:7f:7d
        Target LUN: ALL LUNs
        Flow Verification Status:
        -------------------------
           Initiator Verification Status:   success
           Target Verification Status:      success
           Initiator Linecard Status:       success
           Target Linecard Status:          success
        Feature Status:
        ---------------
          Write-Acceleration enabled
            Write-Acceleration Buffers: 1024
            Configuration Status:  success
          Statistics enabled
            Configuration Status:  success
Flow Id: 4
        Initiator VSAN: 101
        Initiator WWN: 21:00:00:e0:8b:05:76:28
        Target VSAN: 102
        Target WWN: 21:00:00:20:37:38:a7:89
        Target LUN: ALL LUNs
        Flow Verification Status:
        -------------------------
           Initiator Verification Status:   success
           Target Verification Status:      success
```

```
   Initiator Linecard Status:       success
   Target Linecard Status:          success
Feature Status:
---------------
  Write-Acceleration enabled
    Write-Acceleration Buffers: 1024
    Configuration Status:  success
```

Table 12: show scsi-flow Field Descriptions, on page 1604 describes the significant fields shown in the **show scsi-flow** command output.

Table 12: show scsi-flow Field Descriptions

Field	Description
Initiator Verification Status	Verifies that the name server, FLOGI server, and zone server information for the initiator on the local switch are correct.
Target Verification Status	Verifies that the names sever and zone server information for the target on the local switch are correct.
Initiator Linecard Status	Verifies that the initiator is connected to an SSM and if DPP provisioning is enabled for the module.
Target Linecard Status	Verifies in the following order:1. The target switch sees the proper name server and zone server information for the initiator.2. The target switch sees the proper name server, FLOGI server and zone server information for the target.3. The target is connected to an SSM and if DPP provisioning is enabled for that module.

The following example displays SCSI flow services configuration for a specific SCSI flow identifier:

```
switch# show scsi-flow flow-id 3
Flow Id: 3
        Initiator VSAN: 101
        Initiator WWN: 21:00:00:e0:8b:05:76:28
        Target VSAN: 102
        Target WWN: 21:00:00:20:37:38:7f:7d
        Target LUN: ALL LUNs
        Flow Verification Status:
        -------------------------
           Initiator Verification Status:   success
           Target Verification Status:      success
           Initiator Linecard Status:       success
           Target Linecard Status:          success
        Feature Status:
        ---------------
          Write-Acceleration enabled
            Write-Acceleration Buffers: 1024
            Configuration Status:  success
          Statistics enabled
            Configuration Status:  success
```

The following example displays SCSI flow services statistics for all SCSI flow identifiers:

```
switch# show scsi-flow statistics
Stats for flow-id 4 LUN=0x0000
------------------------------
 Read Stats
```

```
  I/O Total count=2
  I/O Timeout count=0
  I/O Total block count=4
  I/O Max block count=2
  I/O Min response time=5247 usec
  I/O Max response time=10160 usec
  I/O Active Count=0
 Write Stats
  I/O Total count=199935
  I/O Timeout count=0
  I/O Total block count=12795840
  I/O Max block count=64
  I/O Min response time=492 usec
  I/O Max response time=10056529 usec
  I/O Active Count=16
 Non Read-Write Stats
  Test Unit Ready=4
  Report LUN=38
  Inquiry=50
  Read Capacity=3
  Mode Sense=0
  Request Sense=0
 Total Stats
  Rx Frame Count=3792063
  Rx Frame Byte Count=6549984752
  Tx Frame Count=3792063
  Tx Frame Byte Count=6549984752
 Error Stats
  SCSI Status Busy=0
  SCSI Status Reservation Conflict=0
  SCSI Status Task Set Full=0
  SCSI Status ACA Active=0
  Sense Key Not Ready=0
  Sense Key Medium Error=0
  Sense Key Hardware Error=0
  Sense Key Illegal Request=0
  Sense Key Unit Attention=28
  Sense Key Data Protect=0
  Sense Key Blank Check=0
  Sense Key Copy Aborted=0
  Sense Key Aborted Command=0
  Sense Key Volume Overflow=0
  Sense Key Miscompare=0
```

The following example displays SCSI flow services statistics for a specific SCSI flow identifier:

```
switch# show scsi-flow statistics flow-id 4
Stats for flow-id 4 LUN=0x0000
------------------------------
 Read Stats
  I/O Total count=2
  I/O Timeout count=0
  I/O Total block count=4
  I/O Max block count=2
  I/O Min response time=5247 usec
  I/O Max response time=10160 usec
  I/O Active Count=0
 Write Stats
  I/O Total count=199935
  I/O Timeout count=0
  I/O Total block count=12795840
  I/O Max block count=64
  I/O Min response time=492 usec
```

```
I/O Max response time=10056529 usec
I/O Active Count=16
```

show_scsi-target

To display information about existing SCSI target configurations, use the **show scsi-target** command.

show scsi-target {**auto-poll**|**custom-list**|**devices** [**vsan vsan-id**] [**fcid fcid-id**]|**disk** [**vsan vsan-id**] [**fcid fcid-id**]|**lun** [**vsan vsan-id**] [**fcid fcid-id**] [{**os** [{**aix**|**all**|**hpux**|**linux**|**solaris**|**windows**}]|**pwwn**|**status**|**tape** [**vsan vsan-id**] [**fcid fcid-id**]}]}

Syntax Description

auto-poll	Displays SCSI target auto polling information.
custom-list	Displays customized discovered targets.
devices	Displays discovered scsi-target devices information.
vsan vsan-range	(Optional) Specifies the VSAN ID or VSAN range. The ID range is 1 to 4093.
fcid fcid-id	(Optional) Specifies the FCID of the SCSI target to display.
disk	Displays discovered disk information.
lun	Displays discovered SCSI target LUN information.
os	Discovers the specified operating system.
aix	(Optional) Specifies the AIX operating system.
all	(Optional) Specifies all operating systems.
hpux	(Optional) Specifies the HPUX operating system.
linux	(Optional) Specifies the Linux operating system.
solaris	(Optional) Specifies the Solaris operating system.
windows	(Optional) Specifies the Windows operating system.
status	Displays SCSI target discovery status.
pwwn	Displays discover pWWN information for each OS.
tape	Displays discovered tape information.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

Use the **show scsi-target auto-poll** command to verify automatic discovery of online SCSI targets.

Examples

The following example displays the status of a SCSI discovery:

```
switch# show scsi-target status
discovery completed
```

The following example displays a customized discovered targets:

```
switch# show scsi-target custom-list---------------
VSAN DOMAIN---------------1   56
```

The following example displays discovered disk information:

```
switch# show scsi-target disk
---------------------------------------------------------------------------
VSAN    FCID        PWWN                      VENDOR    MODEL             REV
---------------------------------------------------------------------------
1       0x9c03d6    21:00:00:20:37:46:78:97   Company 4 ST318203FC        0004
1       0x9c03d9    21:00:00:20:37:5b:cf:b9   Company 4 ST318203FC        0004
1       0x9c03da    21:00:00:20:37:18:6f:90   Company 4 ST318203FC        0004
1       0x9c03dc    21:00:00:20:37:5a:5b:27   Company 4 ST318203FC        0004
1       0x9c03e0    21:00:00:20:37:36:0b:4d   Company 4 ST318203FC        0004
1       0x9c03e1    21:00:00:20:37:39:90:6a   Company 4 ST318203 CLAR18   3844
1       0x9c03e2    21:00:00:20:37:18:d2:45   Company 4 ST318203 CLAR18   3844
1       0x9c03e4    21:00:00:20:37:6b:d7:18   Company 4 ST318203 CLAR18   3844
1       0x9c03e8    21:00:00:20:37:38:a7:c1   Company 4 ST318203FC        0004
1       0x9c03ef    21:00:00:20:37:18:17:d2   Company 4 ST318203FC        0004
```

The following example displays the discovered LUNs for all OSs:

```
switch# show scsi-target lun os all
ST336607FC from SEAGATE (Rev 0006)
FCID is 0xed0001 in VSAN 7, PWWN is 21:00:00:04:cf:fb:42:f8
---------------------------------------------------------------------------
OS  LUN    Capacity Status  Serial Number    Device-Id
           (MB)
---------------------------------------------------------------------------
WIN 0x0    36704    Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
AIX 0x0    36704    Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
SOL 0x0    36704    Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
LIN 0x0    36704    Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
HP  0x0    36704    Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
```

The following example displays the discovered LUNs for the Solaris OS:

```
switch# show scsi-target lun os solaris
ST336607FC from SEAGATE (Rev 0006)
FCID is 0xed0001 in VSAN 7, PWWN is 21:00:00:04:cf:fb:42:f8
---------------------------------------------------------------------------
OS  LUN    Capacity Status  Serial Number    Device-Id
           (MB)
---------------------------------------------------------------------------
SOL 0x0    36704    Online  3JA1B9QA00007338 C:1 A:0 T:3 20:00:00:04:cf:fb:42:f8
```

The following example displays auto-polling information. Each user is indicated by the internal UUID number, which indicates that a CSM or an IPS module is in the chassis:

```
switch# show scsi-target auto-poll
```

```
auto-polling is enabled, poll_start:0 poll_count:1 poll_type:0
USERS OF AUTO POLLING
---------------------
uuid:54
```

The following example displays the port WWN that is assigned to each OS (Windows, AIX, Solaris, Linux, or HPUX):

```
switch# show scsi-target pwwn
------------------------------
OS     PWWN
------------------------------
WIN    24:91:00:05:30:00:2a:1e
AIX    24:92:00:05:30:00:2a:1e
SOL    24:93:00:05:30:00:2a:1e
LIN    24:94:00:05:30:00:2a:1e
HP     24:95:00:05:30:00:2a:1e
```

show sdv

To display information about SAN device virtualization (SDV), use the **show sdv** command in EXEC mode.

show sdv {**database** [{**pending vsan** *vsan-id*|**vsan** *vsan-id*}]|**merge status vsan** *vsan-id*|**pending-diff vsan** *vsan-id*|**session status vsan** *vsan-id*|**statistics vsan** *vsan-id*|**virtual-device name** *device-name* **vsan** *vsan-id*|**zone** [{**active vsan** *vsan-id*|**vsan** *vsan-id*}]}

Syntax Description

database	Displays the SDV database.
pending	(Optional) Displays the pending SDV database.
vsan *vsan-id*	(Optional) Specifies the number of the VSAN. The range is 1 to 4093.
merge status	Displays the SDV merge status.
pending-diff	Displays the SDV pending differences.
session	Displays the SDV session status.
statistics	Displays the SDV statistics.
virtual-device	Displays the SDV virtual devices.
name *device-name*	Specifies the name of the virtual target. The maximum size is 32.
zone	Specifies the zone.
active	(Optional) Specifies the active VSAN.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(2)	This command was introduced.
NX-OS 4.1(1b)	Changed the command output.

Usage Guidelines

None.

Examples

The following example shows how to display SDV database information:

```
switch# show sdv database vsan 1
[ WWN:50:00:53:00:00:1a:30:01 FCID:0xcd01a3 Real-FCID:0x7f000e ]
 *pwwn 20:0e:0d:00:00:01:12:10 primary
  pwwn 20:0e:0d:00:00:01:12:11
```

The following example displays merge status:

```
switch# show sdv merge status vsan 1
Merge Status for VSAN    : 1
------------------------------
Last Merge Time Stamp    : None
Last Merge State         : None
Last Merge Result        : SUCCESS
Last Merge Failure Reason: None [cfs_status: 0]
```

Related Commands

Command	Description
sdv enable	Enables the SAN device virtualization feature.
sdv virtual-device	Specifies the virtual target.

show secure-erase algorithm

To display the list of all Secure Erase algorithms, use the show secure-erase algorithm command.

show secure-erase module module-id algorithm algorithm name

Syntax Description

module module-id	Displays the slot number of the SSM on which Secure Erase is provisioned.
algorithm name	Displays the algorithm name.

Command Default

None.

Command Modes

Exec mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the list of Secure Erase algorithms:

```
switch# show secure-erase module 4 algorithm name 1
switch# Algorithm : 1
Step 0:
faa8bd6c1e838b6b9b0818f30d48f5eecc7e7f572d9d8ac50a9a78b73bf128eb7a71ff40a7c07f55dda1d31f875bca26b170d6b3c0735
55e06d6229f6a5dedeaa0583f0d1ebe28fca8a7cac936d6f0a453af4174fbbcba29f711047cb48e984a3c097519138a628bc6e662bd3d28237d09
1f68a8df05f50effc55390a12ee2c6
Step 1:
05574293e17c749464f7e70cf2b70a11338180a8d262753af5658748c40ed714858e00bf583f80aa225e2ce078a435d94e8f294c3f8ca
aa1f929dd6095a212155fa7c0f2e141d70357583536c9290f5bac50be8b044345d608eefb834b7167b5c3f68ae6ec759d7439199d42c2d7dc82f6
e0975720fa0af1003aac6f5ed11d39
Step 2:
12345678987654356789098765456712345678987654356789098765456712345678987654356789098765456712345678987654356789
09876545671234567898765435678909876545671234567898765435678909876545671234567898765435678909876545671234567898765435
67890987654567123456789876543
```

The following example displays all available Secure Erase algorithms on a module:

```
switch# show secure-erase module 4 algorithm
```

Related Commands

Command	Description
show secure-erase job	Displays the contents of a particular Secure Erase job.

show secure-erase job

To display the contents of a particular job, use the show secure-erase job command.

show secure-erase module module-id job job-id

Syntax Description

module module-id	Displays the slot number of the SSM on which Secure Erase is provisioned.
job-id	Displays the unique number to identify a Secure Erase job.

Command Default

None.

Command Modes

Exec mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the contents of a particular Secure Erase job:

```
switch# show secure-erase module 4 job 2
```

The following example displays the contents of all Secure Erase jobs configured on a module:

```
switch# show secure-erase module 16 job
```

Related Commands

Command	Description
show secure-erase algorithm	Displays the list of Secure Erase algorithms.

show secure-erase job detail

To display the contents of a particular job in detail, use the show secure-erase job detail command.

show secure-erase module module-id job job-id detail

Syntax Description

module module-id	Displays the slot number of the SSM on which Secure Erase is provisioned.
job-id	Displays the unique number to identify a Secure Erase job.

Command Default

None.

Command Modes

Exec mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the contents of a Secure Erase job in a brief form:

```
switch# show secure-erase module 4 job 2 detail
```

Related Commands

Command	Description
show secure-erase job	Displays the contents of a Secure Erase job.

show secure-erase vsan

To display a list of all VIs in the VSAN, use the show secure-erase vsan command.

show secure-erase module module-id vsan vsan-id

Syntax Description

module module-id	Displays the slot number of the SSM on which Secure Erase is provisioned.
vsan-id	Displays the VSAN ID of the target.

Command Default

None.

Command Modes

Exec mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the list of all VIs in the VSAN:

```
switch# show secure-erase module 4 vsan 1
```

Related Commands

Command	Description
show secure-erase algorithm	Displays the list of Secure Erase algorithms.
show secure-erase job	Displays the contents of a particular Secure Erase job.

show sme cluster

To display the information about the Cisco SME cluster, use the show sme cluster command.

show sme cluster {**cluster name** {**detail**|**interface** {**detail**|**node** {**A.B.C.D**|**X:X::X**|**DNS name** **sme slot/port**}|**sme slot/port**|**summary**}|**it-nexus**|**key database** {**detail**|**guid guid name** {**detail**|**summary**}|**summary**}|**load-balancing**|**lun crypto-status**|**node** {{**A.B.C.D**|**X:X::X**|**DNS name**}|**summary**}|**recovery officer** {**index**|**detail index**|**summary index**}|**summary**|**tape** {**detail**|**summary**}|**tape-bkgrp tape group name volgrp volume group name**}|**detail**|**summary**}

Syntax Description

cluster cluster name	Displays Cisco SME cluster information. The maximum length is 32 characters.
detail	Displays Cisco SME cluster details.
interface	Displays information about Cisco SME cluster interface.
node	Display information about Cisco SME cluster remote interface.
A.B.C.D	Specifies the IP address of the remote switch in IPv4 format.
X:X::X	Specifies the IP address of the remote switch in IPv6 format.
DNS name	Specifies the name of the remote database.
sme	Specifies the Cisco SME interface.
slot	Identifies the MPS-18/4 module slot.
port	Identifies the Cisco SME port.
interface summary	Displays Cisco SME cluster interface summary.
it-nexus	Displays the initiator to target connections (IT-nexus) in the Cisco SME cluster.
key database	Shows the Cisco SME cluster key database.
detail	Shows the Cisco SME cluster key database details.
guid guid name	Displays Cisco SME cluster key database guid. The maximum length is 64.
summary	Displays Cisco SME cluster key database summary.
load-balancing	Displays the load balancing status of the cluster.
lun	Displays the logical unit numbers (LUNs) in a cluster.
crypto-status	Displays the crypto status of the LUNs.
node summary	Displays Cisco SME cluster node summary.
recovery officer detail	Displays Cisco SME cluster recovery officer detail.
recovery officer summary	Displays Cisco SME cluster recovery officer summary.

index	Specifies recovery officer index. The range is 1to 8.
detail index	Specifies recovery officer detail index. The range is 1to 8.
summary index	Specifies recovery officer summary index. The range is 1to 8.
tape detail	Displays Cisco SME tape detail
tape summary	Displays the tape summary
tape-bkgrp tape group name	Displays the crypto tape backup group name. The maximum length is 32 characters.
volgrp volume group name	Displays tape volume group name.The maximum length is 32 characters.
detail	Displays Cisco SME cluster details.
summary	Shows Cisco SME cluster summary.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(2)	This command was introduced.
NX-OS 4.1(1c)	Added the syntax description.

Usage Guidelines

None.

Examples

The following example displays the configuration details about a cluster:

```
switch# show sme cluster c1
Cluster ID is 0x2b2a0005300035e1
 Cluster status is online
 Security mode is advanced
 Total Nodes are 1
 Recovery Scheme is 2 out of 5
 Fabric[0] is Fabric_name-excal10
 KMC server 10.21.113.117:8800 is provisioned, connection state is initializing
 Master Key GUID is 10af119cfd79c17f-ee568878c049f94d, Version: 0
 Shared Key Mode is Not Enabled
 Auto Vol Group is Not Enabled
 Tape Compression is Not Enabled
 Tape Key Recycle Policy is Not Enabled
 Key On Tape is Not Enabled
 Cluster Infra Status : Operational
 Cluster is Administratively Up
 Cluster Config Version : 24
```

The following example displays the cluster interface information:

```
switch# show sme cluster clustername1 interface it-nexus
```

```
 --------------------------------------------------------------------------------
    Host WWN                 VSAN    Status    Switch        Interface
    Target WWN
--------------------------------------------------------------------------------
10:00:00:00:c9:4e:19:ed,
2f:ff:00:06:2b:10:c2:e2      4093     online    switch     sme4/1
```

The following example displays the specific recovery officer of a cluster:

```
switch# show sme cluster clustername1 recovery officer

Recovery Officer 1 is set
  Master Key Version is 0
  Recovery Share Version is 0
  Recovery Share Index is 1
  Recovery Scheme is 1 out of 1
  Recovery Officer Label is
  Recovery share protected by a password
Key Type is master key share
    Cluster is clustername1, Master Key Version is 0
    Recovery Share Version is 0, Share Index is 1
```

Related Commands

Command	Description
clear sme	Clears Cisco SME configuration.
show sme cluster	Displays information about Cisco SME cluster.

show sme transport

To display the Cisco SME cluster transport information, use the show sme transport command.

show sme transport ssl truspoint

Syntax Description

ssl	Displays transport Secure Sockets Layer (SSL) information.
trustpoint	Displays transport SSL trustpoint information.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.2(2c)	This command was introduced.
NX-OS 4.1(1c)	Added the syntax of the command.

Usage Guidelines

None.

Examples

The following example displays the internal cluster errors:

```
switch# show sme transport ssl trustpoint
SME Transport SSL trustpoint is trustpoint-label
```

Related Commands

Command	Description
clear sme	Clears Cisco SME configuration.
show sme cluster	Displays information about Cisco SME cluster.

show snmp

To display SNMP status and setting information, use the **show snmp** command.

show snmp [{**community**|**engineID**|**group**|**host**|**sessions**|**trap**|**user** [*user-name*] [**engineID** *engine-id*]}]

Syntax Description

community	(Optional) Displays SNMP community strings.
engineID	(Optional) Displays SNMP engine IDs.
group	(Optional) Displays SNMP groups.
host	(Optional) Displays SNMP hosts.
sessions	(Optional) Displays SNMP sessions.
trap	(Optional) Displays SNMP traps.
user	(Optional) Displays SNMPv3 users.
user-name	(Optional) Specifies the user name. The maximum is 32.
engineID	(Optional) Displays the engine ID.
engine-id	(Optional) Specifies the engine ID. The maximum is 128.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0(x)	Added the **engineid**, **group**, and **sessions** keywords.
3.1(2)	Added the **trap** keyword.

Usage Guidelines

You can view the **show snmp community** output, only when the user role is assigned as network-admin.

Examples

The following example shows how to display SNMP traps:

```
switch# show snmp trap
--------------------------------------------------------------------------------
Trap type                                                              Enabled
--------------------------------------------------------------------------------
entity               : entity_mib_change                              Yes
entity               : entity_module_status_change                    Yes
entity               : entity_power_status_change                     Yes
entity               : entity_module_inserted                         Yes
```

```
entity               : entity_module_removed                        Yes
entity               : entity_unrecognised_module                   Yes
entity               : entity_fan_status_change                     Yes
entity               : entity_power_out_change                      Yes
link                 : delayed-link-state-change                    Yes
link                 : iflink-up                                    Yes
link                 : iflink-down                                  Yes
callhome             : event-notify                                 No
callhome             : smtp-send-fail                               No
cfs                  : state-change-notif                           No
cfs                  : merge-failure                                No
rf                   : redundancy_framework                         Yes
aaa                  : server-state-change                          No
license              : notify-license-expiry                        Yes
license              : notify-no-license-for-feature                Yes
license              : notify-licensefile-missing                   Yes
--More--
```

The following example displays SNMP information:

```
switch# show snmp
sys contact:
sys location:
1631 SNMP packets input
        0 Bad SNMP versions
        0 Unknown community name
        0 Illegal operation for community name supplied
        0 Encoding errors
        64294 Number of requested variables
        1 Number of altered variables
        1628 Get-request PDUs
        0 Get-next PDUs
        1 Set-request PDUs
152725 SNMP packets output
        0 Too big errors
        1 No such name errors
        0 Bad values errors
        0 General errors
Community                      Access
---------                      ------
public                          rw
User                           Group                          Auth  Priv
____                           _____                          ____  ____
admin                          network-admin                  md5   no
```

The following example displays SNMP user details.

```
switch# show snmp user
User                           Group                          Auth  Priv
____                           _____                          ____  ____
steve                          network-admin                  md5   des
sadmin                         network-admin                  md5   des
stever                         network-operator               md5   des
```

The following example displays SNMP community information:

```
switch# show snmp community

Community                      Access
---------                      ------
private                         rw
public                          ro
v93RACqPNH                      ro
```

The following example displays SNMP host information:

```
switch# show snmp host
Host                                 Port Version  Level  Type   SecName
____                                 ____ _______  ______ ____   ______
171.16.126.34                        2162 v2c      noauth trap   public
171.16.75.106                        2162 v2c      noauth trap   public
171.31.124.81                        2162 v2c      noauth trap   public
171.31.157.193                       2162 v2c      noauth trap   public
171.31.157.98                        2162 v2c      noauth trap   public
171.31.49.25                         2162 v2c      noauth trap   public
171.31.49.32                         2188 v2c      noauth trap   public
171.31.49.49                         2162 v2c      noauth trap   public
171.31.49.49                         3514 v2c      noauth trap   public
171.31.49.54                         2162 v2c      noauth trap   public
171.31.58.54                         2162 v2c      noauth trap   public
171.31.58.81                         2162 v2c      noauth trap   public
171.31.58.97                         1635 v2c      noauth trap   public
171.31.58.97                         2162 v2c      auth   trap   public
171.31.58.97                         3545 v2c      auth   trap   public
172.22.00.43                         2162 v2c      noauth trap   public
172.22.00.65                         2162 v2c      noauth trap   public
172.22.05.234                        2162 v2c      noauth trap   public
172.22.05.98                         1050 v2c      noauth trap   public
```

The following example displays SNMP engine ID information:

```
switch# show snmp engineID
Local SNMP engineID:[Dec] 128:000:000:009:003:000:013:236:008:040:192
switch#
```

The following example displays SNMP group information:

```
switch# show snmp group
groupname: network-admin
security model: any
security level: noAuthNoPriv
readview: network-admin-rd
writeview: network-admin-wr
notifyview: network-admin-rd
storage-type: permanent
row status: active
groupname: network-admin
security model: any
security level: authNoPriv
readview: network-admin-rd
writeview: network-admin-wr
notifyview: network-admin-rd
storage-type: permanent
row status: active
groupname: network-operator
security model: any
security level: noAuthNoPriv
readview: network-operator-rd
writeview: network-operator-wr
notifyview: network-operator-rd
storage-type: permanent
row status: active
groupname: network-operator
security model: any
security level: authNoPriv
readview: network-operator-rd
```

```
writeview: network-operator-wr
notifyview: network-operator-rd
storage-type: permanent
row status: active
```

show span drop-counters

To display the SPAN drop counters, use the show span drop-counters command.

show span drop-counters

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
3.3(1a)	This command was introduced.

Usage Guidelines

This command is supported only on a ISOLA platform.

Examples

The following example shows how to configure the SPAN drop counters:

```
switch# config
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# span drop-counters
SPAN Drop-Counters for module 3 is: 0x0
SPAN Drop-Counters for module 7 is: 0x0
```

Related Commands

Command	Description
show span max-queued-packets	Displays the SPAN max-queued packets.

show span max-queued-packets

To display the SPAN max-queued packets, use the show span max-queued-packets command.

show span max-queued-packets

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

This command is supported only ona ISOLA platform.

Examples

The following example displays the SPAN max-queued packets:

```
switch# show span max-queued-packets
max-queued-packets for SPAN sessions: 1
```

Related Commands

Command	Description
span max-queued-packets	Configures the SPAN max-queued packets.

show sprom

To display vendor ID, product component attributes and serial number information that can be used to track field replacable units, use the **show sprom** command.

show sprom {**backplane backplane-index**|**clock clock-module-index**|**fan**|**mgmt-module**|**module module-number sprom-index**|**powersupply powersupply-index**|**sup**}

Syntax Description

backplane *backplane-index*	Displays attributes that can be used to uniquely identify a switch. The range is 1 to 2.
clock *clock-module-index*	Displays attributes of the clock module. There are two clock modules in a switch. This module is absent in MDS9216 type switch. The range is 1 to 2.
fan	Displays attributes that uniquely identified fan.
mgmt-module	Displays attributes of management module. This module is only present in MDS9216 type switch.
module module-number sprom-index	Displays vendor ID, product's component attributes for the given switching module. There can be up to 4 sub components in a module. Each of them will have a SPROM associated with it.
powersupply *powersupply-index*	Displays attributes of the first or the second power supply. This contains information about the power supply capacity in watts when it is used in 110 Volts and 220 Volts. This information is used for power-budget allocation. The range is 1 to 2.
sup	Displays vendor ID, product's component attributes for the current supervisor module.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use the **show sprom** command to get unique information about a specific module, supervisor module, switch, power supply module, or a fan module. If you need to report a problem with a module, supervisor module, switch, power supply module, or a fan module and do not have access to the management station, then you can extract the serial number information from **show sprom**.

Examples

The following example displays management module information. This module and command are specific to the Cisco MDS 9216 switch:

```
switch# show sprom mgmt-module
DISPLAY SAM sprom contents:
Common block:
 Block Signature :0xabab
 Block Version   :2
 Block Length    :156
 Block Checksum  :0x1295
 EEPROM Size     :0
 Block Count     :2
 FRU Major Type  :0x0
 FRU Minor Type  :0x0
 OEM String      :Cisco Systems Inc
 Product Number  :SAM SMITH
 Serial Number   :12345678901
 Part Number     :SAM-SMITH-06
 Part Revision   :A0
 Mfg Deviation   :
 H/W Version     :1.0
 Mfg Bits        :1
 Engineer Use    :0
 snmpOID         :0.0.0.0.0.0.0.0
 Power Consump   :-200
 RMA Code        :0-0-0-0
Linecard Module specific block:
 Block Signature :0x6003
 Block Version   :2
 Block Length    :103
 Block Checksum  :0x3c7
 Feature Bits    :0x0
 HW Changes Bits :0x0
 Card Index      :9009
 MAC Addresses   :00-12-34-56-78-90
 Number of MACs  :4
 Number of EOBC links :4
 Number of EPLD  :0
 Port Type-Num   :200-16
 SRAM size       :0
 Sensor #1       :0,0
 Sensor #2       :0,0
 Sensor #3       :0,0
 Sensor #4       :0,0
 Sensor #5       :0,0
 Sensor #6       :0,0
 Sensor #7       :0,0
 Sensor #8       :0,0
```

The following command displays supervisor module information:

```
switch# show sprom sup
DISPLAY supervisor sprom contents:
Common block:
 Block Signature : 0xabab
 Block Version   : 2
 Block Length    : 156
 Block Checksum  : 0x10a8
 EEPROM Size     : 512
 Block Count     : 2
 FRU Major Type  : 0x6002
 FRU Minor Type  : 0x7d0
 OEM String      : Cisco Systems
 Product Number  : DS-X9530-SF1-K9
 Serial Number   : abcdefgh
 Part Number     : 73-7523-06
```

```
 Part Revision   : 0.0
 Mfg Deviation   : 0.0
 H/W Version     : 0.0
 Mfg Bits        : 0
 Engineer Use    : 0
 snmpOID         : 9.5.1.3.1.1.2.2000
 Power Consump   : -524
 RMA Code        : 0-0-0-0
Supervisor Module specific block:
 Block Signature : 0x6002
 Block Version   : 2
 Block Length    : 103
 Block Checksum  : 0x927
 Feature Bits    : 0x0
 HW Changes Bits : 0x0
 Card Index      : 9003
 MAC Addresses   : 00-05-30-00-18-be
 Number of MACs  : 4
 Number of EPLD  : 1
 EPLD A          : 0x0
 Sensor #1       : 75,60
 Sensor #2       : 60,55
 Sensor #3       : -127,-127
 Sensor #4       : -127,-127
 Sensor #5       : -128,-128
 Sensor #6       : -128,-128
 Sensor #7       : -128,-128
 Sensor #8       : -128,-128
```

Related Commands

Command	Description
show hardware	Displays brief information about the list of field replacable units in the switch.

show ssh

To display Secure Shell information (SSH), use the **show ssh** command.

show ssh {**key** [{**dsa**|**rsa**|**rsa1**}]|**server**}

Syntax Description

key	Displays SSH keys.
dsa	(Optional) Displays DSA SSH keys.
rsa	(Optional) Displays RSA SSH keys.
rsa1	(Optional) Displays RSA1 SSH keys.
server	Displays the SSH server status.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

To display the host key pair details for the specified key or for all keys, if no key is specified, use the **show ssh key** command. To display the status of the SSH protocol (enabled or disabled) and the versions that are enabled for that switch, use the **show ssh server** command.

Examples

The following example displays SSH server status:

```
switch# show ssh server
ssh is enabled
version 1 enabled
version 2 enabled
```

The following example displays host key pair details:

```
switch# show ssh key

rsa1 Keys generated:Sun Jan 13 07:16:26 1980
1024 35
fingerprint:
1024 67:76:02:bd:3e:8d:f5:ad:59:5a:1e:c4:5e:44:03:07
could not retrieve rsa key information
dsa Keys generated:Sun Jan 13 07:40:08 1980
ssh-dss AAAAB3NzaC1kc3MAAABBAJTCRQOydNRel2v7uiO6Fix+OTn8eGdnnDVxw5eJs5OcOEXOyjaW
cMMYsEgxc9ada1NElp8Wy7GPMWGOQYj9CU0AAAAVAMCcWhNN18zFNOIPo7cU3t7d0iEbAAAAQBdQ8UAO
i/Cti84qFb3kTqXlS9mEhdQUo0lHcH5bw5PKfj2Y/dLR437zCBKXetPj4p7mhQ6Fq5os8RZtJEyOsNsA
AABAA0oxZbPyWeR5NHATXiyXdPI7j9i8fgyn9FNipMkOF2Mn75Mi/lqQ4NIq0gQNvQOx27uCeQlRts/Q
wI4q68/eaw==
```

```
fingerprint:
512 f7:cc:90:3d:f5:8a:a9:ca:48:76:9f:f8:6e:71:d4:ae
```

show ssm provisioning

To display the attributes of the Storage Services Module (SSM) installed, use the show ssm provisioning command.

show ssm provisioning

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(2)	This command was introduced.
2.1(1a)	Added Provisioning Status column to the display.

Usage Guidelines

None.

Examples

The following example provisions the SSM installed in the switch:

```
switch# show ssm provisioning
Module   Ports       Application        Provisioning Status
--------------------------------------------------------------
   4      1-32       scsi-flow                   success
```

Table 13: show ssm provisioning Field Descriptions, on page 1631 describes the significant fields shown in the show ssm provisioning command output.

Table 13: show ssm provisioning Field Descriptions

Field	Description
Module	Slot where SSM is installed.
Ports	Ports available on the SSM.
Application	Feature configured on the SSM.
Provisioning Status	Displays the status of the SSM attributes.

Related Commands

Command	Description
ssm enable feature	Enables the SCSI flow feature on the SSM.

show startup-config

To display the startup configuration file, use the **show startup-config** command

show startup-config [log]

Syntax Description

log	(Optional) Displays execution log of last used ASCII startup configuration.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the switch configuration at startup:

```
switch# show startup-config
vsan database
vsan 2
vsan 3
vsan 4
vsan 5
vsan 31
vsan 32 suspend
vsan 100
vsan 300
 interface port-channel 1
switchport mode E
switchport trunk mode off
 interface port-channel 2
fspf cost 100 vsan 2
switchport mode E
no switchport trunk allowed vsan all
switchport trunk allowed vsan add 1-99
switchport trunk allowed vsan add 101-4093
 interface port-channel 3
switchport mode E
switchport trunk mode off
 interface port-channel 4
switchport mode E
no switchport trunk allowed vsan all
switchport trunk allowed vsan add 1-99
switchport trunk allowed vsan add 101-4093
 interface port-channel 5
switchport mode E
no switchport trunk allowed vsan all
switchport trunk allowed vsan add 1-10interface port-channel 5
switchport mode E
no switchport trunk allowed vsan all
```

```
switchport trunk allowed vsan add 1-10
interface port-channel 8
switchport mode E
 interface vsan1
no shutdown
snmp-server community public rw
snmp-server user admin network-admin auth md5 0xe84b06201ae3bfb726a2eab9f485eb57
 localizedkey
snmp-server host 171.69.126.34 traps version 2c public udp-port 2162
snmp-server host 171.69.75.106 traps version 2c public udp-port 2162
vsan database
vsan 3 interface fc2/9
vsan 3 interface fc2/14
vsan 5 interface fc9/11
vsan 2 interface fc9/12
vsan 3 interface port-channel 3
vsan 3 interface port-channel 4
vsan 100 interface port-channel 8
boot system bootflash:/isan-8b-u sup-1
boot kickstart bootflash:/boot-3b sup-1
boot system bootflash:/isan-8b-u sup-2
boot kickstart bootflash:/boot-3b sup-2
ip default-gateway 172.22.90.1
power redundancy-mode combined force
username admin password 5 HyLyYqb4.q74Y  role network-admin
zone name Z1 vsan 1
  member pwwn 10:00:00:00:77:99:60:2c
  member pwwn 21:00:00:20:37:a6:be:14
zone default-zone permit vsan 1
zoneset distribute full vsan 51-58
zoneset name ZS1 vsan 1
  member Z1
zoneset  activate name ZS1 vsan 1
 interface fc2/1
switchport mode E
switchport trunk mode off
no shutdown
 interface fc2/2
 interface fc2/3
channel-group 1 force
no shutdown
interface fc2/6
channel-group 2 force
no shutdown
 interface fc2/7
switchport mode E
no shutdown
no switchport trunk allowed vsan all
switchport trunk allowed vsan add 1-25
interface fc2/9
switchport mode E
switchport trunk mode off
no shutdown
 interface fc2/10
channel-group 3 force
no shutdown
 interface fc2/12
channel-group 4 force
no shutdown
 interface fc2/14
switchport mode E
no shutdown
no switchport trunk allowed vsan all
switchport trunk allowed vsan add 1-99
```

```
switchport trunk allowed vsan add 101-4093
 interface fc2/15
channel-group 6 force
no shutdown
 interface fc2/16
channel-group 6 force
no shutdown
.
.
.
interface fc9/10
switchport mode F
no shutdown
 interface fc9/11
switchport trunk mode off
no shutdown
 interface fc9/12
switchport mode E
switchport speed 1000
switchport trunk mode off
no shutdown
 interface fc9/15
no shutdown
no switchport trunk allowed vsan all
switchport trunk allowed vsan add 1-99
switchport trunk allowed vsan add 101-4093
 interface fc9/16
switchport mode FL
no shutdown
 interface mgmt0
ip address 209.165.200.226 209.165.200.227
no shutdown
```

show switchname

To display the switch network name, use the **show switchname** command.

show switchname [serialnum]

Syntax Description

serialnum	(Optional) Displays switch serial number.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the name of the switch:

```
switch# show switchname
switch-123
```

The following example displays the switch name and serial number:

```
switch# show switchname
switch-123
Serial Number #1   : FOX0712S007
Serial Number #2   :
```

show system

To display the system information, use the **show system** command.

show system {**cores**|**default** {**switchport**|**zone**}|**directory information**|**error-id** {**hex-id**|**list**}|**exception-info**|**pss shrink status [details]**|**redundancy status**|**reset-reason** [**module slot**]|**resources**|**standby manual-boot**|**uptime**}

Syntax Description

cores	Displays core transfer option.
default	Displays system default values.
switchport	Displays default values for switch port attributes.
zone	Displays default values for a zone.
directory information	Displays information of the system manager.
error-id	Displays description about errors.
hex-id	Specifies the error ID in hexadecimal format. The range is 0x0 to 0xffffffff.
list	Specifies all error IDs.
exception-info	Displays last exception log information.
pss shrink status	Displays the last PSS shrink status.
details	(Optional) Displays detailed information on the last PSS shrink status.
redundancy status	Displays Redundancy status.
reset-reason	Displays the last four reset reason codes.
module slot	(Optional) Specifies the module number to display the reset-reason codes.
resources	Displays the CPU and memory statistics.
standby manual-boot	Displays the standby manual boot option.
uptime	Displays how long the system has been up and running.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(3)	Changed the command output.
1.0(2)	This command was introduced.

Release	Modification
3.0(1)	Added the **zone** option.
3.0(1)	Added the standby manual-boot keyword.

Usage Guidelines

Use the **show system redundancy status** command to ensure that the system is ready to accept a switchover.

Examples

The following example shows how to display the system uptime:

```
switch# show system uptime
System start time:          Fri Dec 19 02:26:05 2008
System uptime:              18 days, 6 hours, 14 minutes, 19 seconds
Kernel uptime:              18 days, 4 hours, 48 minutes, 28 seconds
switch#
```

The following example shows how to display the system redundancy status:

```
switch# show system redundancy status
Redundancy mode
---------------
      administrative:   HA
         operational:   None
This supervisor (sup-2)
-----------------------
    Redundancy state:   Active
    Supervisor state:   Active
      Internal state:   Active with no standby
Other supervisor (sup-1)
------------------------
    Redundancy state:   Not present
```

The following example displays port states after the **system default switchport mode f** command is executed:

```
switch# show system default switchport
System default port state is down
System default trunk mode is on
System default port mode is F
```

The following example displays error information for a specified ID:

```
switch# show system error-id 0x401D0019
Error Facility: module
Error Description: Failed to stop Linecard Async Notification.
```

The following example displays the system health information:

```
switch# show system health
Current health information for module 2.
Test                    Frequency       Status          Action
------------------------------------------------------------------
Bootflash                10 Sec         Enabled         Enabled
EOBC                      5 Sec         Enabled         Enabled
Loopback                  5 Sec         Enabled         Enabled
CF checksum               7 Sec         Enabled         Enabled
CF re-flash              30 Sec         Enabled         Enabled
------------------------------------------------------------------
```

```
Current health information for module 3.
Test                    Frequency       Status          Action
------------------------------------------------------------------
Bootflash                10 Sec         Enabled         Enabled
EOBC                      5 Sec         Enabled         Enabled
Loopback                  5 Sec         Enabled         Enabled
------------------------------------------------------------------
Current health information for module 5.
Test                    Frequency       Status          Action
------------------------------------------------------------------
InBand                    5 Sec         Enabled         Enabled
Bootflash                10 Sec         Enabled         Enabled
EOBC                      5 Sec         Enabled         Enabled
Management Port           5 Sec         Enabled         Enabled
CF checksum               7 Sec         Halted          Enabled
CF re-flash              30 Sec         Halted          Enabled
------------------------------------------------------------------
```

The following example displays the system reset information:

```
switch# show system reset reason
----- reset reason for module 6 -----
1) At 520267 usecs after Tue Aug  5 16:06:24 1980
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 1.2(0.73a)
2) At 653268 usecs after Tue Aug  5 15:35:24 1980
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 1.2(0.45c)
3) No time
    Reason: Unknown
    Service:
    Version: 1.2(0.45c)
4) At 415855 usecs after Sat Aug  2 22:42:43 1980
    Reason: Power down triggered due to major temperature alarm
    Service:
    Version: 1.2(0.45c)
```

The following example displays system-related CPU and memory statistics:

```
switch# show system resources
Load average:   1 minute: 0.43   5 minutes: 0.17   15 minutes: 0.11
Processes   :   100 total, 2 running
CPU states  :   0.0% user,   0.0% kernel,   100.0% idle
Memory usage:   1027628K total,    313424K used,    714204K free
                   3620K buffers,   22278K cache
```

Use the **show system cores** command to display the currently configured scheme for copying cores:

```
switch# show system cores
Transfer of cores is enabled
```

Use the **show system default zone** command to display the default values for a zone:

```
switch# show system default zone
system default zone default-zone permit
system default zone distribute active only
```

show system default zone

To verify the configured default zone values, use the show system default zone command.

show system default zone

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.
3.2(1)	Added the basic default zoning mode option.

Usage Guidelines

None.

Examples

The following example shows the default values for default-zone as deny, distribute as active only, and zone mode as basic:

```
switch# show system default zone
system default zone default-zone deny
system default zone distribute active only
system default zone mode basic
```

The following example shows the default values for default-zone as permit, distribute as full, and zone mode as enhanced.

```
switch# show system default zone
system default zone default-zone permit
system default zone distribute active full
system default zone mode enhanced
```

Related Commands

Command	Description
no system default zone mode enhanced	Configures the default value of zone mode as basic.
no system default zone distribute full	Configures the default value of distribute as active only.
no system default zone default-zone permit	Configures the default value of default zone as deny.
system default zone distribute full	Configures the default value of distribute as full.
system default zone mode enhanced	Configures the default value of zone mode as enhanced.

show system health

To display configured Online Health Management System (OHMS) information, use the **show system health** command.

show system health [{**loopback frame-length**|**module** *slot*|**statistics loopback** [{**interface fc** *slot*/*port*|**module** *slot* **timelog**|**timelog**}]}]

Note On a Cisco Fabric Switch for HP c-Class BladeSystem and on a Cisco Fabric Switch for IBM BladeCenter, the syntax differs from **interface fc** *slot*/*port* as follows: **interface bay** *port* | **ext** *port* }

Syntax Description

loopback	(Optional) Displays the OHMS loopback test statistics.
frame-length	(Optional) Displays the loopback frame length.
module *slot*	(Optional) Displays module information.
statistics	(Optional) Displays OHMS statistics.
interface	(Optional) Specifies the required interface.
fc *slot*/*port*	Specifies a Fibre Channel interface on a Cisco MDS 9000 Family Switch.
bay *port* | **ext** *port*	Specifies a Fibre Channel interface on a Cisco MDS 9124 Fabric Switch, a Cisco Fabric Switch for HP c-Class BladeSystem, and a Cisco Fabric Switch for IBM BladeCenter.
iscsi *slot*/*port*	(Optional) Specifies the iSCSI interface at the specified slot and port.
timelog	(Optional) Displays the loopback round-trip times.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.
3.1(2)	Added the **bay** *port* | **ext** *port* keywords and arguments.

Usage Guidelines

None.

Examples

The following example displays the current health of all modules in the switch:

```
switch# show system health
Current health information for module 1.
```

```
Test                    Frequency       Status          Action
-----------------------------------------------------------------
Bootflash                10 Sec         Running         Enabled
EOBC                      5 Sec         Running         Enabled
Loopback                  5 Sec         Running         Enabled
CF checksum               7 Days        Halted          Enabled
CF re-flash              30 Days        Halted          Enabled
-----------------------------------------------------------------
Current health information for module 2.
Test                    Frequency       Status          Action
-----------------------------------------------------------------
Bootflash                10 Sec         Running         Enabled
EOBC                      5 Sec         Running         Enabled
Loopback                  5 Sec         Running         Enabled
-----------------------------------------------------------------
Current health information for module 5.
Test                    Frequency       Status          Action
-----------------------------------------------------------------
Bootflash                10 Sec         Running         Enabled
EOBC                      5 Sec         Running         Enabled
Loopback                  5 Sec         Running         Enabled
-----------------------------------------------------------------
Current health information for module 6.
Test                    Frequency       Status          Action
-----------------------------------------------------------------
Bootflash                10 Sec         Running         Enabled
EOBC                      5 Sec         Running         Enabled
Loopback                  5 Sec         Running         Enabled
CF checksum               7 Days        Halted          Enabled
CF re-flash              30 Days        Halted          Enabled
-----------------------------------------------------------------
Current health information for module 7.
Test                    Frequency       Status          Action
-----------------------------------------------------------------
InBand                    5 Sec         Running         Enabled
Bootflash                10 Sec         Running         Enabled
EOBC                      5 Sec         Running         Enabled
Management Port           5 Sec         Running         Enabled
-----------------------------------------------------------------
Current health information for module 8.
Test                    Frequency       Status          Action
-----------------------------------------------------------------
InBand                    5 Sec         Running         Enabled
Bootflash                10 Sec         Running         Enabled
EOBC                      5 Sec         Running         Enabled
-----------------------------------------------------------------
Current health information for module 10.
Test                    Frequency       Status          Action
-----------------------------------------------------------------
Bootflash                10 Sec         Running         Enabled
EOBC                      5 Sec         Running         Enabled
Loopback                  5 Sec         Running         Enabled
-----------------------------------------------------------------
Current health information for module 11.
Test                    Frequency       Status          Action
-----------------------------------------------------------------
Bootflash                10 Sec         Running         Enabled
EOBC                      5 Sec         Running         Enabled
Loopback                  5 Sec         Running         Enabled
CF checksum               7 Days        Halted          Enabled
CF re-flash              30 Days        Halted          Enabled
-----------------------------------------------------------------
Current health information for module 12.
Test                    Frequency       Status          Action
```

```
----------------------------------------------------------------
Bootflash               10 Sec         Running         Enabled
EOBC                     5 Sec         Running         Enabled
Loopback                 5 Sec         Running         Enabled
----------------------------------------------------------------
Current health information for module 13.
Test                   Frequency       Status          Action
----------------------------------------------------------------
Bootflash               10 Sec         Running         Enabled
EOBC                     5 Sec         Running         Enabled
----------------------------------------------------------------
```

The following example displays the health statistics for all modules:

```
switch# show system health statistics
Test statistics for module # 1
-------------------------------------------------------------------------------
Test Name           State            Freq(s)    Run    Pass    Fail CFail Errs
-------------------------------------------------------------------------------
Bootflash           Running             5s    12900   12900       0     0    0
EOBC                Running             5s    12900   12900       0     0    0
Loopback            Running             5s    12900   12900       0     0    0
-------------------------------------------------------------------------------
Test statistics for module # 3
-------------------------------------------------------------------------------
Test Name           State            Freq(s)    Run    Pass    Fail CFail Errs
-------------------------------------------------------------------------------
Bootflash           Running             5s    12890   12890       0     0    0
EOBC                Running             5s    12890   12890       0     0    0
Loopback            Running             5s    12892   12892       0     0    0
-------------------------------------------------------------------------------
Test statistics for module # 5
-------------------------------------------------------------------------------
Test Name           State            Freq(s)    Run    Pass    Fail CFail Errs
-------------------------------------------------------------------------------
InBand              Running             5s    12911   12911       0     0    0
Bootflash           Running             5s    12911   12911       0     0    0
EOBC                Running             5s    12911   12911       0     0    0
Management Port     Running             5s    12911   12911       0     0    0
-------------------------------------------------------------------------------
Test statistics for module # 6
-------------------------------------------------------------------------------
Test Name           State            Freq(s)    Run    Pass    Fail CFail Errs
-------------------------------------------------------------------------------
InBand              Running             5s    12907   12907       0     0    0
Bootflash           Running             5s    12907   12907       0     0    0
EOBC                Running             5s    12907   12907       0     0    0
-------------------------------------------------------------------------------
Test statistics for module # 8
-------------------------------------------------------------------------------
Test Name           State            Freq(s)    Run    Pass    Fail CFail Errs
-------------------------------------------------------------------------------
Bootflash           Running             5s    12895   12895       0     0    0
EOBC                Running             5s    12895   12895       0     0    0
Loopback            Running             5s    12896   12896       0     0    0
-------------------------------------------------------------------------------
```

The following example displays the statistics for a module:

```
switch# show system health statistics module 3
Test statistics for module # 3
-------------------------------------------------------------------------------
Test Name           State            Freq(s)    Run    Pass    Fail CFail Errs
```

```
--------------------------------------------------------------------------------
Bootflash           Running             5s    12932   12932       0     0    0
EOBC                Running             5s    12932   12932       0     0    0
Loopback            Running             5s    12934   12934       0     0    0
--------------------------------------------------------------------------------
```

The following example displays the loopback test statistics for the entire switch:

```
switch# show system health statistics loopback
-----------------------------------------------------------------
Mod Port Status               Run     Pass     Fail   CFail Errs
  1   16 Running             12953    12953       0       0    0
  3   32 Running             12945    12945       0       0    0
  8    8 Running             12949    12949       0       0    0
-----------------------------------------------------------------
```

The following example displays the loopback test statistics for a specified interface:

```
switch# show system health statistics loopback interface fc 3/1
-----------------------------------------------------------------
Mod Port Status               Run     Pass     Fail   CFail Errs
  3    1 Running                0        0        0       0    0
-----------------------------------------------------------------
```

The following table describes the status value for each module

Table 14: Shows the Status Value for Each Module

Status	Description
Running	OHMS test is running and there are no errors detected.
Failing	OHMS test has started to fail or in the process of failing.
Failed	OHMS test failed.
Stopped	OHMS test stopped. This is a transient state (for example, during upgrades and downgrades).
Exited	OHMS test process or thread exited while running the test.
Not Configured	OHMS test configured to not run on the module.
Int Failed	OHMS test failed because of internal failure.
Diag Failed	OHMS test failed in performing diagnostics.
Suspended	OHMS test suspended because of too many error conditions. OHMS cannot complete the test to determine the hardware status.
Halted	OHMS test is halted because the test is not intended to run on the module. (for example, a specific hardware of which a test is operating is not found on the module).
Enabled	OHMS is disabled by the user but not the test.
Disabled	OHMS test is disabled by the user.

Note Interface-specific counters will remain at zero unless the module-specific loopback test reports errors or failures.

The following example displays the loopback test time log for all modules:

```
switch# show system health statistics loopback timelog
-----------------------------------------------------------------
Mod        Samples     Min(usecs)     Max(usecs)     Ave(usecs)
  1           1872            149            364            222
  3           1862            415            743            549
  8           1865            134            455            349
-----------------------------------------------------------------
```

The following example displays the loopback test statistics for a specified module:

```
switch# show system health statistics loopback module 8 timelog
-----------------------------------------------------------------
Mod        Samples     Min(usecs)     Max(usecs)     Ave(usecs)
  8           1867            134            455            349
-----------------------------------------------------------------
```

The following example displays the loopback test statistics for an interface on a Cisco Fabric Switch for HP c-Class BladeSystem:

```
switch# show system health statistics loopback interface bay1
-----------------------------------------------------------------
Mod Port Status                Run     Pass     Fail   CFail Errs
  1   16 Running                 0        0        0       0    0
-----------------------------------------------------------------
```

The following example displays the frequency and status of the CRC checksum test and a flash update on a single module:

```
switch# show system health module 5
Current health information for module 5.
Test                    Frequency       Status          Action
-----------------------------------------------------------------
Bootflash                10 Sec         Running         Enabled
EOBC                      5 Sec         Running         Enabled
Loopback                  5 Sec         Running         Enabled
CF checksum               7 Days        Running         Enabled
CF re-flash              30 Days        Running         Enabled
-----------------------------------------------------------------
```

The following example displays the CRC checksum test and the flash update statistics on all modules:

```
switch# show system health statistics
Test statistics for module 2
-------------------------------------------------------------------------------
Test Name           State            Frequency  Run    Pass    Fail CFail Errs
-------------------------------------------------------------------------------
Bootflash           Running            10s     1130    1130       0     0    0
EOBC                Running             5s     2268    2268       0     0    0
Loopback            Running             5s     2279    2279       0     0    0
CF checksum         Failed             20s       11       0      23    12    0
CF re-flash         Suspended          30s       12       0       0     0   12
-------------------------------------------------------------------------------
```

```
Test statistics for module 3
------------------------------------------------------------------------------
Test Name           State            Frequency  Run    Pass    Fail CFail Errs
------------------------------------------------------------------------------
Bootflash           Running            10s     1295    1295       0     0    0
EOBC                Running             5s     2591    2591       0     0    0
------------------------------------------------------------------------------
Test statistics for module 4
------------------------------------------------------------------------------
Test Name           State            Frequency  Run    Pass    Fail CFail Errs
------------------------------------------------------------------------------
Bootflash           Running            10s     1299    1299       0     0    0
EOBC                Running             5s     2598    2598       0     0    0
Loopback            Running             5s     2598    2598       0     0    0
CF checksum         Running             7s     2275    2274       0     0    0
CF re-flash         Running            30s      434     434       0     0    0
------------------------------------------------------------------------------
Test statistics for module 5
------------------------------------------------------------------------------
Test Name           State            Frequency  Run    Pass    Fail CFail Errs
------------------------------------------------------------------------------
InBand              Running             5s     2615    2615       0     0    0
Bootflash           Running            10s     1307    1307       0     0    0
EOBC                Running             5s     2615    2615       0     0    0
Management Port     Running             5s     2615    2615       0     0    0
CF checksum         Running             7s     2289    2289       0     0    0
CF re-flash         Running            30s      437     436       0     0    0
------------------------------------------------------------------------------
```

Related Commands

Command	Description
system health module	Configures Online Health Management System (OHMS) features.

show system internal snmp lc

To display the active policies of the line card, use the show system internal snmp lc command.

show system internal snmp lc {**module-id**|**counters**}

Syntax Description

module-id	Specifies the module ID number.
counters	Displays the port monitor line card information for module counters.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.1(1b)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows the port monitor line card information:

```
switch# show system internal snmp lc 4
------------------------------------------------------------------------------
-----------
No. of ports monitored: 0
------------------------------------------------------------------------------
-----------
------------------------------------------------------------------------------
-----------
Ports:
Time since activation: 23:51:52 UTC Jun 30 2000
------------------------------------------------------------------------------
-----------
------------------------------------------------------------------------------
-----------
Counter          Threshold  Interval Rising Threshold event Falling Threshold
event In Use
-------          ---------  -------- ---------------- ----- ------------------ -
---- ------
Link Loss        Delta      60       5                4     1                  4
     Yes
Sync Loss        Delta      60       5                4     1                  4
--More--
switch#
```

The following example shows the port monitor line card information for the module counter:

```
switch# show system internal snmp lc counters
switch#
```

Related Commands

Command	Description
show port monitor active	Shows port monitor active policies.

show tacacs+

To display the TACACS+ Cisco Fabric Services (CFS) distribution status and other details, use the **show tacacs+** command.

show tacacs+ {**distribution status**|**pending**|**pending-diff**}

Syntax Description

distribution status	Displays the status of the TACACS+ CFS distribution.
pending	Displays the pending configuration that is not yet applied.
pending-diff	Displays the difference between the active configuration and the pending configuration.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, TACACS+ must be enabled using the **tacacs+ enable** command.

Examples

The following example shows how to display the TACACS+ distribution status:

```
switch# show tacacs+ distribution status
session ongoing: no
session db: does not exist
merge protocol status: merge activation done
last operation: none
last operation status: none
```

Related Commands

Command	Description
tacacs+ distribute	Initiates TACACS+ configuration distribution.
tacacs+ enable	Enables TACACS+.

show tacacs-server

To display all configured TACACS+ server parameters, use the **show tacacs-server** command.

show tacacs-server [{*server-nameipv4-addressipv6-address*}] [{**directed-request**|**groups**|**sorted**|**statistics**}]

Syntax Description

server-name	(Optional) Specifies the TACACS+ server DNS name. The maximum is 256.
ipv4-address	(Optional) Specifies the TACACS+ server IP address in the format *A.B.C.D* .
ipv6-address	(Optional) Specifies the TACACS+ server IP address in the format *X:X::X* .
directed-request	(Optional) Displays an enabled directed request TACACS+ server configuration.
groups	(Optional) Displays configured TACACS+ server group information.
sorted	(Optional) Displays TACACS+ server information sorted by name.
statistics	(Optional) Displays TACACS+ statistics for the specified TACACS+ server.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	• Added the *server-name* , *ipv4-address* , and *ipv6-address* arguments. • Added the **directed-request** and **statistics** options.

Usage Guidelines

None.

Examples

The following command displays the configured TACACS+ server information:

```
switch# show tacacs-server
Global TACACS+ shared secret:tacacsPword
timeout value:30
total number of servers:3
following TACACS+ servers are configured:
        171.71.58.91:
                available on port:2
        cisco.com:
                available on port:49
        171.71.22.95:
                available on port:49
                TACACS+ shared secret:MyKey
```

The following command displays the configured TACACS+ server groups:

```
switch# show tacacs-server groups
total number of groups:1
following TACACS+ server groups are configured:
        group TacServer:
                server 171.71.58.91 on port 2
```

show tech-support

To display information useful to technical support when reporting a problem, use the **show tech-support** command in EXEC mode.

show tech-support [{**aaa** |**aam** |**acl [details][commands]**|**all binary** {**bootflash:** |**logflash:** |**slot0:** }|**amm module** *number* |**analytics** |**assoc_mgr** |**biosd** |**bloggerd** |**bloggerd-all** |**bootvar** |**brief** |**callhome** |**cdp** |**cert-enroll**|**cfs** [**name** *application-name*]**[commands]**|**cli** |**clis [brief]**|**clock_manager** |**commands** |**dcbx** |**details** [{**include-time** |**commands**}]|**device-alias** |**dftm module** *number* |**dhcp** |**eem** |**eltm** [{**lc** {**vdc-once** |**vdc-specific**}**[detail]**|**sup-only**}]|**epp** |**eth-qos [server-only] [all][snmp]**|**ethpm** |**ethport** |**fc-management** |**fc-redirect** |**fc2 [commands]**|**fcdomain [commands]**|**fcns vsan** *id_range*|**fcoe [commands]**|**fcoe_mgr** |**fcs** |**fib module** *number*|**fib-all** |**flogi** |**forwarding** {**l2** |**l3** |**nve** |**otv**}**multicast[detail]**|**fspf [commands]**|**gold** |**gpixm**|**ha [standby][commands]**|**ilc_helper** |**im** |**inband** |**include-time** |**interface** |**l2fm** [{**binary** {**bootflash:** |**logflash:** |**slot0:** }|[{**clients** |**l2dbg**}][**module** *number*]|**[detail]**}]|**l2pt [detail]**|**lacp [all]**|**license** |**lim** |**link-diag [commands]**|**lldp** |**logging** |**module** {*number* |**all**}|**monitor** |**monitorc** |**monitorc-all**|**npacl [brief]**|**ntp** |**page [time-optimized]**|**pds [brief]**|**pfstat** |**pixm** |**pixm-all** |**pixmc** |**pixmc-all** |**pktmgr [brief]**|**plsm** |**pltfm-config** |**pnp** |**port** |**port-channel** |**port-security** [**vsan** *id_range*]|**qos** |**radius** |**rib**|**rlir** [**vsan** *id_range*]|**rscn** [**vsan** *id_range*]|**security** |**session-mgr** |**slowdrain [commands]**|**snm** |**snmp** |**stats_client** |**stp** |**sup-filesys**|**sysmgr [commands]**|**tacacs+** |**telemetry** |**time-optimized [include-time]**|**vlan** |**vntagc-all** |**vrrp** |**vsan** *id_range* **[commands]**|**vshd** |**xml** |**zone vsan** *id_range* **[commands]**}]

Note On a Cisco Fabric Switch for HP c-Class BladeSystem and on a Cisco Fabric Switch for IBM BladeCenter, the syntax differs from **interface fc** *slot*/*port* as follows:**interface** {**bay** *port* | **ext** *port* }

Syntax Description

aaa	(Optional) Displays information for authentication, authorization, and accounting (AAA) troubleshooting.
aam	(Optional) Displays information for Abstract ACL Manager troubleshooting.
acl	(Optional) Displays information for ACL troubleshooting.
all	(Optional) Collects detailed information of all applications for troubleshooting.
amm module *number*	(Optional) Collects detailed information for Advanced Management Module (AMM) troubleshooting.
analytics	(Optional) Collects detailed information for analytics troubleshooting.
assoc_mgr	(Optional) Collects detailed information for assoc_mgr troubleshooting.
binary	Collects detailed information of all applications in binary format for troubleshooting.
biosd	(Optional) Collects BIOS install log for troubleshooting.
bloggerd	(Optional) Collects detailed information for bloggerd troubleshooting.
bloggerd-all	(Optional) Collects detailed information from all modules for bloggerd troubleshooting.

bootflash:	Bootflash directory.
bootvar	(Optional) Displays information for bootvar troubleshooting.
brief	(Optional) Displays a summary of the information for a component.
callhome	(Optional) Displays callhome troubleshooting information.
cdp	(Optional) Collect information for Cisco Discovery Protocol (CDP) troubleshooting.
cert-enroll	(Optional) Displays certificates information.
cfs	(Optional) Displays information for Cisco Fabric Services (CFS) troubleshooting.
cli	(Optional) Collects information for parser troubleshooting.
clients module *number*	(Optional) Displays information of the L2FM troubleshooting.
clis	(Optional) Collects information for CLI server troubleshooting.
clock_manager	(Optional) Collects information for clock manager troubleshooting.
commands	(Optional) Show commands that are executed as part of show tech-support commands.
dcbx	(Optional) Collects information for Data Center Bridging Exchange (DCBX) component.
details	(Optional) Displays detailed information for each **show** command.
device-alias	(Optional) Displays device alias information.
dftm module *number*	(Optional) Collects information for DFTM troubleshooting.
dhcp	(Optional) Collects information for DHCP troubleshooting.
eem	(Optional) Displays Embedded Event Manager (EEM) information for troubleshooting.
eltm	(Optional) Collects information for ELTM troubleshooting.
epp	(Optional) Collects information for exchange peer parameters (EPP) troubleshooting.
ethpm	(Optional) Collects information for Ethernet port manager (ethpm) troubleshooting.
ethport	(Optional) Collects information for Ethernet port (ethport) troubleshooting.
eth-qos	(Optional) Displays IP QoS manager information for troubleshooting.
fc2	(Optional) Displays fc2 information for troubleshooting.
fcdomain	(Optional) Displays information for Fibre Channel domain troubleshooting.

fc-management	(Optional) Displays Fibre Channel Common Transport (FC-CT) Management Security information for troubleshooting.
fcns	(Optional) Displays information for Fibre Channel Naming Server (FCNS) troubleshooting.
fcoe	(Optional) Collects information for Fibre Channel over Ethernet (FCoE) troubleshooting.
fcoe_mgr	(Optional) Collects information for Fibre Channel over Ethernet (FCoE) Manager troubleshooting.
fc-redirect	(Optional) Displays information for Fibre Channel redirect information troubleshooting.
fcs	(Optional) Collects information for Fabric Configuration Server (FCS) troubleshooting.
fib module *number*	(Optional) Collects information for Fibre Channel and FCoE FIB troubleshooting.
fib-all	(Optional) Collects information from all modules for Fibre Channel and FCoE FIB troubleshooting.
flogi	(Optional) Collects information for fabric login (FLOGI) troubleshooting.
forwarding	(Optional) Forwarding debug information.
fspf	(Optional) Displays information for FSPF troubleshooting.
gold	(Optional) Displays information for Generic Online Diagnostics (GOLD) troubleshooting.
gpixm	(Optional) Collects information for global PIXM troubleshooting.
ha	(Optional) Collects information for high availability (HA) troubleshooting.
ilc_helper	(Optional) Collects information for intelligent line card (ILC) helper troubleshooting.
im	(Optional) Collects information for IM troubleshooting.
inband	(Optional) Displays information for in-band management troubleshooting.
include-time	(Optional) Collects the tech-support information and captures the time taken to execute each command.
interface	(Optional) Collects information for interface level troubleshooting.
l2	Layer 2 debugging information.
l2dbg module *number*	(Optional) Captures additional information of the L2FM clients running on modules for troubleshooting.
l2fm	(Optional) Displays information for L2FM troubleshooting.

l2pt	(Optional) Displays information for L2PT troubleshooting.
l3	Layer 3 debugging information.
lacp	(Optional) Displays information for Link Aggregation Control Protocol (LACP) troubleshooting.
lc	(Optional) Collects information for modules troubleshooting only.
license	(Optional) Displays licensing information.
lim	(Optional) Collects information for LIM troubleshooting.
link-diag	(Optional) Collects information for link diagnostics troubleshooting.
lldp	(Optional) Collects information for Link Layer Discovery Protocol (LLDP) troubleshooting.
logflash:	Logflash directory.
logging	(Optional) Displays information for logging troubleshooting.
monitor	(Optional) Displays information for monitor troubleshooting.
monitorc	(Optional) Displays information for monitorc troubleshooting.
monitorc-all	(Optional) Displays information for module monitorc troubleshooting.
multicast	Multicast debugging information.
name *application-name*	(Optional) Specifies an application that uses the CFS infrastructure. Maximum length is 64 characters.
npacl	(Optional) Displays information for npacl troubleshooting.
ntp	(Optional) Displays information for Network Time Protocol (NTP) troubleshooting.
nve	Network Virtualization Edge (NVE) debugging information.
otv	Overlay Transport Virtualization (OTV) debugging information.
page	(Optional) Displays tech-support information page wise.
pds	(Optional) Displays PDS information for troubleshooting.
pfstat	(Optional) Collects information for pfstat troubleshooting.
pixm	(Optional) Collects information for local VDC PIXM troubleshooting.
pixm-all	(Optional) Collects information for PIXM troubleshooting.
pixmc	(Optional) Collects information for PIXMC troubleshooting.
pixmc-all	(Optional) Collects information for module PIXMC troubleshooting.
pktmgr	(Optional) Displays packet manager information for troubleshooting.

plsm	(Optional) Displays information for PLSM troubleshooting.
pltfm-config	(Optional) Collects information for platform configuration troubleshooting.
pnp	(Optional) Displays plug and play information for troubleshooting.
port	(Optional) Displays information for port manager troubleshooting.
port-channel	(Optional) Displays information for PortChannel troubleshooting.
port-security	(Optional) Displays information for port security troubleshooting.
qos	(Optional) Displays information for QoS troubleshooting.
radius	(Optional) Displays information for radius troubleshooting.
rib	(Optional) Collects information for routing information base (RIB) troubleshooting.
rlir	(Optional) Displays information for Registered Link Incident Report (RLIR) troubleshooting.
rscn	(Optional) Displays information for Registered State Change Notification (RSCN) troubleshooting.
security	(Optional) Displays information for security troubleshooting.
server-only	(Optional) Displays only IP QoS manager server information for troubleshooting.
session-mgr	(Optional) Collects information for session manager troubleshooting.
slot0:	External storage directory.
slowdrain	(Optional) Collects information for slowdrain troubleshooting.
snm	(Optional) Displays information for SNM troubleshooting.
snmp	(Optional) Displays information for SNMP troubleshooting.
standby	(Optional) Collects information from standby supervisor for high availability (HA) troubleshooting.
stats_client	(Optional) Displays information for status client troubleshooting.
stp	(Optional) Displays information for Spanning Tree Protocol (STP) troubleshooting.
sup-filesys	(Optional) Displays information for system file troubleshooting.
sup-only	(Optional) Collects only supervisor specific information for troubleshooting.
sysmgr	(Optional) Displays information for system management troubleshooting.
tacacs+	(Optional) Displays information for Terminal Access Controller Access Control device Plus (TACACS+) troubleshooting.
telemetry	(Optional) Displays information for telemetry troubleshooting.

time-optimized	(Optional) Collects tech-support information faster, but requires more memory and disk space.
vdc-once	Collects information for all modules.
vdc-specific	Collects only virtual device context (VDC) specific information.
vlan	(Optional) Collects information for VLAN troubleshooting.
vntagc-all	(Optional) Collects information for module VNTAGC troubleshooting.
vrrp	(Optional) Displays information for Virtual Router Redundancy Protocol (VRRP) troubleshooting.
vsan *vsan-id*	Displays information for VSAN troubleshooting. Specifies a VSAN ID. The range is 1 to 4093.
vshd	(Optional) Displays information for VSHD troubleshooting.
xml	(Optional) Collects information for XML troubleshooting.
zone	Displays information for zone server troubleshooting.

Command Default

The default output of the **show tech-support** command includes the output of the following **show** commands:

- show version
- show environment
- show module
- show hardware
- show running-config
- show interface
- show accounting log
- show process
- show process log
- show processes log details
- show flash

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.
3.0(1)	Added the **fcdomain**, **port-channel**, and **zone** options.

Release	Modification
3.0(3)	Added the **cfs**, **fcip**, **fspf**, **fta**, **ip**, **license**, **prefpath**, and **vrrp** options.
3.1(1)	Added the **device-alias** keyword.
3.1(2)	Added the **bay** *port* **| ext** *port* keywords and arguments.

Usage Guidelines

The **show tech-support** command is useful when collecting a large amount of information about your switch for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem.

The **show tech-support** command displays the output of several **show** commands at once. The output from this command varies depending on your configuration. Use the **show tech-support** command in EXEC mode to display general information about the switch when reporting a problem.

You can choose to have detailed information for each command or even specify the output for a particular interface, module, or VSAN.

Examples

The following example displays technical support information for a specific module:

```
switch# show tech-support module 1
'terminal length 0'
'show module '
Mod  Ports  Module-Type                      Model              Status
---  -----  -------------------------------- ------------------ ------------
1    16     1/2 Gbps FC/Supervisor           DS-X9216-K9-SUP    active *
2    32     1/2 Gbps FC Module               DS-X9032           ok
Mod  Sw           Hw      World-Wide-Name(s) (WWN)
---  -----------  ------  --------------------------------------------------
1    1.0(0.271)   0.0     20:01:00:05:30:00:21:9e to 20:10:00:05:30:00:21:9e
2    1.0(0.271)   0.0     20:41:00:05:30:00:21:9e to 20:60:00:05:30:00:21:9e
Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-05-30-00-40-b6 to 00-05-30-00-40-ba
2    00-05-30-00-11-22 to 00-05-30-00-11-26
* this terminal session
'show environment'
Clock:
----------------------------------------------------------
Clock           Model                Hw         Status
----------------------------------------------------------
A               Clock Module         --         ok/active
B               Clock Module         --         ok/standby
Fan:
----------------------------------------------------
Fan             Model                Hw         Status
----------------------------------------------------
Chassis         DS-2SLOT-FAN         0.0        ok
PS-1            --                   --         ok
PS-2            --                   --         absent
Temperature:
-------------------------------------------------------------------
Module   Sensor   MajorThresh   MinorThres   CurTemp     Status
                  (Celsius)     (Celsius)    (Celsius)
-------------------------------------------------------------------
1        1        75           60           30          ok
1        2        65           50           28          ok
1        3        -127         -127         40          ok
```

```
1        4        -127          -127          36          ok
2        1        75            60            32          ok
2        2        65            50            26          ok
2        3        -127          -127          41          ok
2        4        -127          -127          31          ok
```

The **show tech-support brief** command provides a summary of the current running state of the switch.

```
switch# show tech-support brief
Switch Name           : vegas01
Switch Type           : DS-X9216-K9-SUP
Kickstart Image       : 1.3(2a) bootflash:///m9200-ek9-kickstart-mz.1.3.1.10.bin
System Image          : 1.3(2a) bootflash:///m9200-ek9-mz.1.3.1.10.bin
IP Address/Mask       : 10.76.100.164/24
Switch WWN            : 20:00:00:05:30:00:84:9e
No of VSANs           : 9
Configured VSANs      : 1-6,4091-4093
VSAN    1:    name:VSAN0001, state:active, interop mode:default
              domain id:0x6d(109), WWN:20:01:00:05:30:00:84:9f [Principal]
              active-zone:VR, default-zone:deny
VSAN    2:    name:VSAN0002, state:active, interop mode:default
              domain id:0x7d(125), WWN:20:02:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny
VSAN    3:    name:VSAN0003, state:active, interop mode:default
              domain id:0xbe(190), WWN:20:03:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny
VSAN    4:    name:VSAN0004, state:active, interop mode:default
              domain id:0x5a(90), WWN:20:04:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny
VSAN    5:    name:VSAN0005, state:active, interop mode:default
              domain id:0x13(19), WWN:20:05:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny
VSAN    6:    name:VSAN0006, state:active, interop mode:default
              domain id:0x1f(31), WWN:20:06:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny
VSAN 4091:    name:VSAN4091, state:active, interop mode:default
              domain id:0x08(8), WWN:2f:fb:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny
VSAN 4092:    name:VSAN4092, state:active, interop mode:default
              domain id:0x78(120), WWN:2f:fc:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny
VSAN 4093:    name:VSAN4093, state:active, interop mode:default
              domain id:0x77(119), WWN:2f:fd:00:05:30:00:84:9f [Principal]
              active-zone:<NONE>, default-zone:deny
--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          FCOT   Oper  Oper   Port
                  Mode   Trunk                          Mode  Speed  Channel
                         Mode                                (Gbps)
--------------------------------------------------------------------------------
fc1/1      1      auto   on      fcotAbsent       --     --           --
fc1/2      1      auto   on      fcotAbsent       --     --           --
fc1/3      1      auto   on      fcotAbsent       --     --           --
fc1/4      1      auto   on      fcotAbsent       --     --           --
fc1/5      1      auto   on      notConnected     swl    --           --
fc1/6      1      auto   on      fcotAbsent       --     --           --
fc1/7      1      auto   on      fcotAbsent       --     --           --
fc1/8      1      auto   on      fcotAbsent       --     --           --
fc1/9      1      auto   on      fcotAbsent       --     --           --
fc1/10     1      auto   on      fcotAbsent       --     --           --
fc1/11     1      auto   on      fcotAbsent       --     --           --
fc1/12     1      auto   on      fcotAbsent       --     --           --
fc1/13     1      auto   on      fcotAbsent       --     --           --
```

```
fc1/14     1      auto   on      fcotAbsent       --     --           --
fc1/15     1      auto   on      fcotAbsent       --     --           --
fc1/16     1      auto   on      fcotAbsent       --     --           --
-------------------------------------------------------------------------------
Interface          Status                          Speed
                                                   (Gbps)
-------------------------------------------------------------------------------
sup-fc0            up                              1
-------------------------------------------------------------------------------
Interface               Status     IP Address        Speed        MTU
-------------------------------------------------------------------------------
mgmt0                   up         10.76.100.164/24  100 Mbps     1500
Power Supply:
------------------------------------------------------
PS  Model                Power     Power       Status
                         (Watts)   (Amp @42V)
------------------------------------------------------
1   WS-CAC-950W          919.38    21.89       ok
2                        --        --          absent
Mod Model                Power     Power       Power     Power       Status
                         Requested Requested   Allocated Allocated
                         (Watts)   (Amp @42V)  (Watts)   (Amp @42V)
--- -------------------  -------   ----------  --------- ----------  ----------
1    DS-X9216-K9-SUP     220.08    5.24        220.08    5.24        powered-up
2    DS-X9032            199.92    4.76        199.92    4.76        powered-up
Power Usage Summary:
--------------------
Power Supply redundancy mode:                   redundant
Total Power Capacity                            919.38   W
Power reserved for Supervisor(s)[-]             220.08   W
Power reserved for Fan Module(s)[-]             47.88    W
Power currently used by Modules[-]              199.92   W
                                                -------
Total Power Available                           451.50
```

The following example displays zone server information for VSAN 1:

```
switch# show tech-support zone vsan 1
`show zone status vsan 1`
VSAN: 1 default-zone: permit distribute: active only Interop: default
    mode: basic merge-control: allow session: none
    hard-zoning: enabled
Default zone:
    qos: disabled broadcast: disabled ronly: disabled
Full Zoning Database :
    Zonesets:0  Zones:0 Aliases: 0
Active Zoning Database :
    Name: vhost-zone  Zonesets:1  Zones:9
Status: Activation failed [Error: Unknown error Dom 21]:
        at 23:36:44 UTC Dec 19 2005
```

The following example displays a partial listing of output from the **show tech-support device-alias** command:

```
switch# show tech-support device-alias
`show device-alias database`
device-alias name dev2 pwwn 10:00:00:00:c9:2e:31:37
device-alias name sdv1 pwwn 50:00:53:00:00:85:c0:01
device-alias name svc1 pwwn 20:0f:00:05:30:00:eb:48
device-alias name sdv-1 pwwn 50:00:53:00:00:e9:7f:a1
device-alias name sdv-2 pwwn 50:00:53:00:01:4e:af:a1
device-alias name sdv-3 pwwn 50:00:53:00:01:da:2f:a1
device-alias name sdv-4 pwwn 50:00:53:00:01:cb:af:a1
```

```
device-alias name qloGics pwwn 21:00:00:e0:8b:06:61:d4
device-alias name sdv-501 pwwn 50:00:53:00:00:85:c1:f5
device-alias name sym-hba1 pwwn 50:06:04:82:ca:e1:26:83
device-alias name fred-hba1 pwwn 22:00:00:20:37:d2:03:ed
device-alias name fred-hba2 pwwn 22:00:00:20:37:d2:10:f9
device-alias name sdv1-4001 pwwn 50:00:53:00:01:0f:0f:a1
device-alias name sdv2-4001 pwwn 50:00:53:00:00:66:4f:a1
device-alias name HDS33074-C pwwn 50:06:0e:80:03:81:32:06
device-alias name clarion2345 pwwn 50:06:01:61:10:60:14:f5
device-alias name iscsi-alias pwwn 27:09:00:08:00:ad:00:03
device-alias name seaGate0306 pwwn 22:00:00:20:37:d2:03:d6
Total number of entries = 18
```

show tech-support fc-management

To display the Fibre Channel Common Transport (FC-CT) management security technical support information, use the show tech-support fc-management command.

show tech-support fc-management

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
6.2(9)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the FC-CT management security technical support information:

```
switch(config)# show tech-support fc-management
`show fc-management status`
Mgmt Security Enabled
`show fc-management database`
Fc-Management Security Database
---------------------------------------------------------------
VSAN       PWWN              FC-CT Permissions per FC services
---------------------------------------------------------------
1    01:01:01:01:01:01:01:01   Zone(RW), Unzoned-NS(RW), FCS(RW), FDMI(RW)
---------------------------------------------------------------
Total 1 entries
 `show fc-management shared-db`
Empty Database
switch(config)#
```

Related Commands

Command	Description
show fc-management	Displays the FC-CT management security information.

show tech-support sme

To display the information for Cisco SME technical support, use the **show tech-support sme** command.

show tech-support sme compressed bootflash:|tftp:

Syntax Description

compressed	Saves the compressed Cisco SME .
bootflash:	Specifies the filename that need to be stored.
tftp:	Specifies the filename that need to be stored.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
3.3(1c)	This command was introduced.
NX-OS 4.1(1c)	Added the Command output.

Usage Guidelines

None.

Examples

The following example displays the information for SME technical support:

```
sw-sme-n1# show tech-support sme
'show startup-config'
version 4.1(1)
username admin password 5 $1$jC/GIid6$PuNDstXwdAnwGaxxjdxi50  role network-admin
no password strength-check
feature telnet
ntp server 10.81.254.131
kernel core target 0.0.0.0
kernel core limit 1
aaa group server radius radius
snmp-server user admin network-admin auth md5 0x7eedfdadb219506ca61b0e2957cc7ef5
 priv 0x7eedfdadb219506ca61b0e2957cc7ef5 localizedkey
snmp-server host 171.71.49.157 informs version 2c public  udp-port 2162
snmp-server enable traps license
snmp-server enable traps entity fru
device-alias database
  device-alias name sme-host-171-hba0 pwwn 21:01:00:e0:8b:39:d7:57
  device-alias name sme-host-171-hba1 pwwn 21:00:00:e0:8b:19:d7:57
  device-alias name sme-host-172-hba0 pwwn 21:01:00:e0:8b:39:c2:58
  device-alias name sme-host-172-hba1 pwwn 21:00:00:e0:8b:19:c2:58
  device-alias name sme-sanblaze-port0-tgt0 pwwn 2f:ff:00:06:2b:0d:39:08
  device-alias name sme-sanblaze-port0-tgt1 pwwn 2f:df:00:06:2b:0d:39:08
--More--
```

show telnet server

To display the state of the Telnet access configuration, use the **show telnet server** command.

show telnet server

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the status of the Telnet server:

```
switch# show telnet server
telnet service enabled
```

show terminal

To display the terminal information, use the **show terminal** command

show terminal

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays terminal information:

```
switch# show terminal
TTY:  Type: "vt100"
Length: 25 lines, Width: 80 columns
Session Timeout: 30 minutes
```

show tlport

To display configured TL port information, use the **show tlport** command

show tlport {**alpa-cache**|**discapp fcid** *fcid-id* [**vsan** *vsan-id*] **[verbose]**|**interface fc** *slot / port* {**all**|**private**|**proxied**|**topology**|**unsupported**}|**list** [**vsan** *vsan-id*]}

Syntax Description

alpa-cache	Displays the contents of the ALPA cache.
discapp	Displays private N port parameters.
fcid *fcid-id*	Specifies the FCID of the N port.
vsan *vsan-id*	(Optional) Specifies the N port VSAN ID. The range is 1 to 4093.
verbose	(Optional) Specifies the verbose mode.
interface	Displays TL ports in the selected interface.
fc *slot*/*port*	Specifies the Fiber Channel interface at the specified slot and port.
all	Displays all proxied and private devices on this TL port.
private	Displays all private devices on this TL port.
proxied	Displays all proxied devices on this TL port.
topology	Displays loop topology for this TL port.
unsupported	Displays all unsupported devices on this TL port.
list	Displays TL ports in all VSANs.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 5.0 and later releases	This command was deprecated.
1.0(2)	This command was introduced.

Usage Guidelines

The **show tlport** command displays the TL port interface configurations. This command provides a list of all TL ports configured on a box and displays the associated VSAN, the FCID for the port (only domain and area are valid), and the current operational state of the TL port (up or initializing).

Examples

The following example displays the TL ports in all VSANs:

```
switch# show tlport list
-------------------------------
Interface Vsan FC-ID    State
------------------------ ------
fc1/16    1    0x420000 Init
fc2/26    1    0x150000 Up
```

The following example displays the detailed information for a specific TL port:

```
switch# show tlport interface fc1/16 all
fc1/16 is up, vsan 1, FCID 0x420000
-------------------------------------------------------------------------------- alpa pWWN
                    nWWN                    SCSI Type Device  FC-ID
-------------------------------------------------------------------------------- 0x01
20:10:00:05:30:00:4a:de 20:00:00:05:30:00:4a:de Initiator Proxied 0xfffc42 0x73
22:00:00:20:37:39:ae:54 20:00:00:20:37:39:ae:54 Target    Private 0x420073 0xef
20:10:00:05:30:00:4a:de 20:00:00:05:30:00:4a:de Initiator Switch  0x0000ef
```

The following example displays TL port information for private devices:

```
switch# show tlport int fc1/16 pri
fc1/16 is up, vsan 1, FCID 0x420000
---------------------------------------------------------------------------
alpa pWWN                   nWWN                    SCSI Type FC-ID
---------------------------------------------------------------------------
0x73 22:00:00:20:37:39:ae:54 20:00:00:20:37:39:ae:54 Target    0x420073
0x74 22:00:00:20:37:38:d3:de 20:00:00:20:37:38:d3:de Target    0x420074
```

The following example displays TL port information for proxied devices:

```
switch# show tlport int fc1/16 prox

fc1/16 is up, vsan 1, FCID 0x420000
---------------------------------------------------------------------------
alpa pWWN                   nWWN                    SCSI Type FC-ID
---------------------------------------------------------------------------
0x01 20:10:00:05:30:00:4a:de 20:00:00:05:30:00:4a:de Initiator 0xfffc42
0x02 21:00:00:e0:8b:01:95:e7 20:00:00:e0:8b:01:95:e7 Initiator 0x420100
```

The following example displays the contents of the alpa-cache:

```
switch# show tlport alpa-cache
-----------------------------------------------------
alpa              pWWN               Interface
-----------------------------------------------------
0x02  22:00:00:20:37:46:09:bd     fc1/2
0x04  23:00:00:20:37:46:09:bd     fc1/2
```

show topology

To display topology information for connected switches, use the **show topology** command.

show topology [**vsan vsan-id**]

Syntax Description

vsan *vsan-id*	(Optional) Displays information for a VSAN. The range is 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(9)	Added a note.
2.0(x)	This command was introduced.

Usage Guidelines

None.

Note In scenarios where the show topology command output has few missing parameters like switchname, IP address etc. Please re-execute this command after few seconds.

Examples

The following example displays topology information:

```
switch# show topology

FC Topology for VSAN 1 :
--------------------------------------------------------------------------------
       Interface  Peer Domain Peer Interface     Peer IP Address(Switch Name)
--------------------------------------------------------------------------------
           fc4/15 0xef(239)            fc1/4  10.126.74.188(sw1-gd99)

FC Topology for VSAN 2 :
--------------------------------------------------------------------------------
       Interface  Peer Domain Peer Interface     Peer IP Address(Switch Name)
--------------------------------------------------------------------------------
           fc4/15 0x6e(110)            fc1/4  10.126.74.188(sw1-gd99)

FC Topology for VSAN 17 :
--------------------------------------------------------------------------------
       Interface  Peer Domain Peer Interface     Peer IP Address(Switch Name)
--------------------------------------------------------------------------------
           fc4/15  0x0c(12)            fc1/4  10.126.74.188(sw1-gd99)

FC Topology for VSAN 27 :
--------------------------------------------------------------------------------
       Interface  Peer Domain Peer Interface     Peer IP Address(Switch Name)
```

```
--------------------------------------------------------------------------------
            fc4/1  0x62(98)         Port 10   10.126.74.183(Brocade4100_110)
           fc4/10  0x41(65)            fc1/3  10.126.74.188(sw1-gd99)
           fc4/12  0x62(98)          Port 7   10.126.74.183(Brocade4100_110)
           fc4/13  0x62(98)         Port 13   10.126.74.183(Brocade4100_110)
           fc4/15  0x41(65)            fc1/4  10.126.74.188(sw1-gd99)

FC Topology for VSAN 72 :
--------------------------------------------------------------------------------
       Interface  Peer Domain Peer Interface     Peer IP Address(Switch Name)
--------------------------------------------------------------------------------
           fc4/15 0x9d(157)            fc1/4  10.126.74.188(sw1-gd99)

FC Topology for VSAN 99 :
--------------------------------------------------------------------------------
       Interface  Peer Domain Peer Interface     Peer IP Address(Switch Name)
--------------------------------------------------------------------------------
           fc4/15 0xd3(211)            fc1/4  10.126.74.188(sw1-gd99)

FC Topology for VSAN 311 :
--------------------------------------------------------------------------------
       Interface  Peer Domain Peer Interface     Peer IP Address(Switch Name)
--------------------------------------------------------------------------------
           fc4/15  0x0c(12)            fc1/4  10.126.74.188(sw1-gd99)

FC Topology for VSAN 312 :
--------------------------------------------------------------------------------
       Interface  Peer Domain Peer Interface     Peer IP Address(Switch Name)
--------------------------------------------------------------------------------
           fc4/15 0x66(102)            fc1/4  10.126.74.188(sw1-gd99)
```

show topology isl

To display ISL topology information for connected switches, use the **show topology** isl command.

show topology isl {**detail**|**port-channel port-channel number detail**|**vsan vsan-id**}

Syntax Description

isl	Displays ISL topology information.
detail	Displays the detailed ISL topology information.
port-channel	Displays the port channel topology information.
port-channel number	Displays the port channel number. The range is from 1 to 256.
vsan	Displays information for a VSAN.
vsan-id	Displays VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the ISL topology information:

```
switch1-12345# show topology isl
```

__________Local________	_______
PC	Domain

-	0x01
-	0x01

2	0x01
2	0x01
4	0x01
4	0x01
5	0x01
5	0x01
6	0x01
6	0x01
7	0x01
7	0x01

```
switch1-12345#
```

The following example displays the detailed ISL topology information:

```
switch1-12345# show topology isl detail
```

_____Local_____
PC

-
-
2

2
4
4
5
5
6
6
7
7

```
switch1-12345#
```

The following example displays ISL port channel topology information:

```
switch1-12345# show topology isl port-channel 4
```

___________Local_____________	__
PC	Do

4	0x
4	0x
4	0x
4	0x
4	0x

4	0x01
4	0x01
4	0x01

```
switch1-12345#
```

The following example displays detailed ISL port channel topology information:

```
switch1-12345# show topology isl port-channel 4 detail
```

```
--------------------------------------------------------------------------------
_____________Local___________
PC
--------------------------------------------------------------------------------
4
4
4
4
4
4
4
4
```

```
switch1-12345#
```

The following example displays the VSAN ID topology information:

```
switch1-12345# show topology isl vsan 100
```

__________Local_________	_____
PC	Domain

-	0x01
-	0x01
2	0x01
2	0x01
4	0x01
4	0x01
5	0x01
5	0x01
6	0x01
6	0x01
7	0x01
7	0x01

```
switch1-12345#
```

The following example displays the detailed VSAN ID topology information:

```
switch1-12345# show topology isl vsan 100 detail
```

_____Local_____
PC

-
-
2
2
4
4
5
5
6
6
7
7

```
switch1-12345#
```

show trunk protocol

To display trunk protocol status, use the **show trunk protocol** command.

show trunk protocol

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays trunk protocol status:

```
switch# show trunk protocol
Trunk protocol is enabled
```

show user-account

To display configured information about user accounts, use the **show user-account** command.

show user-account [{**user-name**|**iscsi**}]

Syntax Description

user-name	(Optional) Specifies the user name.
iscsi	(Optional) Displays the iSCSI user account information.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays information for a specified user:

```
switch# show user-account user1
user:user1
        this user account has no expiry date
        roles:network-operator
no password set. Local login not allowed
Remote login through RADIUS is possible
```

The following example displays information for all users:

```
switch# show user-account
show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:usam
        expires on Sat May 31 00:00:00 2003
        roles:network-admin network-operator
user:msam
        this user account has no expiry date
        roles:network-operator
user:user1
        this user account has no expiry date
        roles:network-operator
no password set. local login not allowed
Remote login through RADIUS is possible
```

show username

To display username information (print the public key part of user keypair information), use the show username command.

show username username keypair

Syntax Description

username	Specifies name of the user.
keypair	Specifies SSH keypairs.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display username information:

```
switch# show username admin keypair
**************************************
rsa Keys generated:Tue Sep  1 01:27:38 2009
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEA5KCbN1Yc5X8HbFZybBNa+sXMzBHGOj1jbuZGXJ3VKH3m
LTz4b9ceyP4FyeHR7QHxBPBr3jJ3zG9rioATOwaG7944F/cadU3THDkQXN0JCVnKrqTdOo5uiIeRe2Mu
MEPfIvnM7MkJGJC2mPHRQKHlF+R3UtJaeAWuiRdKLaKS8Y0=
bitcount:1024
fingerprint:
3f:a6:31:9c:e3:1f:12:e4:49:c9:20:3c:69:6f:d1:67
**************************************
dsa Keys generated:Tue Sep  1 01:38:12 2009
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEA5KCbN1Yc5X8HbFZybBNa+sXMzBHGOj1jbuZGXJ3VKH3m
LTz4b9ceyP4FyeHR7QHxBPBr3jJ3zG9rioATOwaG7944F/cadU3THDkQXN0JCVnKrqTdOo5uiIeRe2Mu
MEPfIvnM7MkJGJC2mPHRQKHlF+R3UtJaeAWuiRdKLaKS8Y0=
bitcount:1024
fingerprint:
3f:a6:31:9c:e3:1f:12:e4:49:c9:20:3c:69:6f:d1:67
**************************************
switch#
```

Related Commands

Command	Description
role	Configures user roles.
show username	Displays username information.

show users

To display all CLI users currently accessing the switch, use the **show users** command.

show users

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays all users:

```
switch# show users
admin    pts/7        Jan 12 20:56 (10.77.202.149)
admin    pts/9        Jan 12 23:29 (modena.cisco.com)
admin    pts/10       Jan 13 03:05 (dhcp-171-71-58-120.cisco.com)
admin    pts/11       Jan 13 01:53 (dhcp-171-71-49-49.cisco.com)
```

show version

To display the version of system software that is currently running on the switch, use the **show version** command.

show version [{**clock-module epld**|**epld** *url*|**image** {**bootflash:**|**slot0:**|**volatile:**} *image-filename*|**module** *slot* **[epld]**}]

Syntax Description

clock-module	(Optional) Displays all current EPLD versions on the clock module.
epld	(Optional) Displays all current versions of EPLDs on a specified module.
epld *url*	(Optional) Displays all EPLD versions that are available at the specified URL (bootflash:, ftp:, scp:, sftp:, slot0:, tftp:, or volatile:)
image	(Optional) Displays the software version of a given image.
bootflash:	(Optional) Specifies internal bootflash memory.
slot0:	(Optional) Specifies CompactFlash memory or PCMCIA card.
volatile:	(Optional) Specifies the volatile directory.
image-filename	(Optional) Specifies the name of the system or kickstart image.
module *slot*	(Optional) Displays the software version of a module in the specified slot.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
1.0(3)	Command was modified.
3.0(1)	Added the **clock-module** option.
NX-OS 4.1(1b)	Changed the command output from SAN-OS to NX-OS.

Usage Guidelines

Use the **show version image** command to verify the integrity of the image before loading the images. This command can be used for both the system and kickstart images.

Use the **show version** command to verify the version on the active and standby supervisor modules before and after an upgrade.

Examples

The following examples display the versions of the system, kickstart, and failed images:

```
switch(boot)# show version image bootflash:system_image
<------------
system image
 image name: m9500-sf1ek9-mz.1.0.3.bin
 system:     version 1.0(3)
 compiled:   10/25/2010 12:00:00
switch(boot)# show version image bootflash:kickstart_image
<-------------
kickstart image
  image name: m9500-sf1ek9-kickstart-mz.1.0.3.upg.bin
  kickstart:  version 1.0(3)
  loader:     version 1.0(3)
  compiled:   10/25/2010 12:00:00
switch# show version image bootflash:bad_image
 <--------------
failure case
Md5 Verification Failed
Image integrity check failed
```

The following example displays current EPLD versions for a specified module.

```
switch# show version module 2 epld
Module Number                       2
EPLD Device                   Version
------------------------------------
Power Manager                    0x06
XBUS IO                          0x07
UD chip Fix                      0x05
Sahara                           0x05
```

The following example displays available EPLD versions.

```
switch# show version epld bootflash:m9000-epld-2.0.1b.img
MDS series EPLD image, built on Mon Sep 20 16:39:36 2004
Module Type                          EPLD Device         Version
------------------------------------------------------------------
MDS 9500 Supervisor 1                XBUS 1 IO              0x09
                                     XBUS 2 IO              0x0c
                                     UD Flow Control        0x05
                                     PCI ASIC I/F           0x04
1/2 Gbps FC Module (16 Port)         XBUS IO                0x07
                                     UD Flow Control        0x05
                                     PCI ASIC I/F           0x05
1/2 Gbps FC Module (32 Port)         XBUS IO                0x07
                                     UD Flow Control        0x05
                                     PCI ASIC I/F           0x05
Advanced Services Module             XBUS IO                0x07
                                     UD Flow Control        0x05
                                     PCI ASIC I/F           0x05
                                     PCI Bridge             0x05
IP Storage Services Module (8 Port)  Power Manager          0x07
                                     XBUS IO                0x03
                                     UD Flow Control        0x05
                                     PCI ASIC I/F           0x05
                                     Service Module I/F     0x0a
                                     IPS DB I/F             0x1a
IP Storage Services Module (4 Port)  Power Manager          0x07
                                     XBUS IO                0x03
                                     UD Flow Control        0x05
                                     PCI ASIC I/F           0x05
                                     Service Module I/F     0x1a
Caching Services Module Power        Manager                0x08
```

```
                                    XBUS IO                 0x03
                                    UD Flow Control         0x05
                                    PCI ASIC I/F            0x05
                                    Service Module I/F      0x72
                                    Memory Decoder 0        0x02
                                    Memory Decoder 1        0x02
MDS 9100 Series Fabric Switch       XBUS IO                 0x03
                                    PCI ASIC I/F            0x40000003
2x1GE IPS, 14x1/2Gbps FC Module     Power Manager           0x07
                                    XBUS IO                 0x05
                                    UD Flow Control         0x05
                                    PCI ASIC I/F            0x07
                                    IPS DB I/F              0x1a
```

The following example displays the entire output for the show version command:

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2008, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.
Software
  BIOS:      version 1.1.0
  loader:    version 1.2(2)
  kickstart: version 4.1(1) [build 4.1(0.155)] [gdb]
  system:    version 4.1(1) [build 4.1(0.155)] [gdb]
  BIOS compile time:       10/24/03
  kickstart image file is: bootflash:///m9200-ek9-kickstart-mzg.4.1.0.155.bin
  kickstart compile time:  10/12/2020 25:00:00 [07/23/2008 10:00:56]
  system image file is:    bootflash:///m9200-ek9-mzg.4.1.0.155.bin
  system compile time:     12/25/2010 12:00:00 [07/23/2008 10:53:42]
Hardware
  cisco MDS 9216i (2 Slot) Chassis ("2x1GE IPS, 14x1/2Gbps FC/Supervisor")
  Intel(R) Pentium(R) III CPU  with 965712 kB of memory.
  Processor Board ID JAB10007017G
  Device name: 10.64.66.22
  bootflash:    1001448 kB
  slot0:              0 kB (expansion flash)
Kernel uptime is 1 day(s), 2 hour(s), 22 minute(s), 40 second(s)
Last reset at 800175 usecs after  Tue Jul 29 11:07:38 2008
  Reason: Reset Requested by CLI command reload
  System version: 4.1(0.151)
  Service:
switch#
```

The following examples display a before and after comparison scenario after the loader version is updated:

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2008, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.
Software
  BIOS:      version 1.1.0
```

```
  loader:    version 1.2(2)<---------------existing version
kickstart: version 4.1(1) [build 4.1(0.155)] [gdb]
  system:    version 4.1(1) [build 4.1(0.155)] [gdb]
  BIOS compile time:       10/24/03
  kickstart image file is: bootflash:///m9200-ek9-kickstart-mzg.4.1.0.155.bin
  kickstart compile time:  10/12/2020 25:00:00 [07/23/2008 10:00:56]
  system image file is:    bootflash:///m9200-ek9-mzg.4.1.0.155.bin
  system compile time:     12/25/2010 12:00:00 [07/23/2008 10:53:42]
switch# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2008, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.
Software
  BIOS:      version 1.1.0
  loader:    version 4.1(0)<---------------new version
```

The following example displays the version details for a specified module:

```
switch# show ver mod 4
Mod No   Mod Type       SW Version           SW Interim Version
4        LC             1.0(3)               1.0(3)
```

show vrrp

To display the VRRP configuration information, use the **show vrrp** command.

show vrrp [**ipv6 vr** *group-id* [**interface** {**gigabitethernet** *slot/port* {**configuration**|**statistics**|**status**}|**mgmt 0** {**configuration**|**statistics**|**status**}|**port-channel** *port-channel* {**configuration**|**statistics**|**status**}|**vsan** *vsan-id* {**configuration**|**statistics**|**status**}}]|**statistics**|**vr** *group-id* [**interface** {**gigabitethernet** *slot/port* {**configuration**|**statistics**|**status**}|**mgmt 0** {**configuration**|**statistics**|**status**}|**port-channel** *port-channel* {**configuration**|**statistics**|**status**}|**vsan** *vsan-id* {**configuration**|**or statistics**|**status**}}]

Syntax Description

ipv6	(Optional) Displays IPv6 virtual router information.
vr	(Optional) Displays the virtual router information.
group-id	(Optional) Specifies the group ID. The range is 1 to 255.
interface	(Optional) Displays the interface type.
gigabitethernet	(Optional) Displays the Gigabit Ethernet interface.
slot/port	(Optional) Specifies the slot and port.
configuration	(Optional) Displays the VRRP configuration.
statistics	(Optional) Displays cumulative VRRP statistics.
status	(Optional) Displays VRRP operational status.
mgmt 0	(Optional) Displays the mgmt0 interface.
port-channel	(Optional) Displays the PortChannel interface.
port-channel	Specifies the Port Channel.
vsan	(Optional) Displays the VSAN interface.
vsan-id	(Optional) Specifies the VSAN ID.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **IPv6** option.

Usage Guidelines

None.

Examples

The following example displays VRRP configured information:

```
switch# show vrrp vr 7 interface vsan 2 configuration
vr id 7 configuration
admin state down
priority 100
no authentication
advertisement-Interval 1
preempt yes
tracking interface vsan1 priority 2
protocol IP
```

The following example displays VRRP status information:

```
switch# show vrrp vr 7 interface vsan 2 status
vr id 7 status
MAC address 00:00:5e:00:01:07
Operational state: init
```

The following example displays VRRP statistics:

```
switch# show vrrp vr 7 interface vsan 2 statistics

vr id 7 statistics
Become master 0
Advertisement 0
Advertisement Interval Error 0
Authentication Failure 0
TTL Error 0
Priority 0 Received 0
Priority 0 Sent 0
Invalid Type 0
Mismatch Address List 0
Invalid Authentication Type 0
Mismatch Authentication 0
Invalid Packet Length 0
```

The following example displays VRRP cumulative statistics:

```
switch# show vrrp statistics

Invalid checksum 0
Invalid version 0
Invalid VR ID 0
```

The following example displays VRRP IPv6 configuration information:

```
switch# show vrrp ipv6 vr 1 interface gigabitethernet 4/8 configuration

IPv6 vr id 1 configuration
admin state up
priority 100
associated ip: 2550:1::3:408:1 accept
advertisement-interval 100
preempt no
protocol IPv6
```

The following example displays VRRP IPv6 statistics information:

```
switch# show vrrp ipv6 vr 1 interface gigabitethernet 4/8 statistics
```

```
IPv6 vr id 1 statistics
Become master 1
Advertisement 0
Advertisement Interval Error 0
TTL Error 0
Priority 0 Received 0
Priority 0 Sent 0
Invalid Type 0
Mismatch Address List 0
Invalid Packet Length 0
```

The following example displays VRRP IPv6 status information:

```
switch# show vrrp ipv6 vr 1 interface gigabitethernet 4/8 status

IPv6 vr id 1 status
MAC address 00:00:5e:00:02:01
Operational state: master
Up time 17 hour(s),  21 min,  43 sec
Master IP address: fe80::20c:30ff:fe0c:f6c7
```

show vsan

To display information about configured VSAN, use the **show vsan** command.

show vsan [{*vsan-id* **[membership]**|**membership interface** {**fc** *slot / port*|**fcip** *fcip-id*|**fv** *slot / dpp-number / fv-port*|**iscsi** *slot / port*|**portchannel** *portchannel-number* **.** *subinterface-number*}}]|**[usage]**

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

vsan vsan-id	(Optional) Displays information for the specified VSAN ID. The range is 1 to 4093.
membership	(Optional) Displays membership information.
interface	(Optional) Specifies the interface type.
fc *slot*/*port*	(Optional) Specifies a Fibre Channel interface on a Cisco MDS 9000 Family Switch.
bay | ext port	Specifies a Fibre Channel interface on a Cisco MDS 9124 Fabric Switch, a Cisco Fabric Switch for HP c-Class BladeSystem, and a Cisco Fabric Switch for IBM BladeCenter.
fcip *fcip-id*	(Optional) Specifies a FC IP interface ID. The range is 1 to 255.
fv *slot*/*dpp-number*/*fv-port*	(Optional) 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 *slot*/*port*	(Optional) Specifies the iSCSI interface in the specified slot/port on a Cisco MDS 9000 Family switch.
port-channel *portchannel-number***.** *subinterface-number*	(Optional) Specifies a PortChannel interface specified by the PortChannel number followed by a dot (.) indicator and the subinterface number.
usage	(Optional) Displays VSAN usage in the system.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(2)	This command was modified.

Release	Modification
3.1(2)	Added the **bay** | **ext** interface.

Usage Guidelines

For the **show vsan membership interface** command, interface information is not displayed if interfaces are not configured on this VSAN.

The interface range must be in ascending order and non-overlapping. You can specify a range using a hyphen and several interfaces using commas:

- The interface range format for an FC interface range is **fc***slot*/*port* - *port* **, fc***slot*/*port* **, fc***slot*/*port* (For example, **show int fc1/1 - 3 , fc1/5 , fc2/5**)
- The interface range format for an FV interface range is **fv***slot*/*dpp*/*fvport* **-** *fvport* , **fv***slot*/*dpp*/*port* , **fv***slot*/*dpp*/*port* (For example, **show int fv2/1/1 - 3 , fv2/1/5 , fv2/2/5**)
- The format for a PortChannel is **port-channel** *portchannel-number***.***subinterface-number* (For example, **show int** port-channel **5.1***)*

Examples

The following examples display configured VSAN information:

```
switch# show vsan 1
vsan 1 information
         name:VSAN0001  state:active
         interoperability mode:yes ß verify mode
         loadbalancing:src-id/dst-id/oxid
         operational state:up
switch# show vsan usage
4 vsan configured
configured vsans:1-4
vsans available for configuration:5-4093
switch # show vsan 1 membership
vsan 1 interfaces:
        fc1/1   fc1/2   fc1/3   fc1/4   fc1/5   fc1/6   fc1/7   fc1/9
        fc1/10  fc1/11  fc1/12  fc1/13  fc1/14  fc1/15  fc1/16  port-channel 99
```

The following example displays membership information for all VSANs.

```
switch # show vsan membership

vsan 1 interfaces:
        fc2/16  fc2/15  fc2/14  fc2/13  fc2/12  fc2/11  fc2/10  fc2/9
        fc2/8   fc2/7   fc2/6   fc2/5   fc2/4   fc2/3   fc2/2   fc2/1
        fc1/16  fc1/15  fc1/14  fc1/13  fc1/12  fc1/11  fc1/10  fc1/9
        fc1/7   fc1/6   fc1/5   fc1/4   fc1/3   fc1/2   fc1/1
vsan 2 interfaces:
vsan 7 interfaces:
        fc1/8
vsan 100 interfaces:
vsan 4094(isolated vsan) interfaces:
```

The following example displays membership information for a specified interface:

```
switch # show vsan membership interface fc1/1
fc1/1
        vsan:1
        allowed list:1-4093
switch# show vsan
vsan 1 information
```

```
          name:VSAN0001  state:active
          interoperability mode:default
          loadbalancing:src-id/dst-id/oxid
          operational state:up
vsan 2 information
          name:VmVSAN  state:active
          interoperability mode:default
          loadbalancing:src-id/dst-id/oxid
          operational state:up
vsan 3 information
          name:Disk_A  state:active
          interoperability mode:default
          loadbalancing:src-id/dst-id/oxid
          operational state:up
vsan 4 information
          name:Host_B  state:active
          interoperability mode:default
          loadbalancing:src-id/dst-id/oxid
          operational state:up
vsan 4094:isolated_vsan
switch# show vsan membership interface fv 2/1/3 , fv2/1/5 - 7
fv2/1/3
        vsan:2
        allowed list:1-4093
fv2/1/5
        vsan:3
        allowed list:1-4093
fv2/1/6
        vsan:4
        allowed list:1-4093
fv2/1/7
        vsan:4
        allowed list:1-409
switch# sh vsan membership interface bay 12
bay12
        vsan:1
        allowed list:1-4093
```

show wwn

To display the status of the WWN configuration, use the **show wwn** command.

show wwn {**oui** |**status** |**block-id** |**number**|**switch**|**vsan-wwn**}

Syntax Description

oui	Displays all OUIs in the OUI database.
status block-id number	Displays WWN usage and alarm status for a block ID. The range is 34 to 1793.
switch	Displays switch WWN.
vsan-wwn	Displays all user-configured VSAN WWNs.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **vsan-wwn** keyword.
7.3(0)D1(1)	The **oui** keyword was added.

Usage Guidelines

None.

Examples

The following example displays the WWN of the switch:

```
switch# show wwn switch
Switch WWN is 20:01:ac:16:5e:52:00:01
```

The following example displays a user-configured VSAN WWN:

```
switch# show wwn vsan-wwn
vsan wwn configured by user
---- ----------------------
100 20:64:08:00:88:0d:5f:81
```

show zone

To display zone information, use the **show zone** command.

show zone [{**active** [**vsan** *vsan-id*]|**analysis** {**active vsan** *vsan-id*|**pending** {**active vsan** *vsan-id*|**vsan** *vsan-id*|**zoneset** *string* **vsan** *vsan-id*}|**vsan** *vsan-id*|**zoneset** *string* **vsan** *vsan-id*}|**ess** [**vsan** *vsan-id*]|**member** {**device-alias** *string* [{**active** [**vsan** *vsan-id*]|**lun 0xhhhh** [{**active** [**vsan** *vsan-id*]|**vsan** *vsan-id*}]|**vsan** *vsan-id*}]|**fcalias** *string* [{**active** [**vsan** *vsan-id*]|**vsan** *vsan-id*}]|**fcid 0xhhhhhh** [{**active** [**vsan** *vsan-id*]|**lun 0xhhhh** [{**active** [**vsan** *vsan-id*]|**vsan** *vsan-id*}]|**vsan** *vsan-id*}]|**pwwn** **hh : hh : hh : hh : hh : hh : hh : hh** [{**active** [**vsan** *vsan-id*]|**lun 0xhhhh** [{**active** [**vsan** *vsan-id*]|**vsan** *vsan-id*}]|**vsan** *vsan-id*}]}|**name** *string* [{**active** [**vsan** *vsan-id*]|**pending** [{**active** [**vsan** *vsan-id*]|**vsan** *vsan-id*}]}]|**vsan** *vsan-id*}]|[{**pending** [{**active** [**vsan** *vsan-id*]|**vsan** *vsan-id*}]|**pending-diff** [**vsan** *vsan-id*]|**policy** [{**pending** [**vsan** *vsan-id*]|**vsan** *vsan-id*}]|**smart-zoning auto-conv** {**log errors**|**status** **vsan** *vsan-id*}|**statistics** [{**lun-zoning** [**vsan** *vsan-id*]|**read-only-zoning** [**vsan** *vsan-id*]|**vsan** *vsan-id*}]|**status** [{**global**|**vsan** *vsan-id*}]|**vsan** *vsan-id*}]

Syntax Description

active	(Optional) Displays zones which are part of an active zone set.
analysis	Displays a summary of zone database information.
device-alias *string*	Specifies a device name.
ess	Displays ESS information.
fcalias *string*	Specifies an fcalias name.
fcid *0xhhhhhh*	Specifies an FCID. The format is 0xhhhhhh, where h is a hexadecimal digit.
global	Displays global zone service parameters.
log errors	Displays the error logs.
lun *0xhhhh*	Specifies a LUN ID. The format is 0xhhhh, where h is a hexadecimal digit.
lun-zoning	This option is deprecated in this release.
member	Displays all zones in which the given member is part of.
name *string*	Specifies a zone name.
pending	Displays what zoning will be after all pending changes are applied.
pending-diff	Displays individual pending zone changes.
policy	Displays zone policies.
pwwn *hh:hh:hh:hh:hh:hh:hh:hh*	Specifies a port world wide name. The format is hh:hh:hh:hh:hh:hh:hh:hh, where h is a hexadecimal digit.
read-only-zoning	This option is deprecated in this release.
smart-zoning auto-conv	Displays the previous auto convert status.

statistics	Displays zone server request and response statistics.
status	Displays the current status of the zone server.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
zoneset *string*	Specifies a zoneset name.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(4)	This command was introduced.
2.1(1a)	Modified the **show zone status** display.
5.2(1)	Deprecated the **lun-zoning and read-only-zoning options.**
6.2(9)	Added the combined zone database size for the show zone status command.

Usage Guidelines

None.

Examples

The following example displays configured zone information:

```
switch# show zone
zone name Zone3 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:9c:48:e5
zone name Zone2 vsan 2
  fwwn 20:41:00:05:30:00:2a:1e
  fwwn 20:42:00:05:30:00:2a:1e
  fwwn 20:43:00:05:30:00:2a:1e
zone name Zone1 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:a6:be:2f
  pwwn 21:00:00:20:37:9c:48:e5
  fcalias Alias1
zone name Techdocs vsan 3
  ip-address 10.15.0.0 255.255.255.0
```

The following example displays zone information for a specific VSAN:

```
switch# show zone vsan 1
zone name Zone3 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:9c:48:e5
zone name Zone2 vsan 1
  fwwn 20:41:00:05:30:00:2a:1e
  fwwn 20:42:00:05:30:00:2a:1e
  fwwn 20:43:00:05:30:00:2a:1e
  fwwn 20:44:00:05:30:00:2a:1e
  fwwn 20:45:00:05:30:00:2a:1e
  fwwn 20:46:00:05:30:00:2a:1e
```

```
  fwwn 20:47:00:05:30:00:2a:1e
  fwwn 20:48:00:05:30:00:2a:1e
  fwwn 20:49:00:05:30:00:2a:1e
  fwwn 20:4a:00:05:30:00:2a:1e
  fwwn 20:4b:00:05:30:00:2a:1e
  fwwn 20:4c:00:05:30:00:2a:1e
  fwwn 20:4d:00:05:30:00:2a:1e
  fwwn 20:4e:00:05:30:00:2a:1e
  fwwn 20:4f:00:05:30:00:2a:1e
  fwwn 20:50:00:05:30:00:2a:1e
  fwwn 20:51:00:05:30:00:2a:1e
  fwwn 20:52:00:05:30:00:2a:1e
  fwwn 20:53:00:05:30:00:2a:1e
  fwwn 20:54:00:05:30:00:2a:1e
  fwwn 20:55:00:05:30:00:2a:1e
  fwwn 20:56:00:05:30:00:2a:1e
  fwwn 20:57:00:05:30:00:2a:1e
  fwwn 20:58:00:05:30:00:2a:1e
  fwwn 20:59:00:05:30:00:2a:1e
  fwwn 20:5a:00:05:30:00:2a:1e
  fwwn 20:5b:00:05:30:00:2a:1e
  fwwn 20:5c:00:05:30:00:2a:1e
  fwwn 20:5d:00:05:30:00:2a:1e
  fwwn 20:5e:00:05:30:00:2a:1e
  fwwn 20:5f:00:05:30:00:2a:1e
  fwwn 20:60:00:05:30:00:2a:1e
zone name Zone1 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:a6:be:2f
  pwwn 21:00:00:20:37:9c:48:e5
  fcalias Alias1
```

The following example displays members of a specific zone:

```
switch# show zone name Zone1
zone name Zone1 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:a6:be:2f
  pwwn 21:00:00:20:37:9c:48:e5
  fcalias Alias1
```

The following example displays all zones to which a member belongs using the FCID:

```
switch# show zone member pwwn 21:00:00:20:37:9c:48:e5
           VSAN: 1
zone Zone3
zone Zone1
fcalias Alias1
```

The following example displays the number of control frames exchanged with other switches:

```
switch# show zone statistics
Statistics For VSAN: 1
********************************
Number of Merge Requests Sent: 24
Number of Merge Requests Recvd: 25
Number of Merge Accepts Sent: 25
Number of Merge Accepts Recvd: 25
Number of Merge Rejects Sent: 0
Number of Merge Rejects Recvd: 0
Number of Change Requests Sent: 0
Number of Change Requests Recvd: 0
Number of Change Rejects Sent: 0
```

```
Number of Change Rejects Recvd: 0
Number of GS Requests Recvd: 0
Number of GS Requests Rejected: 0
Statistics For VSAN: 2
*********************************
Number of Merge Requests Sent: 4
...
Number of GS Requests Rejected: 0
```

The following example displays LUN-zoning details:

```
switch# show zone statistics lun-zoning
LUN zoning statistics for VSAN: 1
************************************************************
S-ID: 0x123456, D-ID: 0x22222, LUN: 00:00:00:00:00:00:00:00
------------------------------------------------------------
Number of Inquiry commands received:            10
Number of Inquiry data No LU sent:             5
Number of Report LUNs commands received:             10
Number of Request Sense commands received:              1
Number of Other commands received:             0
Number of Illegal Request Check Condition sent:             0
S-ID: 0x123456, D-ID: 0x22222, LUN: 00:00:00:00:00:00:00:01
------------------------------------------------------------
Number of Inquiry commands received:              1
Number of Inquiry data No LU sent:             1
Number of Request Sense commands received:              1
Number of Other commands received:             0
Number of Illegal Request Check Condition sent:  0
```

The following example displays read-only zone details:

```
switch# show zone statistics read-only-zoning
Read-only zoning statistics for VSAN: 2
************************************************************
S-ID: 0x33333, D-ID: 0x11111, LUN: 00:00:00:00:00:00:00:64
------------------------------------------------------------
Number of Data Protect Check Condition Sent:             12
switch(config)# show zone status
VSAN: 1 default-zone: deny distribute: active only Interop: default
mode: basic merge-control: allow
session: none
hard-zoning: enabled broadcast: disabled
smart-zoning: disabled
rscn-format: fabric-address
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 4 bytes
Zonesets:0 Zones:0 Aliases: 0
Active Zoning Database :
Database Not Available
Current Total Zone DB Usage: 4 / 2097152 bytes (0 % used)
Pending (Session) DB size:
Full DB Copy size: n/a
Active DB Copy size: n/a
SFC size: 4 / 2097152 bytes (0 % used)
Status:
VSAN: 8 default-zone: deny distribute: full Interop: default
mode: basic merge-control: allow
session: none
hard-zoning: enabled broadcast: disabled
smart-zoning: disabled
```

```
rscn-format: fabric-address
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 1946498 bytes
Zonesets:6 Zones:8024 Aliases: 0
Active Zoning Database :
DB size: 150499 bytes
Name: zoneset-1000 Zonesets:1 Zones:731
Current Total Zone DB Usage: 2096997 / 2097152 bytes (99 % used)
Pending (Session) DB size:
Full DB Copy size: n/a
Active DB Copy size: n/a
SFC size: 2096997 / 2097152 bytes (99 % used)
Status: Zoneset distribution failed [Error: Fabric changing Dom 33]:
at 17:05:06 UTC Jun 16 2014
VSAN: 9 default-zone: deny distribute: full Interop: default
mode: enhanced merge-control: allow
session: none
hard-zoning: enabled broadcast: enabled
smart-zoning: disabled
rscn-format: fabric-address
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 2002584 bytes
Zonesets:4 Zones:7004 Aliases: 0 Attribute-groups: 1
Active Zoning Database :
DB size: 94340 bytes
Name: zoneset-hac13-200 Zonesets:1 Zones:176
Current Total Zone DB Usage: 2096924 / 2097152 b
Pending (Session) DB size:
Full DB Copy size: 0 bytes
Active DB Copy size: 0 bytes
SFC size: 0 / 2097152 bytes (0 % used)
Status: Activation completed at 17:28:04 UTC Jun 16 2014
VSAN: 12 default-zone: deny distribute: full Interop: default
mode: enhanced merge-control: allow
session: none
hard-zoning: enabled broadcast: enabled
smart-zoning: disabled
rscn-format: fabric-address
Default zone:
qos: none broadcast: disabled ronly: disabled
Full Zoning Database :
DB size: 84 bytes
Zonesets:0 Zones:1 Aliases: 0 Attribute-groups: 1
Active Zoning Database :
DB size: 144 bytes
Name: zs1 Zonesets:1 Zones:2
Current Total Zone DB Usage: 228 / 2097152 bytes (0 % used)
Pending (Session) DB size:
Full DB Copy size: 0 bytes
Active DB Copy size: 0 bytes
SFC size: 0 / 2097152 bytes (0 % used)
Status: Commit completed at 14:39:33 UTC Jun 27 201
switch(config)#
```

The following example checks the status of the **zoneset distribute vsan** command and displays the default zone attributes of a specific VSAN or all active VSANs:

```
switch# show zone status vsan 1
VSAN:1 default-zone:deny distribute:active only Interop:default
```

```
    mode:basic merge-control:allow session:none
    hard-zoning:enabled
Default zone:
    qos:low broadcast:disabled ronly:disabled
Full Zoning Database :
    Zonesets:0  Zones:0 Aliases:0
Active Zoning Database :
    Database Not Available
Status:
```

Table 15: show zone status Field Descriptions, on page 1695 describes the significant fields shown in the **show zone status vsan** display.

Table 15: show zone status Field Descriptions

Field	Description
VSAN:	VSAN number displayed.
default-zone:	Default-zone policy either permit or deny.
Default zone:	The Default zone field displays the attributes for the specified VSAN. The attributes include: Qos level, broadcast zoning enabled/disabled, and read-only zoning enabled/disabled.
distribute:	Distribute full-zone set (full) or active-zone set (active only).
Interop:	Display s interop mode. 100 = default, 1 = standard, 2 and 3 = Non-Cisco vendors.
mode:	Displays zoning mode either basic or enhanced.
merge control:	Displays merge policy either allow or restrict.
Hard zoning is enabled	If hardware resources (TCAM) becomes full, hard zoning is automatically disabled.
Full Zoning Database:	Displays values of zone database. Its zones filed displays the total number of zones present, which include those that does not belongs to any zonesets.
Active Zoning Database:	Displays values of active zone database.
Status:	Displays status of last zone distribution.

show zone analysis

To display detailed analysis and statistical information about the zoning database, use the show zone **analysis** command.

show zone analysis {**active vsan vsan-id**|**vsan vsan-id**|**zoneset name vsan vsan-id**}

Syntax Description

active	Displays analysis information for the active zone set.
vsan *vsan-id*	Displays analysis information for the specified VSAN ID. The range is 1 to 4093.
zoneset *name*	Displays zone set analysis information for the specified zone set.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays detailed statistics and analysis of the active zoning database:

```
switch(config-zone)# show zone analysis active vsan 1
Zoning database analysis vsan 1
  Active zoneset: qoscfg
    Activated at: 14:40:55 UTC Mar 21 2014
    Activated by: Local [ CLI ]
    Default zone policy: Deny
    Number of devices zoned in vsan: 8/8 (Unzoned: 0)
    Number of zone members resolved: 10/18 (Unresolved: 8)
    Num zones: 4
    Number of IVR zones: 0
    Number of IPS zones: 0
    Formatted size: 328 bytes / 4096 Kb
switch(config-zone)#
```

Table 16: show zone analysis Field Descriptions for the Active Zoning Database, on page 1697 describes the fields displayed in the output of a **show zone analysis** command for the active zoning database.

Table 16: show zone analysis Field Descriptions for the Active Zoning Database

Field	Description
Active zoneset	Displays the active zone set name. If a zone set has changed in the full zoning database, an asterisk (*) appears after the zone set name. If the active zone set is not present in the full zoning database, a minus sign (-) appears after the zone set name.
Activated at	Displays the time the zone set was activated.

Activated from	Displays the agent that most recently modified the active zoning database. The agent can be one of the following three types:
	• Local: indicates that the active database was last modified locally through a configuration change from one of the following applications:
	  • CLI: The active zoning database was modified by the user from the Command Line Interface.
	  • SNMP: The active zoning database was modified by the user through the Simple Network Management Protocol (SNMP).
	  • GS: The active zoning database was modified from the Generic Services (GS) client.
	  • CIM: The active zoning database was modified by the applications using the Common Information Model (CIM).
	  • INTERNAL: The active zoning database was modified as a result of an internal activation either from Inter-VSAN Routing (IVR) or from the IP Storage services manager.
	• Merge: indicates that the active database was last modified by the Merge protocol. The interface on which the merge occurred is also displayed.
	• Remote: indicates that the active database was last modified by the Change protocol, initiated by a remote switch. The domain, IP address, and switch name of the switch initiating the change are also displayed.
	Note The switch name is displayed on the next line, aligned with the domain, only if the switch name is set. The default switch name *switch* and the *ip-address* are not displayed.

Default zoning policy: permit/deny	Displays the status of the default zoning policy for this VSAN.

Field	Description
Number of devices zoned in vsan: a/b (Unzoned: c | Default-zone: d)	Displays the number of devices that are present in the zoning configuration. • a = The number of unique resolved members in the active database. • b = The number of devices logged in, which is the same as the number of entries in the Fibre Channel name server (FCNS) database. • c = The number of devices logged in, but not zoned in the zoning configuration. • d = The number of devices in the default zone. d is displayed only if the default zoning policy is permit.
Number of zone members resolved: a/b (Unresolved: c)	Displays the number of members that are resolved in this VSAN in the form: a out of b members in the zone set are resolved. The number of resolved members is not necessarily unique. For example, if a pWWN member and a fWWN member resolve to the same FC ID, then that member is counted as two resolved members out of two members present. • a = The number of members resolved. • b = The total number of members present. • c = The total number of members unresolved.
Num zones	Displays the total number of zones that are present in the active zone set.
Number of IVR zones	Displays the number of zones added and activated by IVR.
Number of IPS zones	Displays the number of zones added and activated by the IP Storage services manager (IPS-MGR).
Formatted database size	Displays the total size of the active database when formatted to be sent over the wire. The formatted database size is displayed in kilobytes (KB) in this format: < *X* KB / *Y* KB, as in the following example. Formatted database size: < 1 KB/2000 KB In this example, the formatted database size is less than 1 KB out of the maximum size of 2000 KB.

The following example displays detailed statistics and analysis of the full zoning database:

```
switch# sh zone analysis vsan 1
   Zoning database analysis vsan 1
     Full zoning database
       Last updated at: 14:36:56 UTC Oct 04 2005
       Last updated by: Local [CLI / SNMP / GS / CIM / INTERNAL] or
                        Merge [interface] or
                        Remote [Domain, IP-Address]
                               [Switch name]
       Num zonesets: 1
       Num zones: 1
       Num aliases: 0
       Num attribute groups: 0
       Formatted database size: < 1 Kb / 2000 kb ( < 1% usage)
```

```
Unassigned zones:
  zone name z1 vsan 1
```

Table 17: show zone analysis Field Descriptions for the Full Zoning Database, on page 1699 describes the fields displayed in the output of a **show zone analysis** command for the full zoning database.

Table 17: show zone analysis Field Descriptions for the Full Zoning Database

Field	Description
Last updated at	Displays a time stamp showing when the full zoning database was last updated.

Last Updated by	Displays the agent that most recently modified the full zoning database. The agent can be one of the following three types:
	• Local: indicates that the full database was last modified locally through a configuration change from one of the following applications:
	  • CLI: The full zoning database was modified by the user from the Command Line Interface.
	  • SNMP: The full zoning database was modified by the user through the Simple Network Management Protocol (SNMP).
	  • GS: The full zoning database was modified from the Generic Services (GS) client.
	  • CIM: The full zoning database was modified by the applications using the Common Information Model (CIM).
	  • INTERNAL: The full zoning database was modified as a result of an internal activation either from Inter-VSAN Routing (IVR) or from the IP Storage services manager.
	• Merge: indicates that the full database was last modified by the Merge protocol. In this case, the interface on which the merge occurred is also displayed.
	• Remote: indicates that the full database was last modified by the Change protocol, initiated by a remote switch, when the full zone set distribution was enabled. The domain, IP address, and switch name of the switch initiating the change are also displayed.
	Note The switch name is displayed on the next line, aligned with the domain, only if the switch name is set. The default switch name *switch* and the *ip-address* are not displayed.

Num zonesets	Displays the total number of zone sets in the database.
Num zones	Displays the total number of zones in the database, including unassigned zones.
Num aliases	Displays the total number of aliases in the database, including unassigned FC aliases.
Num attribute groups	Displays the total number of attribute groups in the database. This field applies only when enhanced zoning is used.

Field	Description
Formatted database size	Displays the total size of the full database when formatted to be sent over the wire. The formatted database size is displayed in kilobytes in this format: < *X* KB / *Y* KB, as in the following example. Formatted database size: < 1 KB/2000 KB In this example, the formatted database size is less than 1 KB out of the maximum size of 2000 KB.
Unassigned zones	Displays all the unassigned zones in the VSAN. Only the names of the zones are displayed. The details about the members of the zone are not displayed in this section.

The followng example displays zone set analysis information. See Table 17: show zone analysis Field Descriptions for the Full Zoning Database, on page 1699 for a description of the fields in this example:

```
switch# show zone analysis zoneset zs1 vsan 1
Zoning database analysis vsan 1
  Zoneset analysis: zs1
    Num zonesets: 1
    Num zones: 0
    Num aliases: 0
    Num attribute groups: 0
    Formattted size: 20 bytes / 2048 Kb
```

Related Commands

Command	Description
zone compact database	Compacts a zone database in a VSAN.

show zone internal global-info

To display the zone global information, use the **show zone internal global-info** command.

show zone internal global-info

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
5.2(6)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the zone server internal state for a VSAN:

```
switch# show zone internal global-info
Global Default Zone Max-Limit :
    Global Default Zone Max-Limit: 16000
    Global Default Zone Member Max-Limit: 32000
    Global Default Zoneset Max-Limit: 1000
    Global Default Zone database size Max-Limit: 4000000 bytes
Global Full Database Counters :
    Zonesets: 0 Zones: 0 Huge id zones: 0
    Read-only Zones: 0 QoS Zones: 0
    Broadcast Zones: 0 Smart-zoning Zones: 0
    Aliases: 0 Attribute-groups: 0
    Members: 0 LUN Members: 0 DDAS Members: 0 Smart-zoning members: 0
    Adv Zoning3 Members(IPv4 + dom-If): 0 IPv6 Members: 0
Global Session Database Counters (diff) :
    Zonesets: 0 Zones: 0 Smart-zoning Zones: 0
    Aliases: 0 Attribute-groups: 0
    Members: 0 LUN Members: 0 DDAS Members: 0 Smart-zoning members: 0
Global Active Database Counters :
    Zonesets: 1 Zones: 5 Huge id zones: 0
    Read-only Zones: 0 QoS Zones: 0
    Broadcast Zones: 0 Smart-zoning Zones: 0
    Members: 6 LUN Members: 0 DDAS Members: 0 Smart-zoning members: 0
    Adv Zoning3 Members(IPv4 + dom-If): 0 IPv6 Members: 0
Global Session Active Database Counters (diff) :
    Zones: 0 Smart-zoning Zones: 0
    Members: 0 LUN Members: 0 DDAS Members: 0 Smart-zoning members: 0
Global ISSU Info:
    fs_upgrade = 0 system_upg = 0 lc_upgrade = 0
Global RSCN Generation Info: Enabled
Global Smart-zoning vsan counter: 1
Global port-address RSCN counter: 0
Global Zone EEM Limit :
    Global Zone EEM Limit: 16000
    Global Zone Member EEM Limit: 32000
```

```
    Global Zoneset EEM Limit: 1000
    Global Zone database size EEM Limit: 4000000 bytes
switch#
```

show zone internal vsan

To display the zone server internal state for a VSA, use the **show zone internal vsan** command.

show zone internal vsan vsan-id

Syntax Description

vsan-id	Specifies the VSAN ID. The range is from 1to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
5.2(6)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the zone server internal state for a VSAN:

```
switch# show zone internal vsan 1
VSAN: 1 default-zone: deny(rw) distribute: active only
    E_D_TOV: 2000 R_A_TOV: 10000 D_S_TOV: 5000 F_S_TOV: 5000 F_D_TOV: 2000
    Interop: default IOD: disable bcast: unsupported dflt-bcast: unsupported dfl
t-qos: 0
    Smart-zoning: disabled    Inc Tmp SZ mode: 0    Tmp Smart-zoning: 0
    DBLock:-(F count:0) Ifindex Table Size: 5 Transit Frame Index: 0
    Total Transit Frame Count: 0 Transit Discard Count: 0
Full Database Counters :
    Zonesets: 0 Zones: 0 Huge id zones: 0
    Read-only Zones: 0 QoS Zones: 0
    Broadcast Zones: 0 Smart-zoning Zones: 0
    Aliases: 0 Attribute-groups: 0
    Members: 0 LUN Members: 0 DDAS Members: 0 Smart-zoning members: 0
    Adv Zoning3 Members(IPv4 + dom-If): 0 IPv6 Members: 0
switch#
```

show zone policy

To display the zone policies, use the show zone policy command.

show zone policy

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
5.2(6)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the zone policies:

```
switch# show zone policy
Vsan: 1
   Default-zone: deny
   Distribute: active only
   Broadcast: unsupported
   Merge control: allow
   Generic Service: read-write
   Smart-zone: disabled
switch#
```

show zone smart-zoning auto-conv

To display the previous auto convert status, use the show zone smart-zoning auto-conv command.

show zone smart-zoning auto-conv {**log errors**|**status vsan vsan-id**}

Syntax Description

log	Displays the logged messages.
errors	Displays the error logs for smart zoning auto convert.
status	Displays the previous auto convert status.
vsan	Displays the zones belonging to the specified VSAN.
vsan-id	VSAN ID. The range is from 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
5.2(6)	This command was introduced.

Usage Guidelines

None.

Examples

The following example displays the previous auto convert status for a VSAN:

```
switch# show zone smart-zoning auto-conv status vsan 1
switch#
```

show zone-attribute-group

To display the device name information, use the **show zone-attribute-group** command.

{**show zone-attribute-group** [**name** *group-name*]|[**pending**]|[**vsan** *vsan-id*]}

Syntax Description

name *group-name*	Displays the entire device name database.
pending	Displays the pending device name database information.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to display the contents of pending zone attribute groups.

```
switch# show zone-autoboot-group pending
zone-attribute-group name $default_zone_attr_group$ vsan 4061
zone-attribute-group name admin-group vsan 4061
  broadcast
```

Related Commands

Command	Description
zone-attribute-group name	Configures zone attribute groups.

show zoneset

To display the configured zone sets, use the **show zoneset** command.

show zoneset [{[**active** [**vsan** *vsan-id*]]|[**brief** [{**active** [**vsan** *vsan-id*]|**vsan** *vsan-id*}]]|[{**name** *zoneset-name* [**active vsan** *vsan-id*]|[**brief** [{**active vsan** *vsan-id*|**vsan** *vsan-id*}]]|[**pending** [{**active vsan** *vsan-id*|**brief** [{**active vsan** *vsan-id*|**vsan** *vsan-id*}]|**vsan** *vsan-id*}]]|[**vsan** *vsan-id*]}]|[{**pending** [**active vsan** *vsan-id*]|[**brief** [{**active vsan** *vsan-id*|**vsan** *vsan-id*}]]|[**vsan** *vsan-id*]}]|[**vsan vsan-id**]}]

Syntax Description

active	Displays only active zone sets.
vsan	Displays the VSAN.
vsan-id	Specifies the ID of the VSAN. The range is 1 to 4093
brief	Displays zone set members in a brief list.
name	Displays members of a specified zone set.
zoneset-name	Specifies the zone set name. The maximum is 64.
pending	Displays zone sets members that are in session.

Command Default

None.

Command Modes

EXEC mode

Command History

Release	Modification
1.2(2)	This command was modified.

Usage Guidelines

None.

Examples

The following example displays configured zone set information.

```
switch(config)# show zoneset vsan 1
zoneset name qoscfg vsan 1
  zone name qos1 vsan 1
    zone-attribute-group name qos1-attr-group vsan 1
    pwwn 50:08:01:60:01:5d:51:11
    pwwn 50:08:01:60:01:5d:51:10
    pwwn 50:08:01:60:01:5d:51:13

  zone name qos3 vsan 1
    zone-attribute-group name qos3-attr-group vsan 1
    pwwn 50:08:01:60:01:5d:51:11
    pwwn 50:08:01:60:01:5d:51:12
    pwwn 50:08:01:60:01:5d:51:13

  zone name sb1 vsan 1
    pwwn 20:0e:00:11:0d:10:dc:00
```

```
    pwwn 20:0d:00:11:0d:10:da:00
    pwwn 20:13:00:11:0d:15:75:00
    pwwn 20:0d:00:11:0d:10:db:00
```

The following example displays configured zone set information for a specific VSAN.

```
switch# show zoneset vsan 2-3
zoneset name ZoneSet2 vsan 1
  zone name Zone2 vsan 1
     fwwn 20:52:00:05:30:00:2a:1e
    fwwn 20:53:00:05:30:00:2a:1e
    fwwn 20:54:00:05:30:00:2a:1e
    fwwn 20:55:00:05:30:00:2a:1e
    fwwn 20:56:00:05:30:00:2a:1e
  zone name Zone1 vsan 1
    pwwn 21:00:00:20:37:6f:db:dd
    pwwn 21:00:00:20:37:a6:be:2f
    pwwn 21:00:00:20:37:9c:48:e5
    fcalias Alias1
zoneset name ZoneSet1 vsan 1
  zone name Zone1 vsan 1
    pwwn 21:00:00:20:37:6f:db:dd
    pwwn 21:00:00:20:37:a6:be:2f
    pwwn 21:00:00:20:37:9c:48:e5
    fcalias Alias1
```

T Commands

tacacs+ abort

To discard a TACACS+ Cisco Fabric Services (CFS) distribution session in progress, use the **tacacs+ abort** command **in configuration mode.**

tacacs+ **abort**

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, TACACS+ must be enabled using the **tacacs+ enable** command.

Examples

The following example shows how to discard a TACACS+ CFS distribution session in progress:

```
switch# config terminal
switch(config)# tacacs+ abort
```

Related Commands

Command	Description
show tacacs+	Displays TACACS+ CFS distribution status and other details.
tacacs+ distribute	Enables CFS distribution for TACACS+.
tacacs+ enable	Enables TACACS+.

tacacs+ commit

To apply the pending configuration pertaining to the TACACS+ Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **tacacs+ commit** command **in configuration mode.**

tacacs+ **commit**

Syntax Description

This command has no other arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, TACACS+ must be enabled using the **tacacs+ enable** command.

Examples

The following example shows how to apply a TACACS+ configuration to the switches in the fabric:

```
switch# config terminal
switch(config)# tacacs+ commit
```

Related Commands

Command	Description
show tacacs+	Displays TACACS+ CFS distribution status and other details.
tacacs+ enable	Enables TACACS+.
tacacs+ distribute	Enables CFS distribution for TACACS+.

tacacs+ distribute

To enable Cisco Fabric Services (CFS) distribution for TACACS+, use the **tacacs+ distribute** command. To disable this feature, use the **no** form of the command.

tacacs+ **distribute**
no tacacs+ **distribute**

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, TACACS+ must be enabled using the **tacacs+ enable** command.

Examples

The following example shows how to enable TACACS+ fabric distribution:

```
switch# config terminal
switch(config)# tacacs+ distribute
```

Related Commands

Command	Description
show tacacs+	Displays TACACS+ CFS distribution status and other details.
tacacs+ commit	Commits TACACS+ database changes to the fabric.
tacacs+ enable	Enables TACACS+.

tacacs+ enable

To enable TACACS+ in a switch, use the **tacacs+ enable** command in configuration mode. To disable this feature, use the **no** form of the command.

tacacs+ **enable**
no tacacs+ **enable**

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
NX-OS 4.1(1b)	This command was deprecated.

Usage Guidelines

Additional TACACS+ commands are only available when the TACACS+ feature is enabled.

Using SHA-1 as the hash algorithm may prevent RADIUS or TACACS+ usage.

Examples

The following example shows how to enable TACACS+ in a switch:

```
switch# config terminal
switch(config)# tacacs+ enable
```

Related Commands

Command	Description
show tacacs+	Displays TACACS+ server information.

tacacs-server deadtime

To set a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness, use the **tacacs-server deadtime** command. To disable the monitoring of the nonresponsive TACACS+ server, use the **no** form of the command.

tacacs-server deadtime *time*
no tacacs-server deadtime *time*

Syntax Description

time	Specifies the time interval in minutes. The range is 1 to 1440.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Setting the time interval to zero disables the timer. If the dead time interval for an individual TACACS+ server is greater than zero (0), that value takes precedence over the value set for the server group.

When the dead time interval is 0 minutes, TACACS+ server monitoring is not performed unless the TACACS+ server is part of a server group and the dead time interval for the group is greater than 0 minutes.

Examples

The following example shows how to set a duration of 10 minutes:

```
switch# config terminal
switch(config)# tacacs
-server deadtime 10
```

Related Commands

Command	Description
deadtime	Sets a time interval for monitoring a nonresponsive TACACS+ server.
show tacacs-server	Displays all configured TACACS+ server parameters.

tacacs-server directed-request

To specify a TACACS+ server to send authentication requests to when logging in, use the **tacacs-server directed-request** command. To revert to sending the authentication request to the configured group, use the **no** form of the command.

tacacs-server directed-request
no tacacs-server directed-request

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The user can specify the *username@servername* during login. The user name is sent to the server name for authentication.

Examples

The following example shows how to specify a TACACS+ server to send authentication requests when logging in:

```
switch# config terminal
switch(config)# tacacs
-server
directed-request
```

Related Commands

Command	Description
show tacacs-server	Displays all configured TACACS+ server parameters.
show tacacs-server directed request	Displays a directed request TACACS+ server configuration.

tacacs-server host

To configure TACACS+ server options on a switch, use the **tacacs-server host** command in configuration mode. Use the **no** form of the command to revert to factory defaults.

tacacs-server host {*server-nameipv4-addressipv6-address*} [**key** [{**0**|**7**}] *shared-secret*] [**port** *port-number*] [**test** {**idle-time time**|**password password**|**username name**}] [**timeout** *seconds*]
no tacacs-server host {*server-nameipv4-addressipv6-address*} [**key** [{**0**|**7**}] *shared-secret*] [**port** *port-number*] [**test** {**idle-time time**|**password password**|**username name**}] [**timeout** *seconds*]

Syntax Description

server-name	Specifies the TACACS+ server DNS name. The maximum character size is 253.
ipv4-address	Specifies the TACACS+ server IP address. in the format *A.B.C.D* .
ipv6-address	Specifies the TACACS+ server IP address in the format *X:X::X* .
key	(Optional) Configures the TACACS+ server's shared secret key.
0	(Optional) Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.
shared secret	(Optional) Configures a preshared key to authenticate communication between the TACACS+ client and server.
port *port-number*	(Optional) Configures a TACACS+ server port for authentication. The range is 1 to 65535.
test	(Optional) Configures parameters to send test packets to the TACACS+ server.
idle-time*time*	(Optional) Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.
password*password*	(Optional) Specifies a user password in the test packets. The maximum size is 32.
username*name*	(Optional) Specifies a user name in the test packets. The maximum size is 32.
timeout	(Optional) Configures a TACACS+ server timeout period.
seconds	(Optional) Specifies the timeout (in seconds) between retransmissions to the TACACS+ server. The range is 1 to 60 seconds.

Command Default

Idle-time is not set. Server monitoring is turned off.Timeout is 1 second.Username is test.Password is test.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Added the *ipv6-address* argument and the **test** option.

Usage Guidelines

This command is only available when the TACACS+ feature is enabled using the **tacacs+ enable** command.

When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.

Examples

The following example configures TACACS+ authentication:

```
switch# config terminal
switch(config)# tacacs-server host 10.10.2.3 key HostKey
switch(config)# tacacs-server host tacacs2 key 0 abcd
switch(config)# tacacs-server host tacacs3 key 7 1234
switch(config)# tacacs-server host 10.10.2.3 test idle-time 10
switch(config)# tacacs-server host 10.10.2.3 test username tester
switch(config)# tacacs-server host 10.10.2.3 test password 2B9ka5
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
tacacs+ enable	Enables TACACS+.

tacacs-server key

To configure a global TACACS+ shared secret, use the **tacacs-server key** command. Use the **no** form of this command to removed a configured shared secret.

tacacs-server key [{**0**|**7**}] *shared-secret*
no tacacs-server key [{**0**|**7**}] *shared-secret*

Syntax Description

key	Specifies a global TACACS+ shared secret.
0	(Optional) Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.
shared-secret	Configures a preshared key to authenticate communication between the TACACS+ client and server.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You need to configure the TACACS+ preshared key to authenticate the switch to the TACACS+ server. The length of the key is restricted to 65 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all TACACS+ server configurations on the switch. You can override this global key assignment by explicitly using the **key** option in the **tacacs-server host** command.

This command is only available when the TACACS+ feature is enabled using the **tacacs+ enable** command.

Examples

The following example configures TACACS+ server shared keys:

```
switch# config terminal
switch(config)# tacacs-server key AnyWord
switch(config)# tacacs-server key 0 AnyWord
switch(config)# tacacs-server key 7 public
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
tacacs+ enable	Enable TACACS+.

tacacs-server test

To configure a parameter to send test packets, use the tacacs-server test command. To disable this feature, use the no form of the command.

```
tacacs-server test {{username username|{[password password [idle-time
time]]|[idle-time time]}}|password password [idle-time time]|idle-time time}

no tacacs-server test {{username username|{[password password [idle-time
time]]|[idle-time time]}}|password password [idle-time time]|idle-time time}
```

Syntax Description

username	Specifies the username in test packets.
username	Specifies user name. The maximum size is 32 characters.
password	(Optional) Specifies the user password in test packets.
password	Specifies the user password. The maximun size is 32 characters.
idle-time	(Optional) Specifies the time interval for monitoring the server.
time period	Specifies the time period in minutes. The range is from 1 to 4440.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

Defaults will be used for anything not provided by CLI. Also doing a "no" of any parameters will revert it back to default.

Examples

The following example shows how to display the username in test packets:

```
switch# config t
switch(config)# tacacs-server test username test idle-time 0
switch(config)# tacacs-server test username test password test idle-time 1
switch(config)#
```

The following example shows how to display the time interval for monitoring the server:

```
switch(config)# tacacs-server test idle-time 0
switch(config)#
```

The following example shows how to display the user password in test packets:

```
switch(config)# tacacs-server test password test idle-time 0
switch(config)#
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
tacacs+ enable	Enable TACACS+.

tacacs-server timeout

To specify the time between retransmissions to the TACACS+ servers, use the **tacacs-server timeout** command. You can revert the retransmission time to its default by using the **no** form of the command.

tacacs-server timeout *seconds*
no tacacs-server timeout *seconds*

Syntax Description

seconds	Specifies the time (in seconds) between retransmissions to the RADIUS server. The default is one (1) second and the valid range is 1 to 60 seconds.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(2)	This command was introduced.

Usage Guidelines

This command is only available when the TACACS+ feature is enabled using the **tacacs+ enable** command.

Examples

The following example configures the TACACS+ server timeout value:

```
switch# config terminal
switch(config)# tacacs-server timeout 30
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
tacacs+ enable	Enable TACACS+.

tag

To correlate multiple events in an event manager applet, use the **tag** command. To remove the correlation, use the **no** form of the command.

tag tagname1 { **and** | **andnot** | **or** } **tagname2** [{ **and** | **andnot** | **or** } *tagname3* [{ **and** | **andnot** | **or** } *tagname4*]] **happens occurs in seconds**
no tag tagname1 { **and** | **andnot** | **or** } **tagname2** [{ **and** | **andnot** | **or** } *tagname3* [{ **and** | **andnot** | **or** } *tagname4*]] **happens occurs in seconds**

Syntax Description

tagname	The tag name of a tagged event. A maximum of 4 tag names may be specified. A tag name may comprise of any alphanumeric character (a-z, 0-9). The maximum length is 29 characters.
and	(Optional) Specifies to evaluate tagged events using boolean *and* logic.
andnot	(Optional) Specifies to evaluate tagged events using boolean *andnot* logic.
or	(Optional) Specifies to evaluate tagged events using boolean *or* logic.
happens	Specifies the number of occurrences of the tag combination that must occur before executing the applet actions.
occurs	Numbers of times the event combination occurs. The range is from 1 to 4294967295.
in	Specifies the number of occurrences that must occur within the given time period.
seconds	Maximum amount of time, in seconds, within which the complete event combination occurs. The range is from 0 to 4294967295 seconds.

Command Default

None

Command Modes

config-applet

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Tag names have scope only within the policy they are defined in. Tag names must be already configured in **event** commands before they can be used in a **tag** command.The evaluation of tag logic operators is from left to right since all operators are of equal precedence, that is:

```
((tagA operation1 tagB) operation2 tagC) operation3 tagD
```

When a **cli match** event is tagged, the behavior changes compared to untagged **cli match** events. Commands matching a tagged **cli match** event are executed immediately. If this were not the case, there may be a delay while waiting for other tagged events to match before an **event-default** command in the applet action block is executed.

Examples

The following example shows how to use the tag command. The goal in this example is to save the latest core dump to bootflash (it could also be sent to an SFTP server etc). The first policy is triggered when a process crash is about to generate a core file. It sleeps for 60 seconds while the core file is generated and then increments a counter. The second policy monitors the counter as well as system switchover events. If the counter is greater than 0 and no switchovers have occurred in the last 60 seconds then the latest core file is copied to bootflash and the counter reset to 0. No **exit-op** is specified for the counter so that the second policy can be triggered multiple times at once.

```
switch# configure terminal
switch(config)# event manager applet coreDump
switch(config-applet)# event syslog pattern "SERVICE_CRASHED.*core will be saved"
switch(config-applet)# action 10 cli local sleep 60
switch(config-applet)# action 20 counter name cores value 1 op inc
switch(config-applet)# event manager applet saveCore
switch(config-applet)# exit
switch(config)# event manager applet saveCore
switch(config-applet)# event counter tag coreDumped name cores entry-val 0 entry-op gt
switch(config-applet)# event syslog tag swDone pattern "SWITCHOVER_OVER"
switch(config-applet)# tag coreDumped andnot swDone happens 1 in 60
switch(config-applet)# action 10 cli local sh core | last 1 | sed 's/ \+/ /g' | sed
's_\([0-9]\+\) \([0-9]\+\) .* \([0-9]\+\) .*_copy core://\1/\3/\2 bootflash:_' | vsh
switch(config-applet)# action 20 counter name cores value 0 op set
switch(config-applet)# exit
```

Command	Description
action	Configures a command to be executed when an Embedded Event Manager (EEM) applet is triggered.
event	Configures a detectable condition for an EEM applet.
event manager applet	Registers an EEM applet with the EEM.

tail

To display the last lines (tail end) of a specified file, use the **tail** command in EXEC mode.

tail *filename* [*number-of-lines*]

Syntax Description

filename	The name of the file for which you want to view the last lines.
number-of-lines	(Optional) The number of lines you want to view. The range is 0 to 80 lines.

Command Default

Displays the last 10 lines.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You need two separate CLI terminals to use this command. In one terminal, execute the run-script or any other desired command. In the other, enter the **tail** command for the mylog file. On the second terminal session, you will see the last lines of the mylog file (as it grows) that is being saved in response to the command issued in the first terminal.

If you specify a long file and would like to exit in the middle, press **Ctrl-C** to exit this command.

Examples

The following example displays the last lines (tail end) of a specified file:

```
switch# run-script slot0:test mylog
```

In another terminal, enter the **tail** command for the mylog file:

```
switch# tail mylog
config terminal
```

In the second CLI terminal, you see the last lines of the mylog file (as it grows) that is being saved in response to the command entered in the first terminal.

tape compression

To configure tape compression, use the tape-compression command. To disable this feature, use the no form of the command.

tape-compression
no tape-compression

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Cisco SME cluster configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

Use this command to compress encrypted data.

Examples

The following example enables tape compression:

```
switch#config t
switch(config)#sme cluster c1
switch(config-sme-cl)#tape-compression
```

The following example disables tape compression:

```
switch#config t
switch(config)#sme cluster c1
switch(config-sme-cl)#no tape-compression
```

Related Commands

Command	Description
clear sme	Clears Cisco SME configuration.
show sme cluster	Displays information about the Cisco SME cluster.
show sme cluster tape	Displays information about all tape volume groups or a specific group.

tape-bkgrp

To configure a crypto tape backup group, use the tape-bkgrp command. Use the no form of this command to disable this feature.

tape-bkgrp groupname
no tape-bkgrp groupname

Syntax Description

groupname	Specifies the backup tape group.

Command Default

None.

Command Modes

Cisco SME cluster configuration mode submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

A tape volume group is a group of tapes that are categorized by function. For example, HR1 could be designated tape volume group for all Human Resources backup tapes.

Adding tape groups allows you to select VSANs, hosts, storage devices, and paths that Cisco SME will use for encrypted data. For example, adding a tape group for HR data sets the mapping for Cisco SME to transfer data from the HR hosts to the dedicated HR backup tapes.

Examples

The following example adds a backup tape group:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# tape-bkgrp group1
switch(config-sme-cl-tape-bkgrp)#
```

The following example removes a backup tape group:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# no tape-bkgrp group1
switch(config-sme-cl-tape-bkgrp)#
```

Related Commands

Command	Description
clear sme	Clears Cisco SME configuration.
show sme cluster	Displays information about the Cisco SME cluster

tape-device

To configure a crypto tape device, use the tape-device command. To disable this feature, use the no form of the command.

tape-device device name
no tape-device device name

Syntax Description

device name	Specifies the name of the tape device.

Command Default

None.

Command Modes

Cisco SME tape volume configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

The tape device commands are available in the (config-sme-cl-tape-bkgrp-tapedevice) submode.

Examples

The following example configures a crypto tape device:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# tape-bkgrp group1
switch(config-sme-cl-tape-bkgrp)# tape-device devicename1
switch(config-sme-cl-tape-bkgrp-tapedevice)#
```

The following example removes a crypto tape device:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# tape-bkgrp group1
switch(config-sme-cl-tape-bkgrp)# no tape-device devicename1
switch(config-sme-cl-tape-bkgrp-tapedevice)#
```

Related Commands

Command	Description
clear sme	Clears Cisco SME configuration.
show sme cluster	Displays information about the Cisco SME cluster
show sme cluster tape	Displays information about all tape volume groups or a specific group

tape-keyrecycle

To configure tape key recycle policy, use the tape-keyrecycle command. To disable this feature, use the no form of the command.

tape-keyrecycle
no tape-keyrecycle

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Cisco SME cluster configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

Cisco SME allows you to recycle the tape keys. If you enable tape key recycling, all the previous instances of the tape key will be deleted. If you do not enable tape key recycle, all the previous instances and the current instance of the tape key is maintained, and the current instance is incremented by 1.

Examples

The following example enables tape key recycling:

```
switch# config t
switch(config)#sme cluster c1
switch(config-sme-cl)#tape-keyrecycle
```

The following example disables tape key recycling:

```
switch# config t
switch(config)#sme cluster c1
switch(config-sme-cl)#no tape-keyrecycle
```

Related Commands

Command	Description
clear sme	Clears Cisco SME configuration.
show sme cluster	Displays information about the Cisco SME cluster

tape-read command-id

To configure a SCSI tape read command for a SAN tuner extension N port, use the **tape-read command-id** command.

tape-read command-id *cmd-id* **target** *pwwn* **transfer-size** *bytes* [{**continuous** [**filemark-frequency frequency**]|**num-transactions** *number* [**filemark-frequency frequency**]}]

Syntax Description

cmd-id	Specifies the command identifier. The range is 0 to 2147483647.
target *pwwn*	Specifies the target port WWN. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
transfer-size *bytes*	Specifies the transfer size in multiples of 512 bytes. The range is 512 to 8388608.
continuous	(Optional) Specifies that the command is performed continuously.
filemark-frequency *frequency*	(Optional) Specifies the filemark frequency. The range is 1 to 2147483647.
num-transactions *number*	(Optional) Specifies a number of transactions. The range is 1 to 2147483647.

Command Default

Filemark frequency: 0.

Command Modes

SAN extension N port configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

To stop a continuous SCSI tape read command in progress, use the **stop command-id** command.

Note There can be just one outstanding I/O at a time to the virtual N port that emulates the tape behavior.

Examples

The following example configures a single SCSI tape read command:

```
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)# tape-
read command-id 100 target 22:22:22:22:22:22:22:22 transfer-size 512000 num-transactions
5000000 filemark-frequency 32
```

The following example configures a continuous SCSI tape read command.

```
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)# tape-
read command-id 100 target 22:22:22:22:22:22:22:22 transfer-size 512000 continuous
filemark-frequency 32
```

Related Commands

Command	Description
nport pwwn	Configures a SAN extension tuner N port.
san-ext-tuner	Enables the SAN extension tuner feature.
show san-ext-tuner	Displays SAN extension tuner information.
stop	Cancels a SCSI command in progress on a SAN extension tuner N port.

tape-volgrp

To configure the crypto tape volume group, use the tape-volgrp command. To disable this command, use the no form of the command.

tape-volgrp group name
no tape-volgrp group name

Syntax Description

group name	Specifies the tape volume group name.

Command Default

None.

Command Modes

Cisco SME crypto backup tape group configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

The tape volume group commands are available in the Cisco SME crypto tape volume group (config-sme-cl-tape-bkgrp-volgrp) submode.

Examples

The following example configures a crypto tape volume group:

```
switch# config t
switch(config))# sme cluster c1
switch(config-sme-cl)# tape-bkgrp tbg1
switch(config-sme-cl-tape-bkgrp)# tape-volgrp tv1
switch(config-sme-cl-tape-bkgrp-volgrp)#
```

The following example removes a crypto tape volume group:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# tape-bkgrp tbg1
switch(config-sme-cl-tape-bkgrp)# no tape-volgrp tv1
```

Related Commands

Command	Description
clear sme	Clears Cisco SME configuration.
show sme cluster tape	Displays information about tapes

tape-write command-id

To configure a SCSI tape write command for a SAN tuner extension N port, use the **tape-write command-id** command.

tape-write command-id *cmd-id* **target** *pwwn* **transfer-size** *bytes* [{**continuous** [**filemark-frequency frequency**]|**num-transactions** *number* [**filemark-frequency frequency**]}]

Syntax Description

cmd-id	Specifies the command identifier. The range is 0 to 2147483647.
target *pwwn*	Specifies the target port WWN. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
transfer-size *bytes*	Specifies the transfer size in multiples of 512 bytes. The range is 512 to 8388608.
continuous	(Optional) Specifies that the command is performed continuously.
filemark-frequency *frequency*	(Optional) Specifies the filemark frequency. The range is 1 to 2147483647.
num-transactions *number*	(Optional) Specifies a number of transactions. The range is 1 to 2147483647.

Command Default

Filemark frequency: 0.

Command Modes

SAN extension N port configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

To stop a continuous SCSI tape write command in progress, use the **stop command-id** command.

Note There can be just one outstanding I/O at a time to the virtual N port that emulates the tape behavior.

Examples

The following example configures a single SCSI tape write command:

```
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)# tape-
write command-id 100 target 22:22:22:22:22:22:22:22 transfer-size 512000 num-transactions
5000000 filemark-frequency 32
```

The following example configures a continuous SCSI tape write command:

```
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)# tape-
write command-id 100 target 22:22:22:22:22:22:22:22 transfer-size 512000 continuous
filemark-frequency 32
```

Related Commands

Command	Description
nport pwwn	Configures a SAN extension tuner N port.
san-ext-tuner	Enables the SAN extension tuner feature.
show san-ext-tuner	Displays SAN extension tuner information.
stop	Cancels a SCSI command in progress on a SAN extension tuner N port.

target (iSLB initiator configuration)

To configure an iSLB initiator target, use the **target** command in iSLB initiator configuration submode. To remove the target configuration, use the **no** form of the command.

target {**device-alias device-alias**|**pwwn pWWN**} [**vsan vsan-id**] **[no-zone] [trespass] [revert-primary-port]** [**fc-lun LUN iscsi-lun LUN**] [{**sec-device-alias device-alias**|**sec-pwwn pWWN**}] [**sec-vsan sec-vsan-id**] [**sec-lun LUN**] [**iqn-name target-name**]
no target {**device-alias device-alias**|**pwwn pWWN**} [**vsan vsan-id**] **[no-zone] [trespass] [revert-primary-port]** [**fc-lun LUN iscsi-lun LUN**] [{**sec-device-alias device-alias**|**sec-pwwn pWWN**}] [**sec-vsan sec-vsan-id**] [**sec-lun LUN**] [**iqn-name target-name**]

Syntax Description

device-alias *device-alias*	Specifies the device alias of the Fibre Channel target.
pwwn *pWWN*	Specifies the pWWN of the Fibre Channel target. The format is *hh:hh:hh:hh:hh:hh:hh:hh* .
vsan	(Optional) Assigns VSAN membership to the initiator target.
vsan-id	(Optional) Specifies the VSAN ID. The range is 1 to 4093.
no-zone	(Optional) Indicates no automatic zoning.
trespass	(Optional) Enables trespass support.
revert-primary-port	(Optional) Reverts to the primary port when it comes back up.
fc-lun *LUN*	(Optional) Specifies the Fibre Channel LUN of the Fibre Channel target. The format is 0xhhhh[:hhhh[:hhhh[:hhhh]]]
iscsi-lun *LUN*	(Optional) Specifies the iSCSI LUN. The format is 0xhhhh[:hhhh[:hhhh[:hhhh]]].
sec-device-alias	(Optional) Specifies the device alias of the secondary Fibre Channel target.
target-device-alias	(Optional) Specifies the initiator's target device alias. The maximum size is 64.
sec-pwwn *pWWN*	(Optional) Specifies the pWWN of the secondary Fibre Channel target. The format is *hh:hh:hh:hh:hh:hh:hh:hh* .
sec-vsan	(Optional) Assigns VSAN membership to the initiator.
sec-vsan-id	(Optional) Specifies the VSAN ID. The range is 1 to 4093.
sec-lun LUN	(optional) Specifies the FC LUN of the secondary Fibre Channel target. The format is 0xhhhh[:hhhh[:hhhh[:hhhh]]].
iqn-name	(Optional) Specifies the name of the target.
target-name	Specifies the initiator's target name. The maximum size is 223.

Command Default

None.

Command Modes

iSLB initiator configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can configure an iSLB initiator target using the device alias or the pWWN. You have the option of specifying one or more of the following optional parameters:

- Secondary pWWN
- Secondary device alias
- LUN mapping
- IQN
- VSAN identifier

Note The VSAN identifier is optional if the target is online. If the target is not online, the VSAN identifier is required.

If you configure an IQN for an initiator target, then that name is used to identify the initiator target. Otherwise, a unique IQN is generated for the initiator target.

Examples

The following example configures an iSLB initiator using an IP address and then enters iSLB initiator configuration submode:

```
switch# config t
switch(config)# islb initiator ip-address 209.165.200.226
```

The following example grants iSLB initiator access to the target using a pWWN with auto zoning enabled (default):

```
switch (config-islb-init)# target pwwn 26:00:01:02:03:04:05:06
```

The following example grants iSLB initiator access to the target using a pWWN with auto zoning disabled:

```
switch (config-islb-init)# target pwwn 26:00:01:02:03:04:05:06 no-zone
```

The following example grants iSLB initiator access to the target using a device alias and optional LUN mapping:

switch(config-islb-init)# **target device-alias SampleAlias fc-lun 0x1234 iscsi-lun 0x2345**

The following example grants iSLB initiator access to the target using a device alias and an optional IQN:

switch(config-islb-init)# **target device-alias SampleAlias iqn-name iqn.1987-01.com.cisco.initiator**

The following example grants iSLB initiator access to the target using a device alias and a VSAN identifier:

```
switch(config-islb-init)# target device-alias SampleAlias vsan 10
```

Note The VSAN identifier is optional if the target is online. If the target is not online, the VSAN identifier is required.

The following example disables the configured iSLB initiator target.

```
switch (config-islb-init)# no
 target pwwn 26:00:01:02:03:04:05:06
```

Related Commands

Command	Description
islb initiator	Assigns an iSLB name and IP address to the iSLB initiator and enters iSLB initiator configuration submode.
show islb initiator	Displays iSLB CFS information.
show islb initiator detail	Displays detailed iSLB initiator information.
show islb initiator summary	Displays iSLB initiator summary information.

tclquit

To exit Tcl, use the **tclquit** command.

tclquit

Syntax Description

None.

Command Default

None.

Command Modes

Interactive Tcl shell and Tcl script.

Command History

Release	Modification
NX-OS 5.1(1)	This command was introduced.

Usage Guidelines

Terminates the current Tcl process. Synonym for the **exit** command.

Examples

The following example terminates the current interactive Tcl shell:

```
switch-tcl# tclquit
switch#
```

Related Commands

Command	Description
exit	End the Tcl application (for a list of standard Tcl commands, see the Tcl documentation).

tcp cwm

To configure congestion window monitoring (CWM) TCP parameters, use the **tcp cwm** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp cwm [**burstsize** *size*]
no tcp cwm [**burstsize** *size*]

Syntax Description

burstsize *size*	(Optional) Specifies the burstsize ranging from 10 to 100 KB.

Command Default

Enabled.

The default FCIP burst size is 10 KB.

The default iSCSI burst size is 50 KB

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

Use these TCP parameters to control TCP retransmission behavior in a switch.

Examples

The following example configures a FCIP profile and enables congestion monitoring:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)# tcp cwm
```

The following example assigns the burstsize value at 20 KB:

```
switch(config-profile)# tcp cwm burstsize 20
```

The following example disables congestion monitoring:

```
switch(config-profile)# no tcp cwm
```

The following example leaves the CWM feature in an enabled state but changes the burstsize to the default of 10 KB:

```
switch(config-profile)# no tcp cwm burstsize 25
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.

Command	Description
show fcip profile	Displays FCIP profile information.

tcp keepalive-timeout

To configure the interval between which the TCP connection verifies if the FCIP link is functioning, use the **tcp keepalive-timeout** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp keepalive-timeout *seconds*
no tcp keepalive-timeout *seconds*

Syntax Description

seconds	Specifies the time in seconds. The range is 1 to 7200.

Command Default

60 seconds.

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command can be used to detect FCIP link failures.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)#
```

The following example specifies the keepalive timeout interval for the TCP connection:

```
switch(config-profile)# tcp keepalive-timeout 120
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp maximum-bandwidth-kbps

To manage the TCP window size in Kbps, use the **tcp maximum-bandwidth-kbps** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp max-bandwidth-kbps *bandwidth* **min-available-bandwidth-kbps** *threshold* {**round-trip-time-ms** *milliseconds*|**round-trip-time-us** *microseconds*}
no tcp max-bandwidth-kbps *bandwidth* **min-available-bandwidth-kbps** *threshold* {**round-trip-time-ms** *milliseconds*|**round-trip-time-us** *microseconds*}

Syntax Description

bandwidth	Specifies the Kbps bandwidth. The range is 1000 to 1000000.
min-available-bandwidth-kbps	Configures the minimum slow start threshold.
threshold	Specifies the Kbps threshold. The range is 1000 to 1000000. For Cisco MDS 9250i Multiservice Fabric Switch, the range is 1000 to 10000000.
round-trip-time-ms *milliseconds*	Configures the estimated round-trip time across the IP network to reach the FCIP peer end point in milliseconds. The range is 0 to 300.
round-trip-time-us *microeconds*	Configures the estimated round-trip time across the IP network to reach the FCIP peer end point in microseconds. The range is 0 to 300000.

Command Default

Enabled.

The FCIP defaults are **max-bandwidth** = 1G, **min-available-bandwidth** = 500 Mbps, and **round-trip-time** =1 ms.

The iSCSI defaults are **max-bandwidth** = 10000 Mbps (10Gbps), **min-available-bandwidth** = 8000 Mbps, and **round-trip-time** =1 ms.

Command Modes

FCIP profile configuration submode.

iSCSI interface configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.
6.2(5)	The IPStorage support was increased to 10G on the Cisco MDS 9250i Multiservice Fabric Switch.
6.2(13)	The maximum bandwidth of iSCSI was increased to 10G.

Usage Guidelines

The **maximum-bandwidth** option and the **round-trip-time** option together determine the window size.

The **minimum-available-bandwidth** option and the **round-trip-time** option together determine the threshold below which TCP aggressively increases its size. After it reaches the threshold the software uses standard TCP rules to reach the maximum available bandwidth.

When configuring tcp bandwidth using the **tcp maximum-bandwidth-kbps** and **tcp minimum-bandwidth-kbps** commands, the value should not exceed the maximum speed of the physical IPStorage port.

The maximum and minimum tcp bandwidth of all the FCIP and iSCSI interfaces that are using a specific Gigabit Ethernet or IPStorage port should not exceed the maximum speed of the physical IPStorage port.

For optimal performance the minimum-bandwidth-kbps should be 80%-90% of the maximum-bandwidth-kbps.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)#
```

The following example configures the maximum available bandwidth at 900 Kbps, the minimum slow start threshold as 300 Kbps, and the round trip time as 10 milliseconds:

```
switch(config-profile)# tcp max-bandwidth-kbps 900 min-available-bandwidth-kbps 300
round-trip-time-ms 10
```

The following example reverts to the factory defaults:

```
switch(config-profile)# no tcp max-bandwidth-kbps 900 min-available-bandwidth-kbps 300
round-trip-time-ms 10
```

The following example configures the maximum available bandwidth at 2000 Kbps, the minimum slow start threshold as 2000 Kbps, and the round trip time as 200 microseconds:

```
switch(config-profile)# tcp max-bandwidth-kbps 2000 min-available-bandwidth-kbps 2000
round-trip-time-us 200
```

The following example configures an iSCSI profile:

```
switch# configure terminal
switch(config)# interface iscsi 1/1-2
switch(config-if)#
```

The following example configures the maximum available bandwidth at 9000000 Kbps, the minimum slow start threshold as 8000000 Kbps, and the round trip time as 20 milliseconds:

```
switch(config-if)# tcp max-bandwidth-kbps 9000000 min-available-bandwidth-kbps 8000000
round-trip-time-ms 20
```

The following example configures the maximum available bandwidth at 9000000 Kbps, the minimum slow start threshold as 8000000 Kbps, and the round trip time as 20 milliseconds:

```
switch(config-if)# tcp max-bandwidth-kbps 9000000 min-available-bandwidth-kbps 8000000
round-trip-time-ms 20
```

The following example reverts to the factory defaults:

```
switch(config-if)# no tcp max-bandwidth-kbps 10000000 min-available-bandwidth-kbps 8000000
round-trip-time-ms 20
```

The following example configures the maximum available bandwidth at 5000000 Kbps, the minimum slow start threshold as 4000000 Kbps, and the round trip time as 200 microseconds:

```
switch(config-if)# tcp max-bandwidth-kbps 5000000 min-available-bandwidth-kbps 4000000
round-trip-time-ms 200
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.
show interface iscsi	Displays the iSCSI configuration for the port along with the tcp maximum and minimum bandwidth configuration.

tcp maximum-bandwidth-mbps

To manage the TCP window size in Mbps, use the **tcp maximum-bandwidth-mbps** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp max-bandwidth-mbps *bandwidth* **min-available-bandwidth-mbps** *threshold* {**round-trip-time-ms** *milliseconds*|**round-trip-time-us** *microseconds*}
no tcp max-bandwidth-mbps *bandwidth* **min-available-bandwidth-mbps** *threshold* {**round-trip-time-ms** *milliseconds*|**round-trip-time-us** *microseconds*}

Syntax Description

bandwidth	Specifies the Mbps bandwidth. The range is 1 to 1000.
min-available-bandwidth-mbps	Configures the minimum slow start threshold.
threshold	Specifies the Mbps threshold. The range is 1 to 1000. For Cisco MDS 9250i Multiservice Fabric Switch, the range is 1 to 10000.
round-trip-time-ms *milliseconds*	Configures the estimated round trip time across the IP network to reach the FCIP peer end point in milliseconds. The range is 0 to 300.
round-trip-time-us *microeconds*	Configures the estimated round trip time across the IP network to reach the FCIP peer end point in microseconds. The range is 0 to 300000.

Command Default

Enabled.

The FCIP defaults are **max-bandwidth** = 1G, **min-available-bandwidth** = 500 Mbps, and **round-trip-time** =1 ms.

The iSCSI defaults are **max-bandwidth** = 10000 Mbps (10Gbps), **min-available-bandwidth** = 8000 Mbps, and **round-trip-time** =1 ms.

Command Modes

FCIP profile configuration submode.

iSCSI interface configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.
6.2(5)	The IPStorage support was increased to 10G on the Cisco MDS 9250i Multiservice Fabric Switch.
6.2(13)	The maximum bandwidth of iSCSI was increased to 10G.

Usage Guidelines

The **maximum-bandwidth** option and the **round-trip-time** option together determine the window size.

The **minimum-available-bandwidth** option and the **round-trip-time** option together determine the threshold below which TCP aggressively increases its size. After it reaches the threshold the software uses standard TCP rules to reach the maximum available bandwidth.

When configuring tcp bandwidth using the **tcp maximum-bandwidth-mbps** and **tcp minimum-bandwidth-mbps** commands, the value should not exceed the maximum speed of the physical IPStorage port.

The maximum and minimum tcp bandwidth of all the FCIP and iSCSI interfaces that are using a specific Gigabit Ethernet or IPStorage port should not exceed the maximum speed of the physical IPStorage port.

For optimal performance the minimum-bandwidth-mbps should be 80%-90% of the maximum-bandwidth-mbps.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)#
```

The following example configures the maximum available bandwidth at 900 Mbps, the minimum slow start threshold as 300 Mbps, and the round trip time as 10 milliseconds:

```
switch(config-profile)# tcp max-bandwidth-mbps 900 min-available-bandwidth-mbps 300
round-trip-time-ms 10
```

The following example reverts to the factory defaults:

```
switch(config-profile)# no tcp max-bandwidth-mbps 900 min-available-bandwidth-mbps 300
round-trip-time-ms 10
```

The following example configures the maximum available bandwidth at 2000 Mbps, the minimum slow start threshold as 2000 Mbps, and the round trip time as 200 microseconds:

```
switch(config-profile)# tcp max-bandwidth-mbps 2000 min-available-bandwidth-mbps 2000
round-trip-time-us 200
```

The following example configures an iSCSI profile:

```
switch# configure terminal
switch(config)# interface iscsi 1/1-2
switch(config-if)#
```

The following example configures the maximum available bandwidth at 9000 Mbps, the minimum slow start threshold as 8000 Mbps, and the round trip time as 20 milliseconds:

```
switch(config-if)# tcp max-bandwidth-mbps 9000 min-available-bandwidth-mbps 8000
round-trip-time-ms 20
```

The following example reverts to the factory defaults:

```
switch(config-if)# no tcp max-bandwidth-mbps 10000 min-available-bandwidth-mbps 8000
round-trip-time-ms 20
```

The following example configures the maximum available bandwidth at 5000 Mbps, the minimum slow start threshold as 4000 Mbps, and the round trip time as 200 microseconds:

```
switch(config-if)# tcp max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4000
round-trip-time-ms 200
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.

Command	Description
show fcip profile	Displays FCIP profile information.
show interface iscsi	Displays the iSCSI configuration for the port along with the tcp maximum and minimum bandwidth configuration.

tcp max-jitter

To estimate the maximum delay jitter experienced by the sender in microseconds, use the **tcp max-jitter** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp max-jitter *microseconds*
no tcp max-jitter *microseconds*

Syntax Description

microseconds	Specifies the delay time in microseconds ranging from 0 to 10000.

Command Default

Enabled.

The default value is 100 microseconds for FCIP and 500 microseconds for iSCSI interfaces.

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures delay jitter time:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# fcip profile 3
switch(config-profile)# tcp max-jitter 600
switch(config-profile)# do show fcip profile 3
FCIP Profile 3
    Internet Address is 10.3.3.3  (interface GigabitEthernet2/3)
    Tunnels Using this Profile: fcip3
    Listen Port is 3225
    TCP parameters
        SACK is enabled
        PMTU discovery is enabled, reset timeout is 3600 sec
        Keep alive is 60 sec
        Minimum retransmission timeout is 200 ms
        Maximum number of re-transmissions is 4
        Send buffer size is 0 KB
        Maximum allowed bandwidth is 1000000 kbps
        Minimum available bandwidth is 500000 kbps
        Estimated round trip time is 1000 usec
        Congestion window monitoring is enabled, burst size is 10 KB
        Configured maximum jitter is 600 us
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.

Command	Description
show fcip profile	Displays FCIP profile information.

tcp max-retransmissions

To specify the maximum number of times a packet is retransmitted before TCP decides to close the connection, use the **tcp max-retransmissions** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp max-retransmissions *number*
no tcp max-retransmissions *number*

Syntax Description

number	Specifies the maximum number. The range is 1 to 8.

Command Default

Enabled.

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The default is 4 and the range is from 1 to 8 retransmissions.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
```

The following example specifies the maximum number of retransmissions :

```
switch(config-profile)# tcp max-retransmissions 6
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp min-retransmit-time

To control the minimum amount of time TCP waits before retransmitting, use the **tcp min-retransmit-time** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp min-retransmit-time *milliseconds*
no tcp min-retransmit-time *milliseconds*

Syntax Description

milliseconds	Specifies the time in milliseconds. The range is 200 to 5000.

Command Default

300 milliseconds.

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)#
```

The following example specifies the minimum TCP retransmit time for the TCP connection:

```
switch(config-profile)# tcp min-retransmit-time 500
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp pmtu-enable

To configure path MTU (PMTU) discovery, use the **tcp pmtu-enable** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp pmtu-enable [**reset-timeout** *seconds*]
no tcp pmtu-enable [**reset-timeout** *seconds*]

Syntax Description

reset-timeout *seconds*	(Optional) Specifies the PMTU reset timeout. The range is 60 to 3600 seconds.

Command Default

Enabled.

3600 seconds.

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)#
```

The following example disables PMTU discovery:

```
switch(config-profile)# no tcp pmtu-enable
```

The following example enables PMTU discovery with a default of 3600 seconds:

```
switch(config-profile)# tcp pmtu-enable
```

The following example specifies the PMTU reset timeout to 90 seconds:

```
switch(config-profile)# tcp pmtu-enable reset-timeout 90
```

The following example leaves the PMTU in an enabled state but changes the timeout to the default of 3600 seconds:

```
switch(config-profile)# no tcp pmtu-enable reset-timeout 600
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.

Command	Description
show fcip profile	Displays FCIP profile information.

tcp sack-enable

To enable selective acknowledgment (SACK) to overcome the limitations of multiple lost packets during a TCP transmission, use the **tcp sack-enable** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp sack-enable
no tcp sack-enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The receiving TCP sends back SACK advertisements to the sender. The sender can then retransmit only the missing data segments.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)#
```

The following example enables the SACK mechanism on the switch:

```
switch(config-profile)# tcp sack-enable
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp send-buffer-size

To define the required additional buffering beyond the normal send window size that TCP allows before flow-controlling the switch's egress path for the FCIP interface, use the **tcp send-buffer-size** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp send-buffer-size s *ize*
no tcp send-buffer-size *size*

Syntax Description

size	Specifies the buffer size in KB. The range is 0 to 8192.

Command Default

Enabled.

The default FCIP buffer size is 0 KB.

The default iSCSI buffer size is 4096 KB

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.3(4)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)#
```

The following example configure the advertised buffer size to 5000 KB:

```
switch(config-profile)# tcp send-buffer-size 5000
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp-connections

To configure the number of TCP connections for the FCIP interface, use the **tcp-connections** command. To revert to the default, use the no form of the command.

tcp-connections number
no tcp-connections number

Syntax Description

number	Enters the number of connections. Accepted values are 2 and 5 (For Cisco MDS 9250i Switch only).

Command Default

Two TCP connections.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.
6.2(5)	Added a value, 5 for the number of TCP connections.

Usage Guidelines

Access this command from the switch(config-if)# submode.

Use the **tcp-connections** option to specify the number of TCP connections contained in an FCIP link.

Set the TCP connections to 2 when:

- Both ends or peers of the FCIP tunnel are on Cisco MDS 9222i Switches or Cisco MDS 9000 18/4-Port Multiprotocol Services Modules (MSM) or Cisco MDS 9000 16-Port Storage Services Nodes (SSN).
- One end of the FCIP tunnel is on Cisco MDS 9222i switch, Cisco MDS 9000 18/4-Port Multiprotocol Services Module (MSM), or Cisco MDS 9000 16-Port Storage Services Node (SSN) and the other end is on Cisco MDS 9250i Switch.

Set the TCP connections to 5 when:

- Both ends of the FCIP tunnel are on Cisco MDS 9250i Switches.

Note When both ends of the FCIP tunnel are on Cisco MDS 9250i Switches, the TCP connections can be set to either 2 or 5, we recommend to set the TCP connections to 5 for higher bandwidth.

Examples

The following example configures the TCP connections:

```
switch# config terminal
switch(config)# interface fcip 50
switch(config-if)# tcp-connections 2
switch(config-if)# no tcp-connections 2
```

Related Commands

Command	Description
show interface fcip number	Displays an interface state and statistics.
show running-config interface fcip number	Displays an interface configuration for a specified FCIP interface.

telnet

To log in to a host that supports Telnet, use the **telnet** command in EXEC mode.

telnet {*hostnameip-address*} [*port*]

Syntax Description

hostname	Specifies a host name. Maximum length is 64 characters.
ip-address	Specifies an IP address.
port	(Optional) Specifies a port number. The range is 0 to 2147483647.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example establishes a Telnet session to the specified IP address:

```
switch# telnet 172.22.91.153
Trying 172.22.91.153...
Connected to 172.22.91.153.
Login:xxxxxxxx
Password:xxxxxxxxx
switch#
```

Related Commands

Command	Description
telnet server enable	Enables the Telnet server.

telnet server enable

To enable the Telnet server if you want to return to a Telnet connection from a secure SSH connection, use the **telnet server enable** command. To disable the Telnet server, use the no form of this command

telnet server enable
no telnet server enable

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example enables the Telnet server:

```
switch(config)# telnet server enable
updated
```

The following example disables the Telnet server:

```
switch(config)# no telnet server enable
updated
```

Related Commands

Command	Description
telnet	Logs in to a host that supports Telnet.

terminal alias

To display and define command aliases for a user session, use the **terminal alias** command. To remove the alias definition, use the **no** form of this command.

terminal alias [persist] [*alias-name alias-definition*]
no terminal alias [persist] [*alias-name alias-definition*]

Syntax Description

persist	(Optional) Makes the setting persistent for the current and future sessions for the current user.
alias-name	(Optional) Alias name.
alias-definition	(Optional) Alias definition.

Command Default

Displays the command aliases available to the user session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Aliases that you define with the **terminal alias** command are only available to the current user. Other users cannot use these command aliases. To create aliases that other users can access, use the **cli alias name** command.

The alias setting applies only to the current user session. Use the **persist** keyword to change the setting for the current and future session for the current user.

Examples

This example shows how to define a command alias only for the current user session:

```
switch# terminal alias shint show interface brief
```

This example shows how to define a command alias to persist across a session for the current user:

```
switch# terminal alias persist shver show version
```

This example shows how to display the command aliases available to the current user session:

```
switch# terminal alias
CLI alias commands
==================
shint  :show interface brief
------------------
alias  :show cli alias
```

This example shows how to remove a temporary command alias for the user session:

```
switch# no terminal alias shint
```

Related Commands

Command	Description
cli alias name	Defines a command alias name.

terminal ask-on-term

To enable all confirmation questions on the terminal, use the **terminal ask-on-term** command. To disable all confirmation questions, use the **no** form of this command.

terminal ask-on-term *term*
no terminal ask-on-term *term*

Syntax Description

term	Name of the session where you want to enable or disable the confirmation questions.

Command Default

All confirmation questions are enabled by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Confirmation questions are used in NX-OS to confirm actions that may cause traffic disruption. The **no terminal ask-on-term** command disables even the confirmation questions that are prompted during a reload operation.

Examples

This example shows how to enable all confirmation questions on terminal pts/0 only:

```
switch# terminal ask-on-term pts/0
```

This example shows how to disable all confirmation questions on terminal pts/0 only:

```
switch# no terminal ask-on-term pts/0
```

Related Commands

Command	Description
show users	Displays current user sessions and terminal names.
terminal dont-ask	Disables the terminal from asking you confirmation statements.

terminal color

To change the colors that are used when displaying the commands and outputs on the CLI for a user session, use the **terminal color** command. To revert to the default color, use the **no** form of this command.

terminal color [persist]
no terminal color [persist]

Syntax Description

persist	(Optional) Makes the setting persistent for the current and future sessions for the current user.

Command Default

All CLI prompts, commands, and command outputs display in colors that are defined by the terminal emulator.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The **terminal color** command changes the CLI colors as follows:

- Displays the command prompt in green if the previous command was successful.
- Displays the command prompt in red if an error occurred in the previous command.
- Displays the command in blue.
- Displays output in the default color that is defined by the terminal emulator.

The terminal color setting applies only to the current user session. Use the **persist** keyword to change the setting for the current and future session for the current user.

Examples

This example shows how to enable the terminal display colors for the current user session:

```
switch# terminal color
```

This example shows how to enable the terminal display colors for the current and future sessions for the current user:

```
switch# terminal color persist
```

This example shows how to revert to the default for the current user session:

```
switch# no terminal color
```

This example shows how to revert to the default for the current and future sessions for the current user:

```
switch# no terminal color persist
```

terminal deep-help

To enable the display of syntax of all possible options of a given command, use the **terminal deep-help** command. To disable detailed help, use the **no** form of this command.

terminal deep-help
no terminal deep-help

Command Default

Detailed help is disabled by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

To invoke detailed help for a command, enter the command followed by simultaneously pressing the **Alt** and the **?** keys (the **Alt** key is the **option** key on Mac).

Examples

This example shows the possible options of the zoneset command:

```
switch# terminal deep-help
switch# zoneset alt-?
: zoneset distribute vsan <i0>
: zoneset export vsan <i0>
: zoneset import interface <if0> vsan <i0>
```

terminal dont-ask

To disable confirmation prompts on the CLI, use the **terminal dont-ask** command. To revert to the default, use the **no** form of this command.

terminal dont-ask [persist]
no terminal dont-ask [persist]

Syntax Description

persist	(Optional) Makes the setting persistent for the current and future sessions for the current user.

Command Default

Confirmation prompts are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The terminal confirmation prompt setting applies only to the current user session. Use the **persist** keyword to change the setting for the current and future session for the current user.

Examples

This example shows how to disable the CLI confirmation prompts for the current user session:

```
switch# terminal dont-ask
```

This example shows how to disable the CLI confirmation prompts for the current and future sessions for the current user:

```
switch# terminal dont-ask persist
```

This example shows how to enable the terminal to ask confirmation statements:

```
switch# no terminal dont-ask
```

This example shows how to enable the CLI confirmation prompts for the current and future sessions for the current user:

```
switch# no terminal dont-ask persist
```

Related Commands

Command	Description
terminal ask-on-term	Enables all confirmation questions on the terminal.

terminal edit-mode vi

To enable VI style editing of CLI history commands, use the **terminal edit-mode** command. To revert to the default editing mode, use the **no** form of this command.

terminal edit-mode vi [persist]
no terminal edit-mode vi [persist]

Syntax Description

persist	(Optional) Makes the setting persistent for the current and future sessions for the current user.

Command Default

The command line edit mode is set to EMACS by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The following table provides information about the difference between EMACS and VI mode editing commands:

Command	EMACS	VI
Delete line backward	Ctrl-u	dd
Delete word	Ctrl-w	dw **Note** This command deletes a word when the cursor is placed at the beginning of the word.
Back character	Ctrl-b	h
Forward character	Ctrl-f	l
Beginning of line	Ctrl-a	0
End of line	Ctrl-e	$
Back one word	Esc, b	b
Forward one word	Esc, f	w
Delete character at the cursor	Ctrl-d	x
Replace character at the cursor	—	r

The edit mode setting applies only to the current user session. Use the **persist** keyword to change the setting for the current and future session for the current user.

Examples

This example shows how to change the edit mode for recalled commands to VI style for the current user session:

```
switch# terminal edit-mode vi
```

This example shows how to change the edit mode for recalled commands to VI style for the current and future session for the current user:

```
switch# terminal edit-mode vi persist
```

This example shows how to revert the edit mode for recalled command to EMACS style for the current user session:

```
switch# no terminal edit-mode vi
```

This example shows how to revert the edit mode for recalled command to EMACS style for the current and future sessions for the current user:

```
switch# no terminal edit-mode vi persist
```

terminal event-manager bypass

To bypass all EEM policies that use **event cli match** statements to trap specific CLI commands, use **terminal event-manager bypass** command. To revert, use the **terminal no event-manager bypass** command.

terminal event-manager bypass
terminal no event-manager bypass

Command Default

EEM policies that match CLI commands are effective.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command allows the user to run commands that may be blocked or redirected by EEM policies.

Examples

This example shows a simple event manger applet that matches a CLI command and how to the **terminal event-manager bypass** command allows the user to bypass the EEM policy completely.

```
switch# show running-config eem
event manager applet noClockDetail
event cli match "show clock detail"
action 10 syslog priority critical msg "blocking sh clock detail"
switch# show clock detail
% Command blocked by event manager policy
2019 Jan 1 12:33:44 switch %EEM_ACTION-2-CRIT: blocking sh clock detail
switch# terminal event-manager bypass
switch# show clock detail
Time source is NTP
12:33:55 CET Fri Jan 01 2019
summer-time configuration:
-------------------------
timezone name: CEST
Starts : 5 Sun Mar at 02:00 hours
Ends : 5 Sun Oct at 02:00 hours
Minute offset:
```

This example shows how to restore matching of CLI commands by EEM policies:

```
switch# no terminal event-manager bypass
```

Related Commands

Command	Description
show running-config eem	Displays EEM policy configurations.

terminal exec prompt timestamp

To configure printing timestamps before each CLI command is executed, use the **terminal exec prompt timestamp** command. To remove the configuration, use the **no** form of this command.

terminal exec prompt timestamp
no terminal exec prompt timestamp

Command Default

Timestamp is not shown in the command output.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This setting will automatically print CPU usage and timestamp information before each command is run. This can be helpful in debugging issues.

Examples

This example shows the extra information that is displayed when this command is enabled:

```
switch# terminal exec prompt timestamp
switch# show banner motd
CPU utilization for five seconds: 2%/0%; one minute: 2%; five minutes: 2%
Time source is NTP
12:38:11.777 CET Sun Jan 06 2019
User Access Verification
```

terminal history no-exec-in-config

To exclude EXEC commands from the command history in config mode, use the **terminal history no-exec-in-config** command. To revert to the default, use the **no** form of this command.

terminal history no-exec-in-config
no terminal history no-exec-in-config

Command Default

The CLI command history always includes EXEC commands in configuration mode.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

By default, the Cisco NX-OS CLI history recalls all commands from the current command mode and higher command modes. For example, if you are working in global configuration mode, the command recall keystroke shortcuts recall both EXEC mode and global configuration mode commands. Using the **terminal history no-exec-in-config** command, you can avoid recalling any higher mode commands when you are in a configuration mode.

terminal home

To move the cursor to the line 1 and column 1 of the screen without erasing the screen output, use the **terminal home** command.

terminal home

Command Default

The cursor stays at the current line.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

terminal length

To set the number of lines used by the screen output pager, use the **terminal length** command. To revert to the default number of lines, use the **no** form of this command.

terminal length *lines*
terminal no length

Syntax Description

lines	Number of lines to display. Range is from 0 to 512. Enter 0 to disable paging.

Command Default

If the terminal emulator does not specify a screen length, then the default length is set to 24 lines. Most modern terminals propagate their window length to the switch so that the switch will automatically page output to match the number of lines of the user's window.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If a command output exceeds the number of terminal lines, the session pauses after displaying the number of lines set in the terminal length. Press the space bar to display another screen of lines or press the **Enter** key to display another line. To return to the command prompt, press **Ctrl-C**.

The terminal length setting applies only to the current session.

Examples

This example shows how to set the number of lines of command output to display on the terminal before pausing:

```
switch# terminal length 28
```

This example shows how to revert to the default number of lines:

```
switch# terminal no length
```

Related Commands

Command	Description
show terminal	Displays the terminal session configuration.
terminal width	Sets the number of character columns for the current terminal session.

terminal monitor

To automatically display new syslog messages to the current session, use the **terminal monitor** command.

terminal monitor

Command Default

Logs are printed to the console session and no logs are printed to terminal sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command is helpful for monitoring of unexpected events during changes or debug messages during debugging. Be careful if this command is used for monitoring debugging as the session or system may be overloaded by the number of messages printed.

Related Commands

Command	Description
logging level	Configure different logging level for each facility.
show logging level	Displays the logging level of each syslog facility.

terminal output xml

To set the command output formatting to XML, use the **terminal output xml** command. To set the default output formatting, use the **no** form of this command.

terminal output xml [{**1.0***NX-OS-version*}]
no terminal output xml [{**1.0***NX-OS-version*}]

Syntax Description

1.0	(Optional) XML version 1.0.
NX-OS-version	(Optional) Specifies the XML version depending on the Cisco NX-OS version that is installed on your switch.

Command Default

Command outputs are in free form text for human consumption.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command is useful for scripts or other services that expect XML formatted output from CLI commands.

Examples

This example shows how to set the command output formatting to XML:

```
switch# terminal output xml
```

This example shows how to set the command output formatting to XML version 1.0:

```
switch# terminal output xml 1.0
```

This example shows how to set the command output formatting to XML version 8.1.1b:

```
switch# terminal output xml 8.1.1b
```

This example shows how to set the command output formatting to default:

```
switch# no terminal output xml
```

Related Commands

Command	Description
show terminal output xml version	Displays currently used XML version.

terminal password

To assign a password to be used in the **copy** {**ftp** | **scp** | **sftp**} commands, use the **terminal password** command. To remove the password, use the **no** form of this command.

terminal password
no terminal password

Command Default

There is no password set for the **copy** {**ftp** | **scp** | **sftp**} commands.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The password that is configured by this command is not restricted to the current username. It will be used for the user specified in any **copy** command, which allows another user other than the current user to be given.

This command has two modes: inline and interactive. In the inline mode, the password is echoed on the screen. In the interactive mode, the password is not echoed. To use interactive mode, type the help character *?* instead of a password. When prompted, enter the desired password.

This command is not stored in the switch configuration and is not persistent between logins.

Examples

This example shows how to configure a password in inline mode:

```
switch# terminal password myScpFtpPassword
```

This example shows how to configure a password to be used in the **copy** {**scp** | **ftp** | **sftp**} commands:

```
switch# terminal password?
enter password and type return
```

This example shows how to remove the password that is configured for the **copy** {**scp** | **ftp** | **sftp**} commands:

```
switch# no terminal password
```

Related Commands

Command	Description
copy	Copy a file.

terminal redirection-mode

To configure the file format of the **show** command output that is redirected to a file, use the **terminal redirection-mode** command.

terminal redirection-mode {**ascii**|**zipped**}

Syntax Description

ascii	Sets the redirection mode to ASCII.
zipped	Sets the redirection mode to gzip.

Command Default

The file format of redirected the **show** command output is set to ASCII by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Some of the **show** commands have lengthy outputs, especially **show** commands for debugging such as the **show tech-support** command. You can use the **terminal redirection-mode** command to reduce the size of the file when you redirect the output from the command.

The terminal redirection mode setting applies only to the current session.

Examples

This example shows how automatic zipping of redirected output works. The mode is set to zip, a file is created and then unzipped. The size of each file is checked.

```
switch# terminal redirection-mode zipped
switch# show tech-support acl > shTechAcl.gz
switch# dir shTechAcl.gz
16346 Jan 01 12:34:56 2010 shTechAcl.gz
switch# gunzip shTechAcl.gz
switch# dir shTechAcl
236449 Jan 01 12:34:56 2010 shTechAcl
```

This example shows how to configure ASCII format for the terminal redirection mode:

```
switch# terminal redirection-mode ascii
```

terminal session-timeout

To set the terminal inactivity timeout period for the current session, use the **terminal session-timeout** command.

terminal session-timeout *minutes*

Syntax Description

minutes	Session timeout period in minutes. Range is 0 to 525600.

Command Default

Session timeout is disabled by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

A value of 0 minutes disables the session timeout.

The terminal session inactivity timeout setting applies only to the current session.

Examples

This example shows how to configure the terminal session timeout period to 1 minute:

```
switch# terminal session-timeout 1
```

This example shows how to disable the terminal session timeout:

```
switch# terminal session-timeout 0
```

Related Commands

Command	Description
show terminal	Displays the terminal session configuration.

terminal sticky-mode

To search for a command match in the current mode only, use the **terminal sticky-mode** command.

terminal sticky-mode
terminal no sticky-mode

Command Default

The current mode and all higher modes are searched for matching commands.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Examples

This example shows how commands are constrained to the current mode when this setting is enabled:

```
switch# configure
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# show clock?
*** No matching command found in current mode, matching in (exec) mode ***
  clock  Display current Date
switch(config)# exit
switch# terminal sticky-mode
switch# configure
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# show clock?
 ^
% Invalid command at '^' marker.
```

terminal terminal-type

To set the terminal type, use the **terminal terminal-type** command. To revert to the default type, use the **no** form of this command.

terminal terminal-type *type*
terminal no terminal-type

Syntax Description

type	Sets the terminal type. Maximum length is 80 characters. The supported types are: • ansi • dumb • linux • rxvt • screen • sun • vt100 • vt102 • vt200 • vt220 • vt52 • xterm • xterm-256color • xterm-color • xterm-xfree86

Command Default

The default terminal type is ansi.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Examples

This example shows how to set the terminal type to *xterm* :

```
switch# terminal terminal-type xterm
```

This example shows how to revert to the default terminal type:

```
switch# terminal no terminal-type
```

Related Commands

Command	Description
show terminal	Displays the terminal session configuration.

terminal time

To save the current time to a variable, use the **terminal time** command.

terminal time [*variable*] **[delta]**

Syntax Description

variable	(Optional) Variable name to store the time.
delta	(Optional) Displays the delta time to the currently saved time value.

Command Default

Current time is not saved.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Examples

This example shows how to save the current time to a variable:

```
switch# terminal time t1
```

This example shows how to display the delta time to the currently saved time:

```
switch# terminal time t1 delta
```

terminal verify-only

To verify if a user is permitted to run given commands, use the **terminal verify-only** command.

terminal verify-only [**username** *name*]
terminal no verify-only [**username** *name*]

Syntax Description

username	(Optional) Specifies a user.
name	(Optional) Specifies a username.

Command Default

Remote users are restricted from verifying commands.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

When configured, this command changes the CLI mode to verify if a given command is allowed to be executed but does not execute the command. The full command to be tested should be given. If a username is specified, the tests are for the specified user and not for the current user. Issue the **no** option to revert to normal command execution mode.

Examples

This example shows how to verify if the current user can execute the show clock command:

```
switch# terminal verify-only

switch# show clock
% Success
```

This example shows how to test which commands the user 'a123456' may execute:

```
switch# terminal verify-only username a123456
```

Related Commands

Command	Description
aaa authorization	Configures authorization.
show user-account	Displays information of switch users.

terminal width

To set the number of character columns for the current terminal session, use the **terminal width** command. To revert to the default, use the **no** form of this command.

terminal width *columns*
terminal no width

Syntax Description

columns	Number of columns. The range is from 24 to 511.

Command Default

If the terminal emulator does not specify a screen width, then the default number of character columns is 80. Most modern terminals propagate their window width to the switch so that the switch will automatically page output to match the width of the users window.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The terminal width setting applies only to the current session.

Examples

This example shows how to set the number of columns to display on the terminal:

```
switch# terminal width 70
```

This example shows how to revert to the default number of columns:

```
switch# terminal no width
```

Related Commands

Command	Description
show terminal	Displays the terminal session configuration.
terminal length	Sets the number of lines on a screen for the current terminal session.

test aaa authorization

To verify if the authorization settings are correct or not, use the test aaa authorization command.

test aaa authorization command-type {**commands**|**config-commands**} **user username command cmd**

Syntax Description

command-type	Specifies the command type. You can use the keywords for the command type.
commands	Specifies authorization for all commands.
config-commands	Specifies authorization for configuration commands.
user	Specifies the user to be authorized. The maximum size is 32.
username	Specifies the user to be authorized.
cmd	Specifies command to be authorized.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

```
The following example shows how to verify if the authorization setting s are correct or
not:
switch(config)# test aaa authorization command-type commands user u1 command "feature dhcp"
% Success
switch(config)#
```

Related Commands

Command	Description
show aaa authorization all	Displays all authorization information.

time

To configure the time for the command schedule, use the **time** command**.** To disable this feature, use the **no** form of the command.

time {**daily** *daily-schedule*|**monthly** *monthly-schedule*|**start** {*start-time*|**now**}|**weekly** *weekly-schedule*}
no time

Syntax Description

daily *daily-schedule*	Configures a daily command schedule. The format is *HH*:*MM*, where *HH* is hours (0 to 23) and *MM* is minutes (0 to 59). Maximum length is 5 characters.
monthly *monthly-schedule*	Configures a monthly command schedule. The format is *dm*:*HH*:*MM*, where *dow* is the day of the month (1 to 31), *HH* is hours (0 to 23) and *MM* is minutes (0 to 59). Maximum length is 8 characters.
start	Schedules a job to run at a future time.
start-time	Specifies the future time to run the job. The format is *yyyy*:*mmm*:*dd*:*HH*:*MM*, where *yyyy* is the year, *mmm* is the month (jan to dec), *dd* is the day of the month (1 to 31), *HH* is hours (0 to 23) and *MM* is minutes (0 to 59). Maximum length is 18 characters.
now	Starts the job two minutes after the command is entered.
weekly *weekly-schedule*	Configures a weekly command schedule. The format is *dow*:*HH*:*MM*, where *dow* is the day of the week (1 to 7, Sun to Sat), *HH* is hours (0 to 23) and *MM* is minutes (0 to 59). Maximum length is 10 characters.

Command Default

Disabled.

Command Modes

Scheduler job configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To use this command, the command scheduler must be enabled using the **scheduler enable** command.

Examples

The following example shows how to configure a command schedule job to run every Friday at 2200:

```
switch# config terminal
switch(config)# scheduler schedule name MySchedule
switch(config-schedule)# time weekly 6:22:00
```

The following example starts a command schedule job in two minutes and repeats every 24 hours:

```
switch(config-schedule)# time start now repeat 24:00
```

Related Commands

Command	Description
scheduler enable	Enables the command scheduler.
scheduler schedule name	Configures a schedule for the command scheduler.
show scheduler	Displays schedule information.

time-stamp

To enable FCIP time stamps on a frame, use the **time-stamp** command. To disable this command for the selected interface, use the no form of the command.

time-stamp [**acceptable-diff** *number*]
no time-stamp [**acceptable-diff** *number*]

Syntax Description

acceptable-diff *number*	(Optional) Configures the acceptable time difference for timestamps in milliseconds. The range is 500 to 10000.

Command Default

Disabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Access this command from the switch(config-if)# submode.

The **time-stamp** option instructs the switch to discard frames that are older than a specified time.

Examples

The following example enables the timestamp for an FCIP interface:

```
switch# config terminal
switch(config)# interface fcip 50
switch(config-if)# time-stamp
switch(config-if)# time-stamp acceptable-diff 4000
```

Related Commands

Command	Description
show interface fcip	Displays the configuration for a specified FCIP interface.

tlport alpa-cache

To manually configure entries in an ALPA cache, use the **tlport alpa-cache** command. To disable the entries in an ALPA cache, use the no form of the command.

tlport alpa-cache interface *interface* **pwwn** *pwwn* **alpa** *alpa*
no tlport alpa-cache interface *interface* **pwwn** *pwwn*

Syntax Description

interface *interface*	Specifies a Fibre Channel interface.
pwwn *pwwn*	Specifies the peer WWN ID for the ALPA cache entry.
alpa *alpa*	Specifies the ALPA cache to which this entry is to be added.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(5)	This command was introduced.

Usage Guidelines

Generally, ALPA cache entries are automatically populated when an ALPA is assigned to a device. Use this command only if you want to manually add additional entries.

Examples

The following example configures the specified pWWN as a new entry in this cache:

```
switch# config terminal
switch(config)# tlport alpa-cache interface fc1/2 pwwn 22:00:00:20:37:46:09:bd alpa 0x02
```

Related Commands

Command	Description
show tlport	Displays TL port information.

traceroute

To print the route an IP packet takes to a network host, use the traceroute command in EXEC mode.

traceroute [ipv6] [{**hostname** [**size** *packet-size*]|**ip-address**}]|[{**hostname**|**ip-address**}]

Syntax Description

ipv6	(Optional) Traces a route to an IPv6 destination.
hostname	(Optional) Specifies a host name. Maximum length is 64 characters.
size *packet-size*	(Optional) Specifies a packet size. The range is 0 to 64.
ip-address	(Optional) Specifies an IP address.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the **ipv6** argument.

Usage Guidelines

This command traces the route an IP packet follows to an Internet host by launching UDP probe packets with a small TTL (time to live) and then listening for an ICMP (Internet Control Message Protocol) "time exceeded" reply from a gateway.

Note Probes start with a TTL of one and increase by one until encountering an ICMP "port unreachable." This means that the host was accessed or a maximum flag was found. A line is printed showing the TTL, address of the gateway, and round-trip time of each probe. If the probe answers come from different gateways, the address of each responding system is printed.

Examples

The following example prints the route IP packets take to the network host www.cisco.com:

```
switch# traceroute www.cisco.com
traceroute to www.cisco.com (171.71.181.19), 30 hops max, 38 byte packets
 1  kingfisher1-92.cisco.com (172.22.92.2)  0.598 ms  0.470 ms  0.484 ms
 2  nubulab-gw1-bldg6.cisco.com (171.71.20.130)  0.698 ms  0.452 ms  0.481 ms
 3  172.24.109.185 (172.24.109.185)  0.478 ms  0.459 ms  0.484 ms
 4  sjc12-lab4-gw2.cisco.com (172.24.111.213)  0.529 ms  0.577 ms  0.480 ms
 5  sjc5-sbb4-gw1.cisco.com (171.71.241.174)  0.521 ms  0.495 ms  0.604 ms
 6  sjc12-dc2-gw2.cisco.com (171.71.241.230)  0.521 ms  0.614 ms  0.479 ms
 7  sjc12-dc2-cec-css1.cisco.com (171.71.181.5)  2.612 ms  2.093 ms  2.118 ms
 8  www.cisco.com (171.71.181.19)  2.496 ms *  2.135 ms
```

transceiver-frequency

To set the interface clock to ethernet or Fibre Channel, use the transceiver-frequency command in interface configuration mode. To disable the ethernet clock for the port, use the no form of the command.

transceiver-frequency [ethernet] force
no transceiver-frequency [ethernet] force

Syntax Description

ethernet	(Optional) Specifies the ethernet transceiver frequency for an interface.
force	Specifies the force option.

Command Default

Fibre Channel.

Command Modes

Interface Configuration mode.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to set the interface clock to ethernet or Fibre Channel:

```
switch(config-if)# transceiver-frequency ethernet force
switch(config-if)#
```

transfer-ready-size

To configure the target transfer ready size for SCSI write commands on a SAN tuner extension N port, use the **transfer-ready-size** command.

transfer-ready-size *bytes*

Syntax Description

bytes	Specifies the transfer ready size in bytes. The range is 0 to 2147483647.

Command Default

None.

Command Modes

SAN extension N port configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

For a SCSI write command-id command with a larger transfer size, the target performs multiple transfers based on the specified transfer size.

Examples

The following example configures the transfer ready size 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)# transfer-ready-size 512000
```

Related Commands

Command	Description
nport pwwn	Configures 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.

transport email

To configure the customer ID with the Call Home function, use the **transport email** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

transport email {**from** *email-address*|**reply-to** *email-address*|**smtp-server** *ip-address* [**port** *port-number*]}
no transport email {**from** *email-address*|**reply-to** *email-address*|**smtp-server** *ip-address* [**port** *port-number*]}

Syntax Description

from *email-address*	Specifies the from e-mail address. For example: SJ-9500-1@xyz.com. The maximum length is 255 characters.
reply-to *email-address*	Specifies the reply to e-mail address. For address, example: admin@xyz.com. The maximum length is 255 characters.
smtp-server *ip-address*	Specifies the SMTP server address, either DNS name or IP address. The maximum length is 255 characters.
port *port-number*	(Optional) Changes depending on the server location. The port usage defaults to 25 if no port number is specified.

Command Default

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures the from and reply-to e-mail addresses:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# transport email from user@company1.com
switch(config-callhome)# transport email reply-to person@place.com
```

The following example shows how to remove the callhome configuration for email smtp-server:

switch(config-callhome)# **transport email smtp-server none**

The following example configures the SMTP server and ports:

switch(config-callhome)# **transport email smtp-server**

```
switch(config-callhome)# transport email smtp-server 192.168.1.1
switch(config-callhome)# transport email smtp-server 192.168.1.1 port 30
```

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.

transport email mail-server

To configure an SMTP server address, use the transport email mail-server command. To disable this feature, use the no form of the command.

transport email mail-server {**ipv4**|**ipv6**|**hostname**} [**port** *port number*] [**priority** *priority number*]
no transport email mail-server {**ipv4**|**ipv6**|**hostname**} [**port** *port number*] [**priority** *priority number*]

Syntax Description

ipv4	Specifies IPV4 SMTP address.
ipv6	Specifies IPV6 SMTP address.
hostname	Specifies DNS or IPV4 or IPV6 address.
port port number	(Optional) Specifies SMTP server port. The range is from 1 to 65535.
priority priority number	(Optional) Specifies SMTP server priority. The range is from 1 to 100.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure an SMTP server port:

switch# callhome

```
switch(config-callhome)# transport email mail-server 192.168.10.23 port 4
switch# config t
```

The following example shows how to configure an SMTP server priority:

```
switch(config-callhome)# transport email mail-server 192.168.10.23 priority 60
switch# config t
```

Related Commands

Command	Description
callhome	Configures the Call Home function.

transport http proxy enable

To enable Smart Call Home to send all HTTP messages through the HTTP proxy server, use the transport http proxy enable command. To disable this feature, use the no form of the command.

transport http proxy enable
no transport http proxy enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Callhome Configuration mode.

Command History

Release	Modification
NX-OS 5.2(1)	This command was introduced.

Usage Guidelines

None.

Note You can execute this command only after the proxy server address has been configured.

Note The VRF used for transporting messages through the proxy server is the same as that configured using the transport http use-vrf command.

Examples

The following example shows how to enable Smart Call Home to send all HTTP messages through the HTTP proxy server:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.switch(config)# callhome
switch(config-callhome)# transport http proxy enable
Cannot enable proxy until configured
switch(config-callhome)#
```

Related Commands

Command	Description
callhome	Configures the Call Home function.

transport http proxy server

To configure proxy server address and port, use the transport http proxy server command. To disable this feature, use the no form of the command.

transport http proxy server *ip-address* [**port** *number*]
no transport http proxy server *ip-address* [**port** *number*]

Syntax Description

ip-address	HTTP Proxy server name or IP address (DNS name or IPv4 or IPv6 address)
port	(Optional) Specifies proxy server port.
number	(Optional) Port number. The range is from 1 to 65535.

Command Default

Default port number is 8080.

Command Modes

Callhome Configuration mode.

Command History

Release	Modification
NX-OS 5.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure proxy server address and port:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.switch(config)# callhome
switch(config-callhome)# transport http proxy server 192.0.2.1 port 2
switch(config-callhome)#
```

Related Commands

Command	Description
callhome	Configures the Call Home function.

trunk protocol enable

To configure the trunking protocol, use the **trunk protocol enable** command in configuration mode. To disable this feature, use the no form of the command.

trunk protocol enable
no trunk protocol enable

Syntax Description

Note Trunk protocol is enabled by default from Cisco MDS NX-OS Release 6.2(7) and later.

This command has no other arguments or keywords.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
6.2(7)	This command was deprecated.

Usage Guidelines

If the trunking protocol is disabled on a switch, no port on that switch can apply new trunk configurations. Existing trunk configurations are not affected—the TE port continues to function in trunking mode, but only supports traffic in VSANs that it negotiated previously (when the trunking protocol was enabled). Also, other switches that are directly connected to this switch are similarly affected on the connected interfaces. In some cases, you may need to merge traffic from different port VSANs across a non-trunking ISL. If so, you need to disable the trunking protocol.

Examples

The following example shows how to disable the trunk protocol feature:

```
switch# config terminal
switch(config)# no trunk protocol enable
```

The following example shows how to enable the trunk protocol feature:

```
switch(config)# trunk protocol enable
```

Related Commands

Command	Description
show trunk protocol	Displays the trunk protocol status.

trustedcert

To set the trustedcert, use the trustedcert command. To disable this feature, use the no form of the command.

trustedcert attribute-name *attribute-name* **search-filter** *string* **base-DN** *string*
no trustedcert attribute-name *attribute-name* **search-filter** *string* **base-DN** *string*

Syntax Description

attribute-name attribute-name	Specifies LDAP attribute name. The maximum size is 128 characters.
search-filter	Specifies LDAP search filter. The maximum length is 128 characters.
string	Specifies search map search filter . The maximum length is 128 characters.
base-DN	Configure base DN to be used for search operation. The Maximum length is 63 characters.
string	Specifies search map base DN name. The Maximum length is 63 characters.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

```
The following example shows how to specify the LDAP trustcert :
switch(config)#ldap search-map s1
switch(config-ldap-search-map)# trusted attribute-name cACertificate
"(&(objectClass=certificationAuthority))" base-DN "CN=NTAuthCertificates,CN=Public Key
Services,CN=Services,CN=Configuration,DC=DCBU-ACS"
GROUP_NAME: map1
CRL
ATTR_NAME: map1
SEARCH_FLTR: map1
BASE_DN: DN1
Sending the SET_REQ
switch(config-ldap-search-map)#end
```

Related Commands

Command	Description
show ldap-server groups	Displays the configured LDAP server groups.

tune

To configure the tune IOA parameters, use the tune command. To delete the tune IOA parameter, use the no form of the command.

tune {**lrtp-retx-timeout** *msec*|**round-trip-time** *ms*|**ta-buffer-size** *KB*|**timer load-balance** {**global**|**target** *seconds*|**rscn-suppression** *seconds*|**wa-buffer-size** *MB*|**wa-max-table-size** *KB*}}
no tune {**lrtp-retx-timeout** *msec*|**round-trip-time** *ms*|**ta-buffer-size** *KB*|**timer load-balance** {**global**|**target** *seconds*|**rscn-suppression** *seconds*|**wa-buffer-size** *MB*|**wa-max-table-size** *KB*}}

Syntax Description

lrtp-retx-timeout msec	Specifies LRTP retransmit timeout in milliseconds. The value can vary from 500 to 5000 msec. 2500 msec is the default.
round-trip-time ms	Specifies round-trip time in milliseconds. The value can vary from 1 to 100 ms. 15 ms is the default.
ta-buffer-size KB	Specifies tape acceleration buffer size in KB. The value can vary from 64 to 12288.
timer	Specifies tune IOA timers.
load-balance	Specifies IOA load-balance timers.
global seconds	Specifies global load-balancing timer value. The value can vary from 5 to 30 seconds. 5 seconds is the default.
target seconds	Specifies target load-balancing timer value. The value can vary from 2 to 30 seconds. 2 seconds is the default.
rscn-suppression seconds	Specifies IOA RSCN suppression timer value. The value can vary from 1 to 10 seconds. 5 seconds is the default.
wa-buffer-size MB	Specifies write acceleration buffer size in MB. The value can vary from 50 to 100 MB. 70 MB is the default.
wa-max-table-size KB	Specifies Write Max Table size in KB. The value can vary from 4 to 64 KB. 4 KB is the default.

Command Default

None.

Command Modes

Configuration submode.

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure a IOA RSCN suppression timer value:

```
switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ioa cluster tape_vault
switch(config-ioa-cl)# tune timer rscn-suppression 1
:switch(config-ioa-cl)#
```

The following example shows how to configure an IOA target load-balance timer value:

```
switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ioa cluster tape_vault
switch(config-ioa-cl)# tune timer load-balance target 2
switch(config-ioa-cl)#
```

The following example shows how to configure a global IOA target load-balance timer value:

```
switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ioa cluster tape_vault
switch(config-ioa-cl)# tune timer load-balance global 5
switch(config-ioa-cl)#
```

The following example shows how to configure the round-trip time in milliseconds:

```
switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ioa cluster tape_vault
switch(config-ioa-cl)# tune round-trip-time 15
switch(config-ioa-cl)#
```

The following example shows how to configure the tape acceleration buffer size in KB:

```
switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ioa cluster tape_vault
switch(config-ioa-cl)# tune ta-buffer-size 64
switch(config-ioa-cl)#
```

The following example shows how to configure the write acceleration buffer size in MB:

```
switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ioa cluster tape_vault
switch(config-ioa-cl)# tune wa-buffer-size 15
switch(config-ioa-cl)#
```

The following example shows how to configure the write Max Table Size in KB:

```
switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ioa cluster tape_vault
switch(config-ioa-cl)# tune wa-max-table-size 4
switch(config-ioa-cl)#
```

The following example shows how to configure the LRTP retransmit timeout in milliseconds:

```
switch# conf t
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ioa cluster tape_vault
```

switch(config-ioa-cl)# tune lrtp-retx-timeout 2500

switch(config-ioa-cl)#

Related Commands

Command	Description
flowgroup	Configures IOA flowgroup.

tune-timer

To tune the Cisco SME timers, use the tune-timer command. To disable this command, use the no form of the command.

tune-timer {**global_lb_timer global_lb_timer_value**|**rscn_suppression_timer rscn_suppresion_timer_value**|**tgt_lb_timer tgt_lb_timer_value**}
no tune-timer {**global_lb_timer global_lb_timer_value**|**rscn_suppression_timer rscn_suppresion_timer_value**|**tgt_lb_timer tgt_lb_timer_value**}

Syntax Description

global_lb_timer	Specifies the global load-balancing timer value.
global_lb_timer_value	Identifies the timer value. The range is from 5 to 30 seconds. The default value is 5 seconds.
rscn_suppression_timer	Specifies the Cisco SME Registered State Change Notification (RSCN) suppression timer value.
rscn_suppresion_timer_value	Identifies the timer value. The range is from 1 to 10 seconds. The default value is 5 seconds.
tgt_lb_timer	Specifies the target load-balancing timer value.
tgt_lb_timer_value	Identifies the timer value. The range is from 2 to 30 seconds. The default value is 2 seconds.

Command Default

None.

Command Modes

Cisco SME cluster configuration submode.

Command History

Release	Modification
3.3(1a)	This command was introduced.

Usage Guidelines

The tune-timer command is used to tune various Cisco SME timers such as the RSCN suppression, global load balancing and target load-balancing timers. These timers should be used only in large scaling setups. The timer values are synchronized throughout the cluster.

Examples

The following example configures a global load-balancing timer value:

```
switch# config t
switch(config))# sme cluster c1
switch(config-sme-cl)# tune-timer tgt_lb_timer 6
switch(config-sme-cl)#
```

The following example configures a Cisco SME RSCN suppression timer value:

```
switch# config t
switch(config))# sme cluster c1
```

```
switch(config-sme-cl)# tune-timer rscn_suppression_timer 2
switch(config-sme-cl)#
```

The following example configures a target load-balancing timer value:

```
switch# config t
switch(config))# sme cluster c1
switch(config-sme-cl)# tune-timer rscn_suppression_timer 2
switch(config-sme-cl)#
```

U Commands

undebug all

To disable all debugging, use the **undebug all** command.

undebug all

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use this command to turn off all debugging.

Examples

The following example shows how to disable all debugging on the switch:

```
switch# undebug all
```

Related Commands

Command	Description
no debug all	Also disables all **debug** commands configured on the switch.
show debug	Displays all debug commands configured on the switch.

update license

To update an existing license, use the **update license** command in EXEC mode.

update license {**url**|**bootflash:**|**slot0:**|**volatile:**} **new_license_file old_license_ file**

Syntax Description

update license	Updates an installed, expiring license.
url	Specifies the URL for the license file to be uninstalled.
bootflash:	Specifies the license file location in internal bootflash memory.
slot0:	Specifies the license file in the CompactFlash memory or PCMCIA card.
volatile:	Specifies the license file in the volatile file system.
new_license_file	Location or URL of the new license file.
old_license file	Location or URL of the old license file that needs to be updated.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(2)	This command was introduced.

Examples

The following example updates a specific license:

```
switch# update license bootflash:sanextn2.lic sanextn1.lic
Updating sanextn1.lic:
SERVER this_host ANY
VENDOR cisco
# An example fcports license
INCREMENT SAN_EXTN_OVER_IP cisco 1.000 permanent 1 HOSTID=VDH=ABCD \
        NOTICE=<LicFileID>san_extn1.lic</LicFileID><LicLineID>0</LicLineID> \
        SIGN=33088E76F668

with bootflash:/sanextn2.lic:
SERVER this_host ANY
VENDOR cisco
# An example fcports license
INCREMENT SAN_EXTN_OVER_IP cisco 1.000 permanent 1 HOSTID=VDH=ABCD \
        NOTICE=<LicFileID>san_extn2.lic</LicFileID><LicLineID>1</LicLineID> \
        SIGN=67CB2A8CCAC2

Do you want to continue? (y/n) y
Updating license ..done
```

use-profile

To bind a profile to the FCIP interface, use the **use-profile** option. To disable a configured profile, use the no form of the option.

use-profile *profile-id*
no use-profile *profile-id*

Syntax Description

profile-id	Specifies the profile ID to be used. The range is 1 to 255.

Command Default

None.

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.

This command binds the profile with the FCIP interface.

Examples

The following example shows how to bind a profile to the FCIP interface:

```
switch# config terminal
switch(config)# interface fcip 50
switch(config-if)# use-profile 100
switch(config-if)# no use-profile 100
```

Related Commands

Command	Description
show fcip	Displays information about the FCIP profile.
show interface fcip	Displays an interface configuration for a specified FCIP interface.

user-certdn-match

To set the certificate matching, use the user-certdn-match command. To disable this feature, use the no form of the command.

user-certdn-match attribute-name *attribute-name* **search-filter** *string* **base-DN** *string*
nouser-certdn-match attribute-name *attribute-name* **search-filter** *string* **base-DN** *string*

Syntax Description

attribute-name attribute-name	Specifies LDAP attribute name. The maximum size is 128 characters.
search-filter	Specifies LDAP search filter. The maximum length is 128 characters.
string	Specifies search map search filter . The maximum length is 128 characters.
base-DN	Configure base DN to be used for search operation. The Maximum length is 63 characters.
string	Specifies search map base DN name. The Maximum length is 63 characters.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

```
The following example shows how to set the certificate matching:
switch(config)#ldap search-map s1
switch(config-ldap-search-map)# user-certdn-match attribute-name map1 search-filter map1
base-DN a
switch(config-ldap-search-map)#
```

Related Commands

Command	Description
show ldap-server groups	Displays the configured LDAP server groups.

username

To define a user, use the **username** command in configuration mode. To undo the configuration or revert to factory defaults. Use the **no** form of a command

username *name* [{**expire date**|**Keypair** {**export uri** {**dsa**|**rsa**} **[force]**|**generate** {**dsa**|**rsa**} **[force]**}|**import bootflash : uri**|**volatile : uri** {**dsa**|**rsa**} **[force]** {**iscsi**|**password** [{**0**|**5**|**7**}] **user-password** [**expire date**] [**role rolename**]|**priv-lvl privilege-level**|**role rolename**|**ssh-cert-dn** *distinguished-name* {**dsa**|**rsa**}|**sshkey** {**key-content**|**file** *filename*}}}]
no username *name* [{**expire date**|**Keypair export bootflash : uri**|**volatile : uri** {**dsa**|**rsa**} **[force]**|**generate** {**dsa**|**rsa**} **[force]**|**import bootflash : uri**|**volatile : uri** {**dsa**|**rsa**} **[force] iscsi**|**password** [{**0**|**5**|**7**}] **user-password** [**expire date**] [**role rolename**]|**priv-lvl privilege-level**|**role rolename**|**ssh-cert-dn** *distinguished-name* {**dsa**|**rsa**}|**sshkey** {**key-content**|**file** *filename*}}]

Syntax Description

name	Specifies the name of the user. Maximum length is 32 characters.
expire date	(Optional) Specifies the date when this user account expires (in YYYY-MM-DD format).
Keypair	(Optional) Specifies SSH (Secure shell) user keys.
export uri	Exports keypairs to bootflash or remote directory.
dsa	Specifies DSA keys.
rsa	Specifies RSA keys.
force	(Optional) Specifies the generation of keys even if previous ones are present.
generate	Generates SSH key pairs.
import	Import keypair from bootflash or remote directory.
bootflash: uri	Specifies URI or alias of the bootflash or file system to export.
volatile: uri	Specifies URI or alias of the volatile or file system to import.
iscsi	(Optional) Identifies an iSCSI user.
password	(Optional) Configures a password for the user. The password is limited to 64 characters. The minimum length is 8 characters.
0	(Optional) Specifies a clear text password for the user.
5	(Optional) Specifies a strongly encrypted password for the user.
7	(Optional) Specifies an encrypted password for the user.
user-password	Enters the password. Maximum length is 32 characters.
role rolename	(Optional) Specifies the role name of the user. Maximum length is 32 characters.

priv-lvl privilege-level	(Optional) Specifies privilege level. The range is from 1 to 15 characters.
ssh-cert-dn *distinguished-name*	(Optional) Specifies the SSH X.509 certificate distinguished name. The maximum size is 512.
dsa	(Optional) Specifies the DSA algorithm.
rsa	(Optional) Specifies the RSA algorithm.
sshkey key_content	(Optional) Specifies the actual contents of the SSH public key in OPENSSH format.
file *filename*	(Optional) Specifies a file containing the SSH public key either in OPENSSH or IETF SECH or Public Key Certificate in PEM format.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	Added the keypair and Priv-lvl keyword to the syntax description.
1.0(2)	This command was introduced.
2.0(x)	• Removed the **update_snmpv3** option. • Added level **7** for passwords.
3.0(1)	Added the **ssh-cert-dn**, **dsa**, and **rsa** options.

Usage Guidelines

To change the SNMP password, a clear text CLI password is required. You must know the SNMPv3 password to change the password using the CLI.

The password specified in the username command is synchronized as the auth and priv passphrases for the SNMP user.

Deleting a user using either command results in the user being deleted for both SNMP and CLI.

User-role mapping changes are synchronized in SNMP and CLI.

The SSH X.509 certificate distinguished name (DN) is the distinguished name in the certificate. You need to extract the distinguished name from the certificate and specify the subject name as the argument to the **username** command.

The SSHkey is the public key that we use to authorize any remote machine to login to the switch without the need to enter the password. Basically its the passwordless authentication for the user who has that key. These keys are used by the SSH Server of the switch to authenticate a user.

The SSH keys will be used by the SSH client on the switch while doing an SSH/SCP to connect to the remote host from the switch. This keypair can be used to do a passwordless SSH/SCP from the switch to a remote server.

Examples

The following example shows how to configure the privilege level that the user need to assign:

```
switch(config)# username admin priv-lvl 13
switch(config)#
```

The following example shows how to generate SSH keys:

```
switch(config)# username admin keypair generate rsa force
generating rsa key(1024 bits).....
.generated rsa key
switch(config)#
```

The following example shows how to delete SSH keys:

```
switch(config)# no username admin keypair generate rsa force
generating rsa key(1024 bits).....
.generated rsa key
switch(config)#
```

The following example shows how to export a keypair to bootflash or to the volatile directory:

```
switch(config)# username admin keypair export bootflash:xyz rsa force
Enter Passphrase:
switchg(config)#
```

The user can configure the same set of SSH keypairs on different switches by copying the public and private keypair to that switch and importing them using the following commands.

The following example shows how to import keypair from bootflash or volatile directory:

```
switch(config)# username admin keypair import bootflash:xyz rsa force
Enter Passphrase:
switchg(config)#
```

The following example shows how to define a user:

```
switch(config)# username knuckles password testpw role bodega
switch(config)# do show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:knuckles
        this user account has no expiry date
        roles:bodega
```

The following example configures the name for a user to log in using iSCSI authentication:

```
switch(config)# username iscsi
```

The following example places you in the mode for the specified role (techdocs). The prompt indicates that you are now in the role configuration submode. This submode is now specific to the techdocs group.

```
switch(config)# username role name techdocs
switch(config-role)#
```

The following example deletes the role called techdocs:

```
switch(config)# no username role name techdocs
```

The following example assigns a description to the new role. The description is limited to one line and can contain spaces:

```
switch(config-role)# description Entire Tech. Docs. group
```

The following example resets the description for the Tech. Docs. group:

```
switch(config-role)# no description
```

The following example creates or updates the user account (usam) along with a password (abcd) that is set to expire on 2009-05-31:

```
switch(config)# username usam password abcd expire 2009-05-31
```

The following example creates or updates the user account (msam) along with a password (abcd) specified in clear text (indicated by 0):

```
switch(config)# username msam password 0 abcd role network-operator
```

The following example specifies an encrypted (specified by 5) password (!@*asdsfsdfjh!@df) for the user account (user1):

```
switch(config)# username user1 password 5!@*asdsfsdfjh!@df
```

The following example adds the specified user (usam) to the network-admin role:

```
switch(config)# username usam role network-admin
```

The following example deletes the specified user (usam) from the vsan-admin role:

```
switch(config)# no username usam role vsan-admin
```

The following example shows how to define a distinguished name on a switch for SSH certificate authentication:

```
switch# config t
switch(config)# username knuckles ssh-cert-dn /CN=excal-1.cisco.com rsa

switch(config)# do show user-account

user:admin
        this user account has no expiry date
        roles:network-admin
user:knuckles
        this user account has no expiry date
        roles:network-operator
        ssh cert DN : /CN=excal-1.cisco.com; Algo: x509v3-sign-rsa
```

The following example specifies the SSH X.509 certificate distinguished name and DSA algorithm for an existing user account (usam):

```
switch(config)# username usam ssh-cert-dn usam-dn dsa
```

The following example specifies the SSH X.509 certificate distinguished name and RSA algorithm for an existing user account:

```
switch(config)# username user1 ssh-cert-dn user1-dn rsa
```

The following example deletes the SSH X.509 certificate distinguished name for the user account:

```
switch(config)# no username admin ssh-cert-dnadmin-dn dsa
```

The following example identifies the contents of the SSH key for the specified user (usam):

```
switch(config)# username usam sshkey fsafsd2344234234ffgsdfg
```

The following example deletes the SSH key content identification for the user (usam):

```
switch(config)# no username usam sshkey fsafsd2344234234ffgsdfgffsdfsfsfssf
```

The following example updates the SNMPv3 password for the specified user (joe). The local CLI password and the SNMP password are updated. If user Joe does not exist, the command fails:

```
switch(config)# username joe password wxyz6789 update-snmpv3 abcd1234
```

Related Commands

Command	Description
role	Configures user roles.
show username	Displays username information.

username (iSCSI initiator configuration and iSLB initiator configuration)

To assign a username for iSCSI login authentication, use the **username** command in iSCSI initiator configuration submode. To assign a username for iSLB login authentication, use the **username** command in iSLB initiator configuration submode. To disable this feature, use the **no** form of the command.

username *username*
no username *username*

Syntax Description

username	Specifies the username for iSCSI or iSLB login authentication.

Command Default

None.

Command Modes

iSCSI initiator configuration submode.iSLB initiator configuration submode.

Command History

Release	Modification
1.3(2)	This command was introduced.
3.0(1)	Added iSLB initiator configuration submode.

Usage Guidelines

None.

Examples

The following example assigns the username for iSCSI login authentication of an iSCSI initiator:

```
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)# username iSCSIloginUsername
switch(config-iscsi-init)#
```

The following example assigns the username tester for iSLB login authentication of an iSLB initiator:

```
switch# config t
switch(config)# islb initiator ip-address 100.10.10.10
```

switch**(config-iscsi-islb-init)# username ?**

<WORD> Enter username <Max Size - 128>

switch**(config-iscsi-islb-init)# username tester**

The following example removes the username tester for an iSLB initiator:

```
switch (config-iscsi-islb-init)# no
 username tester
```

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 a configured iSCSI initiator.
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 configured iSLB initiator.
show islb initiator detail	Displays detailed iSLB initiator information.
show islb initiator summary	Displays iSLB initiator summary information.

userprofile

To set the userprifile, use the userprofile command. To disable this feature, use the no form of the command.

userprofile attribute-name *attribute-name* **search-filter** *string* **base-DN** *string*
no userprofile attribute-name *attribute-name* **search-filter** *string* **base-DN** *string*

Syntax Description

attribute-name attribute-name	Specifies LDAP attribute name. The maximum size is 128 characters.
search-filter string	Specifies search map search filter. The maximum length is 128 characters.
base-DN string	Specifies search map base-DN name. The maximum length is 128 characters.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

```
The following example shows how to set the pubkey matching :
switch(config)#ldap search-map s1
switch(config-ldap-search-map)# userprofile attribute-name map1 search-filter map1 base-DN
 a
```

Usage Guidelines

None.

Examples

```
The following example shows how to set the CRLLookup:---add the output
switch(config)# ldap search-map map1
switch(config-ldap-search-map)# crllook attribute-name map1 search-filter map1 b
ase-DN DN1
GROUP_NAME: map1
CRL
ATTR_NAME: map1
SEARCH_FLTR: map1
BASE_DN: DN1
Sending the SET_REQ
switch(config-ldap-search-map)#
switch(config-ldap-search-map)#end
```

Command	Description
show crypto ssh-auth-map	displays mapping filters applied for SSH authentication.

user-pubkey-match

To set the user-pubkey matching, use the user-pubkey-match command. To disable this feature, use the no form of the command.

user-pubkey-match attribute-name *attribute-name* **search-filter** *string* **base-DN** *string*
nouser-pubkey-match attribute-name *attribute-name* **search-filter** *string* **base-DN** *string*

Syntax Description

attribute-name attribute-name	Specifies LDAP attribute name. The maximum size is 128 characters.
search-filter	Specifies LDAP search filter. The maximum length is 128 characters.
string	Specifies search map search filter . The maximum length is 128 characters.
base-DN	Configure base DN to be used for search operation. The Maximum length is 63 characters.
string	Specifies search map base DN name. The Maximum length is 63 characters.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

```
The following example shows how to set the pubkey matching :
switch(config)#ldap search-map s1
switch(config-ldap-search-map)# user-pubkey-match attribute-name map1 search-filter map1
base-DN a
switch(config-ldap-search-map)#
```

Related Commands

Command	Description
show ldap-server groups	Displays the configured LDAP server groups.

user-switch-bind

To set the user-switch-bind, use the user-switch-bind command. To disable this feature, use the no form of the command.

user-switch-bind attribute-name *attribute-name* **search-filter** *string* **base-DN** *string*
nouser-switch-bind attribute-name *attribute-name* **search-filter** *string* **base-DN** *string*

Syntax Description

attribute-name attribute-name	Specifies LDAP attribute name. The maximum size is 128 characters.
search-filter	Specifies LDAP search filter. The maximum length is 128 characters.
string	Specifies search map search filter . The maximum length is 128 characters.
base-DN	Configure base DN to be used for search operation. The Maximum length is 63 characters.
string	Specifies search map base DN name. The Maximum length is 63 characters.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

```
The following example shows how to set the pubkey matching :
switch(config)#ldap search-map s1
switch(config-ldap-search-map)# user-switch-bind attribute-name a search-filter a base-DN
a
switch(config-ldap-search-map)#
```

Related Commands

Command	Description
show ldap-server groups	Displays the configured LDAP server groups.

V Commands

virtual-domain (SDV virtual device configuration submode)

To configure a persistent virtual domain, use the **virtual-domain** command in SDV virtual device configuration submode. To remove a persistent virtual domain, use the **no** form of the command.

virtual-domain *domain-name*
no virtual-domain *domain-name*

Syntax Description

domain-name	Specifies the persistent virtual domain. The range is 1 to 239 or 0x1 to 0xef.

Command Default

No virtual domains are configured by default.

Command Modes

SDV virtual device configuration submode.

Command History

Release	Modification
3.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure a persistent virtual domain:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# sdv virtual-device name sqa1 vsan 1
switch(config-sdv-virt-dev)# virtual-domain 1
```

Related Commands

Command	Description
sdv enable	Enables or disables SAN device virtualization.
show sdv statistics	Displays SAN device virtualization statistics.

virtual-fcid (SDV virtual device configuration submode)

To configure a persistent virtual FC ID, use the **virtual-fcid** command in SDV virtual device configuration submode. To remove a persistent virtual FC ID, use the the **no** form of the command.

virtual-fcid *fc-id*
no virtual-fcid *fc-id*

Syntax Description

fc-id	Specifies the persistent virtual FC ID. The format is *0xhhhhhh,* where *h* is a hexadecimal number.

Command Default

No virtual FC IDs are configured by default.

Command Modes

SDV virtual device configuration submode.

Command History

Release	Modification
3.1(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure a persistent virtual FC ID:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# sdv virtual-device name sqa1 vsan 1
switch(config-sdv-virt-dev)# virtual-fcid 0xd66e54
```

Related Commands

Command	Description
sdv enable	Enables or disables SAN device virtualization.
show sdv statistics	Displays SAN device virtualization statistics.

vrrp

To enable VRRP, use the vrrp command in configuration mode. Use the **no** form of the command to revert to the factory defaults or to negate a command.

vrrp *ipv4-vr-group-number* {**address** *ip-address* **[secondary]**|**advertisement-interval** *seconds*|**authentication** {**md5** *keyname* **spi** *index*|**text** *password*}|**preempt**|**priority** *value*|**shutdown**|**track** **interface** {**mgmt 0**|**vsan** *vsan-id*} **ipv6** *ipv6-vr-group-number* {**address** *ipv6-address*|**advertisement-interval** *centiseconds*|**preempt**|**priority** *value*|**shutdown**|**track** **interface** {**mgmt 0**|**vsan** *vsan-id*}}}
no vrrp *ipv4-vr-group-number* {**address** *ip-address* **[secondary]**|**advertisement-interval** *seconds*|**authentication** {**md5** *keyname* **spi** *index*|**text** *password*}|**preempt**|**priority** *value*|**shutdown**|**track** **interface** {**mgmt 0**|**vsan** *vsan-id*} **ipv6** *ipv6-vr-group-number* {**address** *ipv6-address*|**advertisement-interval** *centiseconds*|**preempt**|**priority** *value*|**shutdown**|**track** **interface** {**mgmt 0**|**vsan** *vsan-id*}}}

Syntax Description

ipv4-vr-group-number	Specifies an IPv4 virtual router group number. The range is 1 to 255.
address *ip-address*	Adds or removes an IP address to the virtual router.
secondary	(Optional) Configures a virtual IP address without an owner.
advertisement-interval *seconds*	Sets the time interval between advertisements. For IPv4, the range is 1 to 255 seconds.
authentication	Configures the authentication method.
md5 *keyname*	Sets the MD5 authentication key. Maximum length is 16 characters.
spi *index*	Sets the security parameter index. The range is 0x0 to 0xffffff.
text *password*	Sets an authentication password. Maximum length is 8 characters.
preempt	Enables preemption of lower priority master.
priority *value*	Configures the virtual router priority. The range is 1 to 254.
shutdown	Disables the VRRP configuration.
track	Tracks the availability of another interface.
interface fc *slot*/*port*	Adds a member using the Fibre Channel interface to a Cisco MDS 9000 Family switch.
mgmt 0	Specifies the management interface.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
ipv6 *ipv6-vr-group-number*	Specifies VRRP IPv6 on the interface. The range is 1 to 255.
address *ipv6-address*	Adds or removes an IPv6 address to the virtual router.

advertisement-interval *centiseconds*	Sets the time interval between advertisements. For IPv6, the range is 100 to 4095 centiseconds.

Command Default

Disabled.

Command Modes

Interface configuration mode.

Command History

Release	Modified
1.0(2)	This command was introduced.
3.0(1)	• Added the **IPv6** option. • Added the **address** and **advertisement-interval** options that are specific to IPv6.

Usage Guidelines

You enter the Virtual Router configuration submode to access the options for this command. From the VSAN or mgmt0 (management) interface configuration submode, enter **vrrp** *number* to enter the switch(config-if-vrrp)# prompt. By default, a virtual router is always disabled (**shutdown**). VRRP can be configured only if this state is disabled. Be sure to configure at least one IP address before attempting to enable a virtual router.

The total number of of VRRP groups that can be configured on a Gigabit Ethernet port, including main interfaces and subinterfaces, cannot exceed seven. This limitation applies to both IPv4 and IPv6 groups.

Note If you configure secondary VRRP IPv6 addresses on an IPFC VSAN interface, you must remove the secondary VRRP IPv6 addresses before downgrading to a release prior to Cisco Release 3.0(1). This is required only when you configure IPv6 addresses.

Examples

The following example enables VRRP configuration:

```
switch(config-if-vrrp)# no
 shutdown
```

The following example disables VRRP configuration:

```
switch(config-if-vrrp)# shutdown
```

The following example configures an IPv4 address for the selected VRRP:

```
switch# config terminal
switch(config)# interface vsan
1 switch(config-if)# vrrp 250

switch(config-if-vrrp)# address 10.0.0.10
```

Related Commands

Command	Description
clear vrrp	Clears all the software counters for the specified virtual router.
show vrrp	Displays VRRP configuration information.

vsan (iSCSI initiator configuration and iSLB initiator configuration)

To assign an iSCSI or iSLB initiator to a VSAN other than the default VSAN, use the **vsan** command in iSCSI initiator configuration submode or iSLB initiator configuration submode. To disable this feature, use the **no** form of the command.

vsan *vsan-id*
no vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN ID. The range 1 to 4093.

Command Default

None.

Command Modes

iSCSI initiator configuration submode.iSLB initiator configuration submode.

Command History

Release	Modification
1.3(2)	This command was introduced.
3.0(1)	Added iSLB initiator configuration submode.

Usage Guidelines

When you configure an iSLB initiator in a VSAN other than VSAN 1 (the default VSAN), the initiator is automatically removed from VSAN 1. For example, if you configure an iSLB initiator in VSAN 2 and you also want it to be present in VSAN 1, you must explicitly configure the initiator in VSAN 1.

Examples

The following example assigns an iSCSI initiator to a VSAN other than the default VSAN:

```
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)# vsan 40
switch(config-iscsi-init)#
```

The following example assigns an iSLB initiator to a VSAN other than the default VSAN:

```
switch# config t
switch(config)# islb initiator ip-address 100.10.10.10
```

ips-hac2(config-islb-init)# vsan ?

<1-4093> Enter VSAN

ips-hac2(config-islb-init)# vsan 10

The following example removes the iSLB initiator:

```
switch (config-islb-init)# no
 vsan 10
```

Related Commands

Command	Description
iscsi initiator name	Assigns an iSCSI name and changes to iSCSI initiator configuration submode.
show islb initiator	Displays iSLB initiator information.
show iscsi initiator	Displays information about a configured iSCSI initiator.
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 configured iSLB initiator.
show islb initiator detail	Displays detailed iSLB initiator information.
show islb initiator summary	Displays iSLB initiator summary information.

vsan database

To create multiple fabrics sharing the same physical infrastructure, assign ports to VSANs, turn on or off interop mode, load balance either per originator exchange or by source-destination ID, and in order to be able to define these VSANs and specify the various VSAN attributes, use the vsan database command in the vsan database submode.

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following examples show how to create multiple fabrics sharing the same physical infrastructure and how to assign ports to VSANs:

```
switch# config terminal
switch(config)# vsan database
switch(config-vsan-db)#
```

Related Commands

Command	Description
vsan wwn	Configures a WWN for a suspended VSAN that has interop mode 4 enabled.

vsan interface

To add the interfaces to a VSAN, use the **vsan interface** command. Use the **no** form of this command to delete a configured role.

vsan *vsan-id* **interface** {**fc** *slot/port*|**fcip** *fcip-id*|**fv** *slot/dpp-number/v-port*|**iscsi** *slot/port*|**port-channel** *portchannel-number.subinterface-number*}
no vsan *vsan-id* **interface** {**fc** *slot/port*|**fcip** *fcip-id*|**fv** *slot/dpp-number/v-port*|**iscsi** *slot/port*|**port-channel** *portchannel-number.subinterface-number*}

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
interface fc *slot*/*port*	(Optional) Specifies the Fibre Channel interface by slot and port number on a Cisco MDS 9000 Family switch.
interface bay port | **ext** port	(Optional) Specifies the Fibre Channel interface by port number 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.
fcip *fcip-id*	(Optional) Specifies the FCIP interface on a Cisco MDS 9000 Family switch.
fv *slot*/*dpp-number*/*fv-port*	Configures the virtual F port (FV port) interface in the specified slot along with the data path processor (DPP) number and the FV port number.
iscsi *slot*/*port*	(Optional) Configures the iSCSI interface in the specified slot/port on a Cisco MDS 9000 Family switch.
port-channel *portchannel-number***.** *subinterface-number*	Configures the PortChannel interface specified by the PortChannel number followed by a dot (.) indicator and the subinterface number.

Command Default

All interfaces are in VSAN 1 by default.

Command Modes

Configuration mode—vsan database submode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

You can configure a role so that it only allows commands to be performed for a selected set of VSANs. By default, the VSAN policy of a role is **permit**. In other words, the role can perform commands configured by the **rule** command in all VSANs. In order to selectively allow VSANs for a role, the VSAN policy needs to be set to **deny** and then the appropriate VSANs need to be permitted.

Examples

The following example show how to add the interfaces to a VSAN:

```
switch# config terminal
switch(config)# vsan database
switch(config-vsan-db)# vsan 2
switch(config-vsan-db)# vsan 2 interface fv2/8/2
switch(config-vsan-db)# vsan 2 interface iscsi 2/1
switch(config-vsan-db)# end
switch#
```

vsan interop

To specify the VSAN interoperability mode value, use the **vsan interop** command. Use the **no** form of this command to delete a configured role.

vsan vsan-id interop [*mode*] [**loadbalancing** {**src-dst-id**|**src-dst-ox-id**}]
no vsan vsan-id interop [*mode*] [**loadbalancing** {**src-dst-id**|**src-dst-ox-id**}]

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
interop	Turns on interoperability mode.
mode	Specifies the interop mode. The range is 1 to 4.
loadbalancing	Configures load-balancing scheme.
src-dst-id	Sets src-id/dst-id for load-balancing.
src-dst-ox-id	Sets ox-id/src-id/dst-id for load-balancing (default).

Command Default

interop mode none and src-dst-ox-id.

Command Modes

Configuration mode—vsan database submode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

You can configure a role so that it only allows commands to be performed for a selected set of VSANs. By default, the VSAN policy of a role is **permit**. In other words, the role can perform commands configured by the **rule** command in all VSANs. In order to selectively allow VSANs for a role, the VSAN policy needs to be set to **deny** and then the appropriate VSANs need to be permitted.

Examples

The following example shows how to specify the Interoperability mode value for Src-id/dst-id loadbalancing:

```
switch# config terminal
switch(config)# vsan database
switch(config-vsan-db)# vsan 2
switch(config-vsan-db)# vsan 1 interop 1 loadbalancing src-dst-id
vsan 1:interoperability mode 1 allowed domain list [97-127] does not include all
 assigned and configured domains or conflicts with existing allowed domain lists
switch(config-vsan-db)#
```

vsan loadbalancing

To configure the VSAN loadbalancing scheme, use the **vsan loadbalancing** command. Use the **no** form of this command to delete a configured role.

vsan vsan-id loadbalancing {**src-dst-id**|**src-dst-ox-id**}
no vsan vsan-id loadbalancing {**src-dst-id**|**src-dst-ox-id**}

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
loadbalancing	Configures load-balancing scheme.
src-dst-id	Sets src-id/dst-id for load-balancing.
src-dst-ox-id	Sets ox-id/src-id/dst-id for load-balancing (default).

Command Default

. src-dst-ox-id

Command Modes

Configuration mode—vsan database submode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

You can configure a role so that it only allows commands to be performed for a selected set of VSANs. By default, the VSAN policy of a role is **permit**. In other words, the role can perform commands configured by the **rule** command in all VSANs. In order to selectively allow VSANs for a role, the VSAN policy needs to be set to **deny** and then the appropriate VSANs need to be permitted.

Examples

The following example shows how to configure loadbalancing scheme for a Src-id/dst-id loadbalancing:

```
switch# config terminal
switch(config)# vsan database
switch(config-vsan-db)# vsan 2 loadbalancing src-dst-ox-id
switch(config-vsan-db)#
```

vsan name

To assign a name to a VSAN, use the **vsan name** command. Use the **no** form of this command to delete a configured role.

vsan *vsan-id* **name** *name* **interop** [*mode*] **loadbalancing** {*src-dst-idsrc-dst-ox-id*}
loadbalancing {*src-dst-idsrc-dst-ox-id*}
suspend [**interop** [*mode*] [**loadbalancing** {*src-dst-idsrc-dst-ox-id*}]]
no vsan *vsan-id* **name** *name* **interop** [*mode*] **loadbalancing** {*src-dst-idsrc-dst-ox-id*}
loadbalancing {*src-dst-idsrc-dst-ox-id*}
suspend [**interop** [*mode*] [**loadbalancing** {*src-dst-idsrc-dst-ox-id*}]]

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
name *name*	Assigns a name to the VSAN. Maximum length is 32 characters.
interop	Turns on interoperability mode.
mode	Specifies the interop mode. The range is 1 to 4.
loadbalancing	Configures load-balancing scheme.
src-dst-id	Sets src-id/dst-id for load-balancing.
src-dst-ox-id	Sets ox-id/src-id/dst-id for load-balancing (default).

Command Default

no name, no suspend, interop mode none and src-dst-ox-id.

Command Modes

Configuration mode—vsan database submode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

You can configure a role so that it only allows commands to be performed for a selected set of VSANs. By default, the VSAN policy of a role is **permit**. In other words, the role can perform commands configured by the **rule** command in all VSANs. In order to selectively allow VSANs for a role, the VSAN policy needs to be set to **deny** and then the appropriate VSANs need to be permitted.

Examples

The following example shows how to assign a name to a VSAN:

```
switch# config terminal
switch(config)# vsan database
switch(config-vsan-db)# vsan 2 name vname
switch(config-vsan-db)#
```

vsan policy deny

To configure a VSAN-based role, use the **vsan policy deny** command in configuration mode. Use the **no** form of this command to delete a configured role.

vsan policy deny permit vsan *vsan-id*
no vsan policy deny permit vsan *vsan-id*

Syntax Description

permit	Remove commands from the role.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

Permit.

Command Modes

Configuration mode—role name submode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

You can configure a role so that it only allows commands to be performed for a selected set of VSANs. By default, the VSAN policy of a role is **permit**. In other words, the role can perform commands configured by the **rule** command in all VSANs. In order to selectively allow VSANs for a role, the VSAN policy needs to be set to **deny** and then the appropriate VSANs need to be permitted.

Examples

The following example places you in sangroup role submode:

```
switch# config t
switch(config)# role name sangroup
switch(config-role)#
```

The following example changes the VSAN policy of this role to deny and places you in a submode where VSANs can be selectively permitted:

```
switch(config)# vsan policy deny
switch(config-role-vsan)
```

The following example deletes the configured VSAN role policy and reverts to the factory default (permit):

```
switch(config-role)# no vsan policy deny
```

The following example permits this role to perform the allowed commands for VSANs 10 through 30:

```
switch(config-role)# permit vsan 10-30
```

The following example removes the permission for this role to perform commands for VSAN 15 to 20:

```
switch(config-role-vsan)# no permit vsan 15-20
```

vsan suspend

To suspend a VSAN, use the **vsan suspend** command. Use the **no** form of this command to delete a configured role.

vsan vsan-id suspend [**interop [mode]** [**loadbalancing** {**src-dst-id**|**src-dst-ox-id**}] **src-dst-ox-id**]
no vsan vsan-id suspend [**interop [mode]** [**loadbalancing** {**src-dst-id**|**src-dst-ox-id**}] **src-dst-ox-id**]

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
suspend	Suspends the VSAN.
interop	Turns on interoperability mode.
mode	Specifies the interop mode. The range is 1 to 4.
loadbalancing	Configures load-balancing scheme.
src-dst-id	Sets src-id/dst-id for load-balancing.
src-dst-ox-id	Sets ox-id/src-id/dst-id for load-balancing (default).

Command Default

interop mode none and src-dst-ox-id..

Command Modes

Configuration mode—vsan database submode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

You can configure a role so that it only allows commands to be performed for a selected set of VSANs. By default, the VSAN policy of a role is **permit**. In other words, the role can perform commands configured by the **rule** command in all VSANs. In order to selectively allow VSANs for a role, the VSAN policy needs to be set to **deny** and then the appropriate VSANs need to be permitted.

Danger

vsan suspend command done on an active VSAN is a very invasive command that requires a lot of supervisor processing. The supervisor is responsible for logging each device out, deprogramming ACLs, removing FCNS entries, generating RSCNs, etc. Because of this, care should be taken when doing this when there are many devices logged into the switch in the VSAN. After suspending the VSAN a minimum of 5 minutes should elapse prior to doing an no vsan suspend to ensure that all of the prior processing has completed.

Examples

The following example shows how to suspend a VSAN and enable interop mode 4:

```
switch# config t
switch(config)# vsan database
switch(config-vsan-db)# vsan 100 suspend
```

```
switch(config-vsan-db)#
```

W Commands

write command-id

To configure a SCSI write command for a SAN tuner extension N port, use the **write command-id** command.

write command-id *cmd-id* **target** *pwwn* **transfer-size** *bytes* [**outstanding-ios** *value* [{**continuous**|**num-transactions** *number*}]]

Syntax Description

cmd-id	Specifies the command identifier. The range is 0 to 2147483647.
target *pwwn*	Specifies the target port WWN. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
transfer-size *bytes*	Specifies the transfer size in multiples of 512 bytes. The range is 512 to 8388608.
outstanding-ios *value*	(Optional) Specifies the number of outstanding I/Os. The range is 1 to 1024.
continuous	(Optional) Specifies that the command is performed continuously.
num-transactions *number*	(Optional) Specifies a number of transactions. The range is 1 to 2147483647.

Command Default

The default for outstanding I/Os is 1.

Command Modes

SAN extension N port configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

To stop a SCSI write command in progress, use the **stop** command.

Examples

The following example configures a continuous SCSI write command:

```
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)# write command-id 100 target 22:22:22:22:22:22:22:22 transfer-size
512000 outstanding-ios 2 continuous
```

Related Commands

Command	Description
nport pwwn	Configures a SAN extension tuner N port.
san-ext-tuner	Enables the SAN extension tuner feature.
show san-ext-tuner	Displays SAN extension tuner information.
stop	Cancels a SCSI command in progress on a SAN extension tuner N port.

write erase

To clear a startup configuration, enter the **write erase** command from the EXEC mode prompt.

write erase [{**boot**|**debug**}]

Syntax Description

boot	(Optional) Destroys boot configuration.
debug	(Optional) Clears the existing debug configuration.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Once this command is issued, the switch's startup configuration reverts to factory defaults. The running configuration is not affected. The **write erase** command erases the entire startup configuration with the exception of any configuration that affects the loader functionality.

The **write erase boot** command only erases the configuration that affects the loader functionality. The loader functionality configuration includes the boot variables and the mgmt0 IP configuration information (IP address, netmask, and default gateway).

Examples

The following example clears the existing startup configuration completely:

```
switch# write erase
```

The following example clears the loader functionality configuration:

```
switch# write erase boot
This command will erase the boot variables and the ip configuration of interface mgmt 0
```

write-accelerator

To enable write acceleration and tape acceleration for the FCIP interface, use the **write-accelerator** command **in configuration mode**. To disable this feature or revert to the default values, use the no form of the command.

write-accelerator [**tape-accelerator** [**flow-control-butter-size** *bytes*]]
no write-accelerator [**tape-accelerator** [**flow-control-butter-size**]]

Syntax Description

tape-accelerator	(Optional) Enables tape acceleration.
flow-control-butter-size *bytes*	(Optional) Specifies the flow control buffer size.

Command Default

Disabled.

The default flow control buffer size is 256 bytes.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(x)	Added **tape-accelerator** and flow-control-butter-size options.

Usage Guidelines

The write acceleration feature is disabled by default and must be enabled on both sides of the FCIP link. If it is only enabled on one side of the FCIP tunnel, then the tunnel will not initialize.

In Cisco MDS SAN-OS Release 3.x, the **write-accelerator** command enables read acceleration if both ends of an FCIP tunnel are running SAN-OS Release 3.x.

If one end of an FCIP tunnel is running SAN-OS Release 3.x, and the other end is running SAN-OS Release 2.x, the **write-accelerator** command enables write acceleration only.

Tip FCIP tape acceleration does not work if the FCIP port is part of a PortChannel or if there are multiple paths between the initiator and the target port. Such a configuration might cause SCSI discovery failure or broken write or read operations.

Examples

The following command enables write acceleration on the specified FCIP interface:

```
switch# config terminal
switch(config)# interface fcip 51
switch(config-if)# write-accelerator
```

The following command enables write acceleration and tape acceleration on the specified FCIP interface:

```
switch# config terminal
```

```
switch(config)# interface fcip 51
switch(config-if)# write-accelerator tape-accelerator
```

The following command disables tape acceleration on the specified FCIP interface:

```
switch# config terminal
switch(config)# interface fcip 51
switch(config-if)# no write-accelerator tape-acceleration
```

The following command disables both write acceleration and tape acceleration on the specified FCIP interface:

```
switch# config terminal
switch(config)# interface fcip 51
switch(config-if)# no write-accelerator
```

Related Commands

Command	Description
show interface fcip	Displays an interface configuration for a specified FCIP interface.

wwn oui

To add a new Organizationally Unique Identifier (OUI) to the OUI database, use the **wwn oui** command. To delete OUIs, use the **no** form of this command.

wwn oui *id*
no wwn oui {*id* | **all**}

Syntax Description

id	Specifies the OUI. The range is from 0x1 to 0xffffff.
all	Deletes all the user-defined OUIs.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
7.3(0)D1(1)	This command was introduced.

Usage Guidelines

OUIs identify WWNs as Cisco manufactured devices.

This command should be used when connecting another Cisco device to an MDS device when the MDS device does not recognize the other Cisco device as a Cisco device. The newly added device is usually not recognized when the NX-OS version on the MDS device is older than the other Cisco device. The other Cisco device can be another MDS device or it can be some other device such as a Cisco Nexus device.

The following example shows how to add an OUI to the OUI database:

```
switch# configure terminal
switch(config)# wwn oui 0x1000
```

The following example shows how to delete an OUI from the OUI database:

```
switch# configure terminal
switch(config)# no wwn oui 0x1000
```

Related Commands

Command	Description
show wwn oui	Displays all OUIs in the OUI database.
wwn secondary-mac	Allocates secondary MAC addresses.

wwn secondary-mac

To allocate secondary MAC addresses, use the **wwn secondary-mac** command.

www secondary-mac wwn-id range address-range

Syntax Description

wwn-id	The secondary MAC address with the format hh:hh:hh:hh:hh:hh:hh:hh.
range address-range	The range for the specified WWN. The only valid value is 64.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command cannot be undone.

Changes to the worldwide names are only performed as required. They should not be changed on a daily basis. These changes should be made by an administrator or individual who is completely familiar with switch operations.

Examples

The following example allocates a secondary range of MAC addresses:

```
switch(config)# wwnm secondary-mac 00:99:55:77:55:55 range 64
This command CANNOT be undone.
Please enter the BASE MAC ADDRESS again: 00:99:55:77:55:55
Please enter the mac address RANGE again: 64
From now on WWN allocation would be based on new MACs.
Are you sure? (yes/no) no
You entered: no. Secondary MAC NOT programmed
```

wwn vsan

To configure a WWN for a suspended VSAN that has interop mode 4 enabled, use the **wwn vsan** command in configuration mode. To discard the configuration, use the **no** form of the command.

wwn vsan *vsan-id* **vsan-wwn** *wwn*
no wwn vsan *vsan-id* **vsan-wwn** *wwn*

Syntax Description

vsan-id	Specifies the VSAN ID. The range is 1 to 4093.
vsan-wwn *wwn*	Specifies the WWN for the VSAN. The format is hh:hh:hh:hh:hh:hh:hh:hh.

Command Default

None.

Command Modes

Configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

This command can succeed only if the following conditions are satisfied:

- The VSAN must be suspended.
- The VSAN must have interop mode 4 enabled before you can specify the switch WWN for it.
- The switch WWN must be unique throughout the entire fabric.
- The configured switch WWN must have McData OUI [08:00:88].

Examples

The following example shows how to assign a WWN to a VSAN.

```
switch# config t
switch(config)# wwn vsan 100 vsan-wwn 20:64:08:00:88:0d:5f:81
WWN can be configured for vsan in suspended state only
switch(config)# vsan database
switch(config-vsan-db)# vsan 100 suspend
switch(config-vsan-db)# exit
switch(config)# wwn vsan 100 vsan-wwn 20:64:08:00:88:0d:5f:81
switch(config)#
```

Related Commands

Command	Description
vsan database	Creates multiple fabrics sharing the same physical infrastructure, assigns ports to a VSAN, turns on or off interop mode, and load balances either per originator exchange or source-destination ID.

Z Commands

zone broadcast enable vsan

To enable zone broadcast frames for a VSAN in basic zoning mode, use the **zone broadcast enable VSAN** command **in configuration mode.** To disable this feature, use the **no** form of the command.

zone broadcast enable vsan *vsan-id*
no zone broadcast enable vsan *vsan-id*

Syntax Description

vsan-id	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
5.x	This command was deprecated.
2.0(x)	This command was introduced.

Usage Guidelines

Broadcast frames are sent to all Nx ports. If any NL port attached to an FL port shares a broadcast zone with the source of the broadcast frame, then the frames are broadcast to all devices in the loop.

This command only applies to basic zoning mode.

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 zone configuration broadcasting over the fabric:

```
switch# config terminal
switch(config)# zone broadcast enable vsan 10
```

Related Commands

Command	Description
show zone	Displays zone information.

zone clone

To clone a zone name, use the **zone clone** command in configuration mode.

zone clone *origZone-Name cloneZone-Name* **vsan** *vsan-id*

Syntax Description

origZone-Name cloneZone-Name	Clones a zone attribute group from the current name to a new name. Maximum length of names is 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

Use the **no** form of the **zone name (configuration mode)** command to delete the zone name.

Examples

The following example creates a clone of the original zone group named origZone into the clone zone group cloneZone on VSAN 45:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# zone clone origZone cloneZone vsan 45
```

Related Commands

Command	Description
show zone	Displays zone information.

zone commit vsan

To commit zoning changes to a VSAN, use the **zone commit vsan** command in configuration mode. To negate the command, use the **no** form of the command.

zone commit vsan *vsan-id* **[force]**
no zone commit vsan *vsan-id* **[force]**

Syntax Description

vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
force	(Optional) Forces the commit.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1a)	This command was introduced.

Usage Guidelines

Use the **no** form of the **zone commit vsan command to clear a session lock on a switch where the lock originated**.

Examples

The following example commits zoning changes to VSAN 200:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# zone commit vsan 200
```

Related Commands

Command	Description
show zone	Displays zone information.

zone compact vsan

To compact a zone database in a VSAN, use the **zone compact vsan** command.

zone compact vsan *vsan-id*

Syntax Description

vsan-id	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Prior to Cisco MDS SAN-OS Release 3.0(1), only 2000 zones were supported per VSAN. Starting with SAN-OS Release 3.0(1), 8000 zones are supported.

If more than 2000 zones are added, then a configuration check is registered to indicate that downgrading to a previous release could cause you to lose the zones over the limit. To avoid the configuration check, you can delete the excess zones and compact the zone database for the VSAN. If there are 2000 zones or fewer after you delete excess zones, the compacting process reissues zone IDs and the configuration can be supported by previous versions.

If you want to downgrade, you should configure less than 2001 zones across all VSANs and then issue the **zone compact vsan** command on all VSANs.

If you attempt to merge VSANs, the merge will fail if more than 2000 zones are present in a VSAN and the neighboring VSAN cannot support more than 2000 zones.

Activation will fail if more than 2000 zones are present in the VSAN and all the switches in the fabric cannot support more than 2000 zones.

Examples

The following example shows how to compact a zone database in VSAN 1:

```
switch# config terminal
switch(oongif)# zone compact vsan 1
```

Related Commands

Command	Description
show zone	Displays zone information.
show zone analysis	Displays detailed analysis and statistical information about the zoning database.

zone confirm-commit enable

To enable the display of the pending-diff and subsequent confirmation of pending-diff on issuing a zone commit, use the **zone confirm-commit enable** command in configuration mode. To disable this feature command, use the **no** form of the command.

zone confirm-commit enable vsan *vsan-id*
no zone confirm-commit enable vsan *vsan-id*

Syntax Description

vsan	Enables the zone pending-diff display during commit for a VSAN.
vsan-id	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(9)	This command was introduced.

Usage Guidelines

This command is available only in enhanced mode.

If the zone confirm-commit command is enabled for a VSAN, on committing the pending database, the pending-diff is displayed on the console and the user is prompted for Yes or No. If the zone confirm-commit command is disabled, the pending-diff is not displayed and the user is not prompted for Yes or No.

Note If this feature is enabled, downgrade is blocked by a configuration check. To resume downgrade correctly, confirm-commit has to be disabled on all VSANs.

Examples

The following example shows how to enable the confirm messages during commit for a VSAN:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# zone confirm-commit enable vsan 1
switch(config)#
```

The following example shows how to disable the confirm messages during commit for a VSAN:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no zone confirm-commit enable vsan 1
switch(config)#
```

Related Commands

Command	Description
show running-config zone | inc confirm	Checks if the confirm-commit option is enabled for any VSAN.

zone convert smart-zoning

To configure smart zoning convert commands, use the **zone convert smart-zoning** command in configuration mode.

zone convert smart-zoning {**fcalias name** *fcalias-name* **vsan** *vsan-id*|**vsan** *vsan-id*|**zone name** *zone-name* **vsan** *vsan-id*|**zoneset name** *zoneset-name* **vsan** *vsan-id*}

Syntax Description

fcalias name	Specifies auto-convert commands for a fcalias.
fcalias-name	Specifies the fcalias name. The maximum size is 64 characters.
vsan	Specifies the auto convert commands for a VSAN.
vsan-id	Specifies the VSAN ID. The range is from 1 to 4093.
zone name	Specifies the auto convert commands for a given zone.
zone-name	Specifies the zone name. The maximum size is 64 characters.
zoneset name	Specifies the auto convert commands for a zoneset.
zoneset-name	Specifies the zoneset name. The maximum size is 64 characters.
vsan	Specifies the VSAN.
vsan-id	Specifies the VSAN ID. The range is from 1to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(7)	Changed the command output.
5.2(6)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to Specify the auto convert commands for a VSAN.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# zone convert smart-zoning vsan 1
smart-zoning auto_convert initiated. This operation can take few minutes. Please wait..
switch(config)#
```

Related Commands

Command	Description
show zone	Displays zone information.

zone convert zone

To convert the zone member type from one type to another, use the zone convert zone command in the configuration mode.

zone convert zoneset name source-member-type dest-member-type vsan vsan-id

Syntax Description

name	Displays the name of the zone or zoneset. All members of the specified zone or zoneset will be converted to the new type.
source-member-type	Displays the member type of the members that have to be converted. The values of the supported source member types include fWWN, pWWN, Device-Alias, FCID, Interface and Interface-Domain.
dest-member-type	Displays the member type of the destination member. The values of the supported destination member types include fWWN, pWWN, Device-Alias, FCID, Interface, and Interface-Domain.
vsan vsan-id	Displays the VSAN ID.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

To use this command, all members have to be logged in. The conversion will fail even if a single member conversion is not achieved.

Table 18: Conversion Matrix of the Member Types, on page 1856 describes the conversion matrix of the member types supported by this command.

Table 18: Conversion Matrix of the Member Types

Source Member Types	Supported Destination Member Types
fWWN	pWWN, FCID, Device-alias, Interface, Interface-Domain
Interface	pWWN, FCID, Device-alias, Interface, Interface-Domain
Interface-Domain	pWWN, FCID, Device-alias, Interface
pWWN	FCID, Device-Alias
FCID	pWWN, Device-Alias
Device-Alias	FCID, pWWN

Examples

The following example shows the zone member type conversion:

```
switch# show zoneset name zs1
zoneset name zs1 vsan 1
  zone name zone2 vsan 1
    fcid 0x0b04d3
    fcid 0x0b04cd
    fcid 0x0b04ce
    fcid 0x0b04d1
    fcid 0x0b04d2

  zone name zone1 vsan 1
    fcid 0x0b04d6
    fcid 0x0b04d9
switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# zone convert zoneset name zs1 fcid pwwn vsan 1
switch(config)# ex
switch# show zoneset name zs1
zoneset name zs1 vsan 1
  zone name zone2 vsan 1
    pwwn 22:00:00:0c:50:02:cf:56
    pwwn 22:00:00:0c:50:02:cf:72
    pwwn 22:00:00:0c:50:02:ca:b5
    pwwn 22:00:00:0c:50:02:cb:43
    pwwn 22:00:00:0c:50:02:cd:c0

  zone name zone1 vsan 1
    pwwn 22:00:00:0c:50:02:cb:0c
    pwwn 22:00:00:0c:50:02:c9:a2
```

Related Commands

Command	Description
show zone	Displays the zone information.
show zoneset	Displays the configured zone sets.

zone copy

To copy the active zone set to the full zone set, use the **zone copy** command in EXEC mode. Use the **no** form of the command to negate the command or revert to the factory defaults.

zone copy active-zoneset full-zoneset vsan *vsan-id*
zone copy vsan *vsan-id* **active-zoneset** {**bootflash : ftp : |full-zoneset|scp : |sftp : |tftp : |volatile :** }

Syntax Description

active-zoneset	Copies from the active zone set.
full-zoneset	Copies the active zone set to the full-zone set.
vsan *vsan-id*	Configures to copy active zone set on a VSAN to full zone set.The ID of the VSAN is from 1 to 4093.
bootflash:	Copies the active zone set to a location in the bootflash: directory.
ftp:	Copies the active zone set to a remote location using the FTP protocol.
scp:	Copies the active zone set to a remote location using the SCP protocol.
sftp:	Copies the active zone set to a remote location using the SFTP protocol.
slot0:	Copies the active zone set to a location in the slot0: directory.
tftp:	Copies the active zone set to a remote location using the TFTP protocol.
volatile:	Copies the active zone set to a location in the volatile: directory.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(1)	This command was modified.

Usage Guidelines

None.

Examples

The following example copies the active zone set to the full zone set:

```
switch# zone copy active-zoneset full-zoneset vsan 1
```

The following example copies the active zone set in VSAN 3 to a remote location using SCP:

```
switch# zone copy vsan 3 active-zoneset scp://guest@myserver/tmp/active_zoneset.txt
```

Related Commands

Command	Description
show zone	Displays zone information.

zone default-zone

To define whether a default zone (nodes not assigned a created zone) permits or denies access to all in the default zone, use the **zone default-zon**e command in configuration mode. Use the **no** form of the command to negate the command or revert to the factory defaults.

zone default-zone [permit] vsan *vsan-id*
no zone default-zone [permit] vsan *vsan-id*

Syntax Description

permit	(Optional) Permits access to all in the default zone.
vsan *vsan-id*	Sets default zoning behavior for the specified VSAN. The ID of the VSAN is from 1 to 4093.

Command Default

All default zones are permitted access.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Use the **zone default-zone permit vsan** command to define the operational values for the default zone in a VSAN. This command applies to existing VSANs; it has no effect on VSANs that have not yet been created.

Use the **system default zone default-zone permit** command to use the default values defined for the default zone for all VSANs. The default values are used when you initially create a VSAN and it becomes active.

Examples

The following example permits default zoning in VSAN 2:

```
switch# config terminal
switch(config)# zone default-zone permit vsan 2
```

Related Commands

Command	Description
show zone	Displays zone information.
system default zone default-zone permit	Configures default values for a zone.

zone gs

To change zone generic service permission for a given VSAN, use zone gs command. To set the value for zone generic service permission as none (deny) for a given VSAN, use the no form of the command.

zone gs {**read**|**read-write**} **vsan** *vsan-id*
no zone gs {**read**|**read-write**} **vsan** *vsan-id*

Syntax Description

read	Specifies the zone generic service permission as read only.
read-write	Specifies the zone generic service permission as read write.
vsan	Specifies the zone generic service permission as read only on a given VSAN.
vsan-id	Specifies VSAN ID. The range is from 1 to 4093.

Command Default

read-write.

Command Modes

Configuration mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

Zone generic service permission setting is used to control zoning operation through the GS (generic service) interface. The zone generic service permission can be read-only, read-write or none (deny). Modifying gs permission value as write only is not supported.

Examples

The following example shows how to configure zone generic service permission value as read only for a given VSAN:

```
switch# config terminal
switch(config)# zone gs read vsan 1
switch(config)#
```

The following example shows how to configure zone generic service permission value as read-write for a given VSAN:

```
switch# config terminal
switch(config)# zone gs read-write vsan1
switch(config)#
```

The following example shows how to configure zone generic service permission value as none(deny) for a given VSAN:

```
switch# config terminal
switch(config)# no zone gs read-write vsan 1
switch(config)#
```

Related Commands

Command	Description
show zone policy vsan	Displays the zone policy for a given VSAN.

zone merge-control restrict vsan

To restrict zone database merging, use the **zone merge-control restrict vsan** command **in configuration mode.** To disable this feature, use the **no** form of the command.

zone merge-control restrict vsan *vsan-id*
no zone merge-control restrict vsan *vsan-id*

Syntax Description

vsan-id	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

If merge control setting is restricted and the two databases are not identical, the ISLs between the switches are isolated.

Examples

The following example shows how to configure zone merge control:

```
switch# config terminal
switch(config)# zone merge-control restrict vsan 10
```

Related Commands

Command	Description
show zone	Displays zone information.

zone mode enhanced vsan

To enable enhanced zoning for a VSAN, use the **zone mode enhanced vsan** command **in configuration mode.** To disable this feature, use the **no** form of the command.

zone mode enhanced vsan *vsan-id*
no zone mode enhanced vsan *vsan-id*

Syntax Description

vsan-id	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

Before using the **zone mode enhanced vsan** command, verify that all switches in the fabric are capable of working in enhanced zoning mode. If one or more switches are not capable of working in enhanced zoning mode, then the request to enable enhanced zoning mode is rejected.

When the **zone mode enhanced vsan** command completes successfully, the software automatically starts a session, distributes the zoning database using the enhanced zoning data structures, applies the configuration changes, and sends a release change authorization (RCA) to all switches in the fabric. All switches in the fabric then enable enhanced zoning mode.

Examples

The following example shows how to enable enhanced zoning mode:

```
switch# config terminal
switch(config)# zone mode enhanced vsan 10
```

Related Commands

Command	Description
show zone	Displays zone information.

zone name (configuration mode)

To create a zone, use the **zone name** command **in configuration mode.** Use the **no** form of the command to negate the command or revert to the factory defaults.

zone name *zone-name* **vsan** *vsan-id* **attribute** {**broadcast**|**smart-zoning**|**qos priority** {**high**|**low**|**medium**}|**read-only**} **attribute-group** *group-name* **member** {**device-alias** *alias-name* [**lun** *lun-id*]|**domain-id** *domain-id* **port-number** *port-number*|**fcalias** *name*|**fcid** *fcid-value* [**lun** *lun-id*]|**fwwn** *fwwn-id*|**interface fc** *slot / port* [{**domain-id** *domain-id*|**swwn** *swwn-id*}]|**ip-address** *ip-address* [*subnet-mask*]|**pwwn** *pwwn-id* [**lun** *lun-id*]|**symbolic-nodename** *identifier* **member** {**device-alias** *alias-name* [**lun** *lun-id*]|**domain-id** *domain-id* **port-number** *port-number*|**fcalias** *name*|**fcid** *fcid-value* [**lun** *lun-id*]|**fwwn** *fwwn-id*|**interface fc** *slot / port* [{**domain-id** *domain-id*|**swwn** *swwn-id*}]|**ip-address** *ip-address* [*subnet-mask*]|**pwwn** *pwwn-id* [**lun** *lun-id*]|**symbolic-nodename** *identifier*}}
no zone name *zone-name* **vsan** *vsan-id* **attribute** {**broadcast**|**smart-zoning**|**qos priority** {**high**|**low**|**medium**}|**read-only**} **attribute-group** *group-name* **member** {**device-alias** *alias-name* [**lun** *lun-id*]|**domain-id** *domain-id* **port-number** *port-number*|**fcalias** *name*|**fcid** *fcid-value* [**lun** *lun-id*]|**fwwn** *fwwn-id*|**interface fc** *slot / port* [{**domain-id** *domain-id*|**swwn** *swwn-id*}]|**ip-address** *ip-address* [*subnet-mask*]|**pwwn** *pwwn-id* [**lun** *lun-id*]|**symbolic-nodename** *identifier* **member** {**device-alias** *alias-name* [**lun** *lun-id*]|**domain-id** *domain-id* **port-number** *port-number*|**fcalias** *name*|**fcid** *fcid-value* [**lun** *lun-id*]|**fwwn** *fwwn-id*|**interface fc** *slot / port* [{**domain-id** *domain-id*|**swwn** *swwn-id*}]|**ip-address** *ip-address* [*subnet-mask*]|**pwwn** *pwwn-id* [**lun** *lun-id*]|**symbolic-nodename** *identifier*}}
interface {**bay port**|**ext port**}

Syntax Description

zone-name	Specifies the name of the zone. Maximum length is 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
attribute	Sets zone attributes.
read-only	Sets read-only attribute for the zone (default is read-write).
broadcast	Sets broadcast attribute for the zone.
smart-zoning	Sets the smart zoning for the zone.
qos priority {**high** | **low** | **medium**	Sets QoS attribute for the zone (default is low).
attribute-group *group-name*	Configures an attribute group. Maximum length is 64 characters.
member	Adds a member to a zone.
device-alias *alias-name*	Adds a member using the device alias name.
lun *lun-id*	Specifies the LUN number in hexadecimal format.
domain-id *domain-id*	Adds a member using the domain ID.
port-number *port-number*	Adds a member using the port number of the domain ID portnumber association.
fcalias *name*	Adds a member using the fcalias name.

fcid fcid-id	Adds a member using the FCID member in the format *0***x***hhhhhh*.
fwwn fwwn-id	Adds a member using the fabric port WWN in the format *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
interface fc *slot*/*port*	Adds a member using the Fibre Channel interface to a Cisco MDS 9000 Family switch.
interface bay | ext port	Adds a member using the Fibre Channel interface to a Cisco Fabric Switch for HP c-Class BladeSystem or to a Cisco Fabric Switch for IBM BladeCenter . The range is 0 to 48.
swwn *swwn-id*	(Optional) Specifies the switch WWN in the format *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
ip-address ip-address	Adds a member using the IP address.
subnet-mask	(Optional) Specifies an optional subnet mask.
pwwn pwwn-id	Adds a member using the port WWN in the format *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*.
symbolic-nodename *identifier*	Adds a member using the symbolic node name in the form of a name or an IP address.

Command Default

Zone attribute is read-only.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
1.2(1)	Added the **attribute**, **interface**, and **lun** subcommands.
2.0(x)	• Added the **broadcast** and **qos priority** options to the **attribute** subcommand. • Added the **attribute-group** subcommand. • Added the **device-alias** *aliasname* [lun *lun-id*] option to the **member** subcommand.
3.1(2)	Added the **interface bay | ext** option to the **member** subcommand.
5.2(6)	Added the smart-zoning keyword to the syntax description.

Usage Guidelines

Zones are assigned to zone sets, zone sets are then activated from one switch and propagate across the fabric to all switches. Zones allow security by permitting and denying access between nodes (hosts and storage). **zone name** commands are issued from the configuration mode. Configure a zone for a VSAN from the config-zone submode.

Use the **show wwn switch** command to retrieve the sWWN. If you do not provide a sWWN, the software automatically uses the local sWWN.

Broadcast frames are sent to all Nx ports.

If any NL port attached to an FL port shares a broadcast zone with the source of the broadcast frame,

The frames then are broadcast to all devices in the loop.

Examples

The following example configures attributes for the specified zone (Zone1) based on the member type (pWWN, fabric pWWN, FCID, or FC alias) and value specified:

```
switch# config terminal
switch(config)# zone name Zone1 vsan 10
```

switch(config-zone)# **attribute broadcast**

switch(config-zone)# **attribute read-only**

The following example configures members for the specified zone (Zone2) based on the member type (pWWN, fabric pWWN, FCID, or FC alias) and value specified:

```
switch# config terminal
switch(config)# zone name Zone2 vsan 10
```

switch(config-zone)# **attribute broadcast**

switch(config-zone)# **attribute read-only**

pWWN example:

```
switch(config-zone)# member pwwn 10:00:00:23:45:67:89:ab
Fabric pWWN example:
switch(config-zone)# member fwwn 10:01:10:01:10:ab:cd:ef
FC ID example:
switch(config-zone)# member fcid 0xce00d1
FC alias example:
switch(config-zone)# member fcalias Payroll
Domain ID example:
switch(config-zone)# member domain-id 2 portnumber 23
FC alias example:
switch(config-zone)# member ipaddress 10.15.0.0 255.255.0.0
Local sWWN interface example:
switch(config-zone)# member interface fc 2/1
Remote sWWN interface example:
switch(config-zone)# member interface fc2/1 swwn 20:00:00:05:30:00:4a:de
Domain ID interface example:
switch(config-zone)# member interface fc2/1 domain-id 25
The following example shows how to remove the smart zoning configuration:
switch# config terminal
switch(config)# zone name Zone2 vsan 10
```

switch(config-zone)# no **attribute smart-zoning**

switch(config-zone)#

Related Commands

Command	Description
zone-attribute-group name	Configures zone attribute groups.
zone rename	Renames zones.

Command	Description
show zone	Displays zone information.

zone name (zone set configuration submode)

To configure a zone in a zone set, use the **zone name** command in zone set configuration submode. To delete the zone from the zone set, use the **no** form of the command.

zone name *zone-name*
no zone name *zone-name*

Syntax Description

zone-name	Specifies the name of the zone. Maximum length is 64 characters.

Command Default

None.

Command Modes

Zone set configuration mode.

Command History

Release	Modification
1.0(2)	This command was modified.

Usage Guidelines

None.

Examples

The following example configure a zone in a zone set:

```
switch# config terminal
switch(config)# zoneset name Sample vsan 1
switch(config-zoneset)# zone name MyZone
```

The following example deletes a zone from a zone set:

switch(config-zoneset)# **no zone name Zone2**

Related Commands

Command	Description
show zoneset	Displays zone set information.
zone name (configuration mode)	Configure zones.
zoneset	Configures zone set attributes.

zone rename

To rename a zone, use the **zone rename** command **in configuration mode.**

zone rename *current-name new-name* **vsan** *vsan-id*

Syntax Description

current-name	Specifies the current fcalias name. Maximum length is 64 characters.
new-name	Specifies the new fcalias name. Maximum length is 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to rename a zone:

```
switch# zone rename ZoneA ZoneB vsan 10
```

Related Commands

Command	Description
show zone	Displays zone information.
zone name	Creates and configures zones.

zone rscn address-format port

To configure switch to send the port-address format RSCN for zone configuration changes , use the zone rscn address-format port. To revert to the default settings, use the no form of the command.

zone rscn address-format port vsan *vsan-id*
no zone rscn address-format port vsan *vsan-id*

Syntax Description

vsan	Specifies the VSAN ID.
vsan-id	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the switches to the port-address format.

```
switch(config)# zone rscn address-format port vsan 10
switch#
```

Related Commands

Command	Description
show zone	Displays zone information.
zone name	Creates and configures zones.

zone smart-zoning enable

To enable the smart zoning feature, use the **zone smart-zoning enable** command. **To disbale this feature, use the no form of this command.**

zone smart-zoning enable vsan *vsan-id*
no zone smart-zoning enable vsan *vsan-id*

Syntax Description

vsan	Specifies the smart zoning feature on the given VSAN.
vsan-id	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
5.2(6)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable the smart zoning feature on the given VSAN:

```
switch# zone smart-zoning enable vsan 10
```

Related Commands

Command	Description
show zone	Displays the zone information.

zone-attribute-group clone

To clone a zone attribute group, use the **zone-attribute-group clone** command **in configuration mode.**

zone attribute clone *origAttGrp-Name cloneAttGrp-Name* **vsan** *vsan-id*

Syntax Description

origAttGrp-Name cloneAttGrp-Name	Clones a zone attribute group from the current name to a new name. Maximum length of names is 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

To remove the zone attribute group, use the **no** form of the **zone-attribute-group name** command.

Examples

The following example shows how to clone a zone attribute group with the original name origZoneAttGrp to a copy named cloneZoneAttGrp on VSAN 45:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# zone-attribute-group clone origZoneAttGrp cloneZoneAttGrp vsan 45
```

Related Commands

Command	Description
show zone-attribute-group	Displays zone attribute group information.

zone-attribute-group name

To create and configure a zone attribute group for enhanced zoning, use the **zone-attribute-group name** command **in configuration mode.** To remove the zone attribute group, use the **no** form of the command.

zone attribute group name *zone-name* **vsan** *vsan-id*
no zone attribute group name *zone-name* **vsan** *vsan-id*

Syntax Description

zone-name	Specifies the zone attribute name. Maximum length is 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

You can use this command to create a zone attribute group and to modify an existing zone attribute group.

Zone attribute groups are only supported for enhanced zoning. You can enable enhanced zoning using the **zone mode enhanced vsan** command.

Examples

The following example shows how to create a zone attribute group and enter attribute group configuration submode:

```
switch# config terminal
switch(config)# zone-attribute-group name admin-attributes vsan 10
switch(config-attribute-group)#
```

Related Commands

Command	Description
show zone-attribute-group	Displays zone attribute group information.
zone mode enhanced vsan	Enables enhanced zoning for a VSAN.

zone-attribute-group rename

To rename a zone attribute group, use the **zone-attribute-group rename** command **in configuration mode.**

zone attribute group rename *current-name new-name* **vsan** *vsan-id*

Syntax Description

current-name	Specifies the current zone attribute name. Maximum length is 64 characters.
new-name	Specifies the new zone attribute name. Maximum length is 64 characters.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to rename a zone attribute group:

```
switch# config terminal
switch(config)# zone-attribute-group rename Group1 Group2 vsan 10
```

Related Commands

Command	Description
show zone-attribute-group	Displays zone attribute group information.

zonename (iSLB initiator configuration)

To assign a zone name for the initiator, use the **zonename** command in iSLB initiator configuration submode. To remove the zone name for the initiator, use the **no** form of the command.

zonename *name*
no zonename *name*

Syntax Description

zonename *name*	Assigns the zone name for the initiator. The maximum size is 55.

Command Default

Automatically generated.

Command Modes

iSCSI initiator configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You can configure a zone name where the iSLB initiators and initiator targets are added. If you do not specify a zone name, the IPS manager creates one dynamically. iSLB zone sets have the following considerations:

- Auto-zoning of the initiator with the initiator targets is enabled by default.
- A zone set must be active for a VSAN for auto-zones to be created in that VSAN. The zoneset activate command creates auto-zones only if at least one other change has been made to the zone set.
- iSLB zone set activation might fail if another zone set activation is in process or if the zoning database is locked. Retry the iSLB zone set activation if a failure occurs. To avoid this problem, only perform only one zoning related operation (normal zones, IVR zones, or iSLB zones) at a time.
- If IVR and iSLB are enabled in the same fabric, at least one switch in the fabric must have both features enabled. Any zoning related configuration or activation operation (for normal zones, IVR zones, or iSLB zones) must be performed on this switch. Otherwise, traffic might be disrupted in the fabric.

Examples

The following example assigns the zone name for the iSLB initiator:

```
switch# config t
switch(config)# islb initiator ip-address 100.10.10.10
```

ips-hac2(config-iscsi-islb-init)# zonename ?

<WORD> Enter zone name <Max Size - 55>

ips-hac2(config-islb-init)# zonename testzone1

The following example removes the zone name and reverts to the default zone name for the iSLB initiator:

```
switch (config-islb-init)# no
 zonename testzone1
```

Related Commands

Command	Description
islb initiator	Assigns an iSLB name and IP address to the iSLB initiator and enters iSLB initiator configuration submode.
show islb initiator	Displays iSCSI server load balancing (iSLB) CFS information.
show islb initiator detail	Displays detailed iSLB initiator information.
show islb initiator summary	Displays iSLB initiator summary information.

zoneset (configuration mode)

To group zones under one zone set, use the **zoneset** command. To negate the command or revert to the factory defaults, use the **no** form of the command.

zoneset {**activate name** *zoneset-name* **vsan** *vsan-id* [**force**] |**clone** *zoneset-currentName zoneset-cloneName*|**distribute full vsan** *vsan-id*|**name** *zoneset-name* **vsan** *vsan-id*|**rename** *current-name new-name* **vsan** *vsan-id*}
no zoneset {**activate name** *zoneset-name* **vsan** *vsan-id*|**clone** *zoneset-currentName zoneset-cloneName*|**distribute full vsan** *vsan-id*|**name** *zoneset-name* **vsan** *vsan-id*|**rename** *current-name new-name* **vsan** *vsan-id*}

Syntax Description

activate	Activates a zone set
force	Forces to activate a new zone set even when the zone set overwrite control is activated.
clone *zoneset-currentName zoneset-cloneName*	Clones a zone set from the current name to a new name. Maximum length of names is 64 characters.
name *zoneset-name*	Specifies a name for a zone set. Maximum length is 64 characters.
distribute full vsan vsan-id	Enables zone set propagation. Activates a zone set on the specified VSAN. The range is 1 to 4093.
rename	Renames a zone set.
current-name	Specifies the current fcalias name.
new-name	Specifies the new fcalias name.

Command Default

None.

Command Modes

Configuration mode (config)

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0(x)	Added the **rename** option.
2.1(1a)	Added the **clone** option.
6.2(13)	Added the **force** option.

Usage Guidelines

Zones are activated by activating the parent zone set.

The **zoneset distribute full vsan** command distributes the operational values for the default zone to all zone sets in a VSAN. If you do not want to distribute the operation values, use the **system default zone distribute**

full command to distribute the default values. The default values are used when you initially create a VSAN and it becomes active.

The **zoneset distribute full vsan** command applies to existing VSANs; it has no effect on VSANs that have not yet been created.

Examples

The following example activates a zone set named gottons in VSAN 333:

```
switch# config terminal
switch(config)# zoneset activate name gottons vsan 333
Zoneset Activation initiated. check zone status
```

The following example clones a zone set named zSet1 into a new zoneset named zSetClone in VSAN 45:

```
switch(config)# zoneset ?
  activate    Activate a zoneset
  clone       Zoneset clone command
  distribute  Enable zoneset propagation
  name        Configure a zoneset
  rename      Zoneset rename command
switch(config)# zoneset clone ?
  <WORD>  Current zoneset name (Max Size - 64)
switch(config)# zoneset clone existing ?
  <WORD>  New zoneset name (Max Size - 64)
switch(config)# zoneset clone existing new ?
  vsan  Clone zoneset name on a vsan
switch(config)# zoneset clone existing new vsan ?
  <1-4093>  VSAN id
switch(config)# zoneset clone existing new vsan 1 ?
  <cr>  Carriage Return
switch(config)# zoneset clone existing zSet1 zSetClone vsan 45
```

The following example distributes the operational values for the default zone to all zone sets in VSAN 22:

```
switch(config)# zoneset distribute full vsan 22
```

Related Commands

Command	Description
show zoneset	Displays zone set information.
system default zone distribute full	Configures default values for distribution to a zone set
zoneset overwrite-control	Enabling this command for a VSAN causes the **zoneset activate** command to fail if the zone set name is different from the currently active zone set name and the **force** parameter is not specified. This can prevent an inadvertent zoneset activation.

zoneset (EXEC mode)

To merge zone set databases, use the **zoneset** command in EXEC mode.

zoneset {**distribute**|**export**|**import interface** {*fc slot-number*|*fcip interface-number*|*port-channel port-number*}} **vsan** *vsan-id*
import interface {**bay-ext** *port*|**port-channel** *port-number*}

Syntax Description

distribute	Distributes the full zone set in the fabric.
export	Exports the zone set database to the adjacent switch on the specified VSAN. The active zone set in this switch becomes the activated zone set of the merged SAN.
import	Imports the zone set database to the adjacent switch on the specified interface. The active zone set in the adjacent switch becomes the activated zone set of the merged SAN.
interface	Configures the interface.
fc slot-number	Configures a Fibre Channel interface for the specified slot number and port number on an MDS 9000 Family switch.
fcip *interface-number*	Selects the FCIP interface on an MDS 9000 Family switch to configure the specified interface from 1 to 255.
interface bay| ext *port*	(Optional) Configures a Fibre Channel interface for the specified port ona Cisco Fabric Switch for HP c-Class BladeSystem or on a Cisco Fabric Switch for IBM BladeCenter . The range is 0 to 48.
	Specifies PortChannel interface.
vsan *vsan-id* port-channel *port-number*	Merges the zone set database of a VSAN on the specified interface. The ID of the VSAN is from 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.3(2)	This command was introduced.
3.1(2)	Added the **interface bay| ext** option.

Usage Guidelines

You can also use the **zoneset import** and the **zoneset export** commands for a range of VSANs.

The **zoneset distribute vsan** *vsan-id* command is supported in **interop 2** and **interop 3** modes not in **interop 1** mode.

Note If a port is part of a PortChannel in the interface, you cannot import the zone set database of the port; therfore, you should import the zone set database of the PortChannel.

Examples

The following example imports the zone set database from the adjacent switch connected through the VSAN 2 interface:

```
switch# zoneset import interface fc1/3 vsan 2
```

The following example exports the zone set database to the adjacent switch connected through VSAN 5:

```
switch# zoneset export vsan 5
```

The following example distributes the zone set in VSAN 333:

```
switch# zoneset distribute vsan 333
Zoneset distribution initiated. check zone status
```

Related Commands

Command	Description
show zone status vsan	Displays the distribution status for the specified VSAN.
show zoneset	Displays zone set information.

zoneset overwrite-control vsan

Enabling the **zoneset overwrite-control** command for a VSAN causes the **zoneset activate** command to fail if the zone set name is different from the currently active zone set name, and the force parameter is not specified. This can prevent an inadvertent zoneset activation. To disable this feature, use the no form of this command.

zoneset overwrite-control vsan *id*

Syntax Description

vsan	Specifies a virtual storage area network (VSAN).
id	VSAN ID. The VSAN ID is in the range of 1 to 4093.

Command Default

This feature is disabled by default.

Command Modes

Configuration mode (config)

Command History

Release	Modification
6.2(13)	This command was introduced.

Usage Guidelines

The **zoneset overwrite-control vsan** *id* command can be enabled only in an enhanced zone mode. Even when the **zoneset overwrite-control vsan** *id* command is enabled, the user can override it and continue with the activation of a new zoneset using the **zoneset activate name** *name* **vsan** *id* **force** command.

Examples

The following example shows how to enable the activation overwrite control for a specified VSAN:

```
switch(config)# zoneset overwrite-control vsan 3
WARNING: This will enable Activation Overwrite control. Do you want to continue? (y/n) [n]
```

Related Commands

Command	Description
show zone status vsan *vsan-id*	Displays zone settings for a VSAN, including if overwrite control is enabled or disabled for the VSAN.
show zoneset	Displays zone set information.
zoneset (configuration mode)	Configures zoneset.