

C Commands

- callhome, on page 5
- callhome mft-put, on page 7
- callhome test, on page 8
- callhome test-keepalive, on page 9
- cd, on page 10
- cdp, on page 12
- certificate, on page 15
- cfs distribute, on page 16
- cfs ipv4 distribute, on page 17
- cfs ipv4 mcast-address, on page 19
- cfs ipv6 distribute, on page 21
- cfs ipv6 mcast-address, on page 23
- cfs region, on page 25
- cfs static-peers, on page 27
- channel mode active, on page 28
- channel-group, on page 29
- cimserver, on page 30
- cimserver clearcertificate, on page 32
- cimserver loglevel, on page 33
- class, on page 34
- clear accounting log, on page 36
- clear analytics, on page 37
- clear arp-cache, on page 39
- clear asic-cnt, on page 40
- clear callhome session, on page 42
- clear cdp, on page 43
- clear cores, on page 44
- clear counters (EXEC mode), on page 45
- clear counters (SAN extension N port configuration mode), on page 46
- clear counters interface, on page 47
- clear counters interface all, on page 48
- clear crypto ike domain ipsec sa, on page 49
- clear crypto sa domain ipsec, on page 50

- clear debug-logfile, on page 51
- clear device-alias, on page 52
- clear dpvm, on page 53
- clear dpvm merge statistics, on page 54
- clear fabric-binding statistics, on page 55
- clear fcanalyzer, on page 56
- clear fcflow stats, on page 57
- clear fcns statistics, on page 58
- clear fc-redirect config, on page 59
- clear fc-redirect decommission-switch, on page 60
- clear fcs statistics, on page 61
- clear fctimer session, on page 62
- clear ficon, on page 63
- clear fspf counters, on page 64
- clear install failure-reason, on page 65
- clear ip access-list counters, on page 66
- clear ips arp, on page 67
- clear ips stats, on page 68
- clear ips stats fabric interface, on page 69
- clear ipv6 access-list, on page 70
- clear ipv6 neighbors, on page 71
- clear islb session, on page 72
- clear ivr fcdomain database, on page 73
- clear ivr service-group database, on page 74
- clear ivr zone database, on page 75
- clear ldap-server statistics, on page 76
- clear license, on page 77
- clear line, on page 78
- clear lldp counters, on page 79
- clear logging, on page 80
- clear ntp, on page 82
- clear port-security, on page 83
- clear processes log, on page 84
- clear qos statistics, on page 85
- clear radius-server statistics, on page 86
- clear radius session, on page 87
- clear rlir, on page 88
- clear rmon alarms, on page 90
- clear rmon all-alarms, on page 91
- clear rmon hcalarms, on page 92
- clear rmon log, on page 93
- clear role session, on page 94
- clear rscn session vsan, on page 95
- clear rscn statistics, on page 96
- clear santap module, on page 97
- clear scheduler logfile, on page 98

- clear screen, on page 99
- clear scsi-flow statistics, on page 100
- clear sdv, on page 101
- clear snmp hostconfig, on page 102
- clear snmp counters, on page 103
- clear ssh hosts, on page 104
- clear ssm-nvram santap module, on page 105
- clear system reset-reason, on page 106
- clear tacacs+ session, on page 107
- clear tacacs-server statistics, on page 108
- clear tlport alpa-cache, on page 109
- clear user, on page 110
- clear vrrp, on page 111
- clear zone, on page 113
- clear zone smart-zoning, on page 115
- cli, on page 116
- cli alias name, on page 118
- cli var name (configuration), on page 120
- cli var name (EXEC), on page 121
- client-trustpoint, on page 122
- clis, on page 123
- clock, on page 124
- clock format, on page 126
- clock set, on page 127
- cloud discover, on page 128
- cloud discovery, on page 129
- cloud-discovery enable, on page 131
- cluster, on page 132
- code-page, on page 133
- commit, on page 135
- commit (DMM job configuration submode), on page 136
- configure terminal, on page 137
- contract-id, on page 138
- copy, on page 139
- copy licenses, on page 143
- copy startup-config running-config, on page 144
- copy ssm-nvram standby-sup, on page 145
- counter (port-group-monitor configuration mode), on page 146
- counter (port-monitor configuration mode), on page 148
- counter tx-slowport-count, on page 152
- counter tx-slowport-oper-delay, on page 154
- counter txwait, on page 156
- crllookup, on page 158
- crypto ca authenticate, on page 159
- crypto ca crl request, on page 161
- crypto ca enroll, on page 163

- crypto ca export, on page 165
- crypto ca import, on page 166
- crypto ca lookup, on page 168
- crypto ca remote ldap, on page 169
- crypto ca test verify, on page 170
- crypto ca trustpoint, on page 171
- crypto cert ssh-authorize, on page 173
- crypto certificatemap mapname, on page 174
- crypto global domain ipsec security-association lifetime, on page 175
- crypto ike domain ipsec, on page 176
- crypto ike domain ipsec rekey sa, on page 177
- crypto ike enable, on page 178
- crypto ipsec enable, on page 179
- crypto key generate rsa, on page 180
- crypto key zeroize rsa, on page 182
- crypto map domain ipsec (configuration mode), on page 183
- crypto map domain ipsec (interface configuration submode), on page 185
- crypto transform-set domain ipsec, on page 186
- customer-id, on page 188

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.

certificate

To use an SSL or TLS certificate, use the **certificate** command.

certificate *certificate_path host_name*

Syntax Description

certificate_path	Specifies the path to the Privacy Enhanced Mail (PEM) certificate file.
host_name	Host name associated with the PEM file.

Command Default

No certificate is used.

Command Modes

Telemetry configuration mode (config-telemetry)

Command History

Release	Modification
8.3(1)	This command was introduced.

Examples

This example shows how to install an SSL or TLS certificate:

```
switch# configure
switch(config)# telemetry
switch(config-telemetry)# certificate /bootflash/test.pem foo.test.google.fr
```

Related Commands

Command	Description
feature telemetry	Enables the SAN Telemetry Streaming feature.
telemetry	Enters SAN Telemetry Streaming configuration mode.

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 analytics

To reset flow metrics for a view instance, use the **clear analytics** command.

clear analytics query *"query_string"*

Syntax Description

query *"query_string"*	Query syntax.

Command Default

None.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.3(1)	This command was modified. Added the **query** keyword. This command has changed from **clear analytics** *"query_string"* to **clear analytics query** *"query_string"*.
8.2(1)	This command was introduced.

Usage Guidelines

Note

- The *"query_string"* must have the format *"select all from <view-name>"*.
- You can clear the flow metrics without installing a push query.

Clear resets metrics of a view instance, whereas purge deletes specific view instance and its associated flow metrics momentarily. After clearing the database, the database will continue to collect flow metrics for the specified *"query_string"*. When you clear metrics of a view instance, the values of the metrics are reset to default. The *"query_string"* is a query syntax where you can specify query semantics such as **select**, **table**, **limit**, and so on. For example, "select all from fc-scsi.port." For more information, see the "Cisco MDS 9000 Series NX-OS SAN Analytics and Telemetry Configuration Guide."

Using a combination of sort and limit in the *"query_string"* allows you to display the first record or the last record of the flow metrics that is used for sorting. This data is useful in determining the port that has the most IO transactions, port that is using the least read and write IO bandwidth, and so on.

Examples

These examples show how to clear flow metrics:

1. This example shows an output before clearing the flow metrics:

```
switch# show analytics query 'select port,initiator_id, target_id,lun,
total_read_io_count,total_write_io_count,read_io_rate,
write_io_rate from fc-scsi.scsi_initiator_itl_flow where initiator_id=0xe80001'
{ "values": {
        "1": {
                "port": "fc1/8",
```

```
                "initiator_id": "0xe80001",
                "target_id": "0xe800a1",
                "lun": "0000-0000-0000-0000",
                "total_read_io_count": "0",
                "total_write_io_count": "1139010960",
                "read_io_rate": "0",
                "write_io_rate": "7071",
                "sampling_start_time": "1528535447",
                "sampling_end_time": "1528697495"
        }
}}
```

2. This example shows how to clear the flow metrics of an initiator ITL flow view type:

```
switch# clear analytics query 'select port,initiator_id,
target_id,lun,total_read_io_count,total_write_io_count,read_io_rate,
write_io_rate from fc-scsi.scsi_initiator_itl_flow where initiator_id=0xe80001'
```

3. This example shows an output after clearing the flow metrics:

```
switch# show analytics query 'select port,initiator_id, target_id,lun,
total_read_io_count,total_write_io_count,read_io_rate, write_io_rate from
fc-scsi.scsi_initiator_itl_flow where initiator_id=0xe80001'
{ "values": {
        "1": {
                "port": "fc1/8",
                "initiator_id": "0xe80001",
                "target_id": "0xe800a1",
                "lun": "0000-0000-0000-0000",
                "total_read_io_count": "0",
                "total_write_io_count": "0",
                "read_io_rate": "0",
                "write_io_rate": "0",
                "sampling_start_time": "0",
                "sampling_end_time": "0"
        }
}}
```

Related Commands

Command	Description
analytics query	Installs a push analytics query.
feature analytics	Enables the SAN Analytics feature on a switch.
purge analytics	Deletes a view instance and its associated flow metrics.
show analytics port-sampling	Displays the SAN analytics port sampling information.
show analytics query	Displays the SAN analytics query information.
show analytics type	Displays the SAN analytics type.
ShowAnalytics	Displays the SAN analytics information in a tabular format.

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

clear counters [**interface** *interface* | **snmp**]

Syntax Description

interface	Specifies the interface.
snmp	Clear SNMP interface counters.

Command Default

This command by default clears counters all interfaces.

Command Modes

Exec 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 counters for the interface fc2/9:

```
switch(config)# clear counters interface fc2/9
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. After clearing the security associations for IPsec, ensure that you wait for at least 10 seconds before you run the **system switchover** 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 terminates 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 ldap-server statistics

clear ldap-server statistics *hostname*

clear	Reset functions
ldap-server	Clear LDAP related parameters
statistics	Clear LDAP statistics
hostname	DNS name or IP address

Command Default None

Command Modes /exec

Command History

Release	Modification

Usage Guidelines None

Example

Table 1: Related Commands

Command Syntax	Description

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 lldp counters

Use the **clear lldp counters**command to clear the LLDP statistics.

clear lldp { **counters** | **interface** *interface* }

clear	Reset functions
lldp	Reset the lldp counters
counters	Reset the lldp traffic counters to zero
interface	Clear lldp traffic counters for each interface
interface	Enter interface

Command Default

None

Command Modes

EXEC mode.

Command History

Release	Modification
8.5(1)	This command was introduced.

Usage Guidelines

None

Example

```
clear lldp counters
```

Table 2: Related Commands

Command Syntax	Description
show lldp interface	Displays LLDP interface information

clear logging

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

clear logging { **dropcount** | **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**, **rxwait**, **register-log**, **stack-trace**, **starttime**, **status**, **system-health**, **txwait**, and so on.
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
9.2(1)	The TxWait OBFL file size was increased from 512 KB to 8 MB.
3.0(1)	Added the **onboard**, **module** and **session** options.
1.0(2)	This command was introduced.

Usage Guidelines

From Cisco MDS NX-OS Release 9.2(1), the TxWait OBFL file size was increased from 512 KB to 8 MB.

If you are upgrading to Cisco MDS NX-OS Release 9.2(1) or later releases, ensure that you use the **clear logging onboard txwait** command after upgrading. Otherwise, the file will be automatically deleted and recreated at the new file size when the file size exceeds 512 KB.

If you are downgrading from Cisco MDS NX-OS Release 9.2(1) or later releases and the file size is more than 512 KB, you will be prompted with a message to use the **clear logging onboard txwait** command to delete the file after downgrading.

If you are downgrading from Cisco MDS NX-OS Release 9.2(1) or later releases and the file size is less than 512 KB, the file is automatically deleted and recreated at the 512 KB file size after downgrading.

Therefore, we recommend that you use the **clear logging onboard txwait** command immediately in the following two instances:

- After upgrading from any release prior to Cisco MDS NX-OS Release 9.2(1) to Release 9.2(1) or later

- After downgrading from Cisco MDS NX-OS Release 9.2(1) or later to any release prior to Cisco MDS NX-OS Release 9.2(1)

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 snmp counters

To clear all the SNMP counters protocol statistics, use the **clear snmp counters**command. The counters which are cleared with the help of this command are **SNMP packet counts**, **SNMP errors** and **SNMP protocol-specific counters**.

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.1(2)	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-related counters.

```
switch# clear snmp counters
switch#
```

Related Commands

Command	Description
show snmp	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).

client-trustpoint

Use the **client-trustpoint** command to specify which trustpoint holds the client certificate that the switch presents to the EST server for mutual TLS (mTLS) authentication.

Use the **no** form of the command to remove the association with the trust point.

client-trustpoint *bootstrap_trustpoint*

no client-trustpoint *bootstrap_trustpoint*

Syntax Description

client	Configure client certificate information
trustpoint *bootstrap_trustpoint*	Specifies the trustpoint containing the switch client certificates.

Command Default

None.

Command Modes

trustpoint-est configuration submode

Command History

Release	Modification
9.4(5)	This command was introduced.

Usage Guidelines

The specified trustpoint must already be created before using this command.

Examples

```
switch# configure terminal
switch(config)# crypto ca trustpoint engineering-est-tp
switch(config-trustpoint)# management-method est
switch(config-trustpoint-est)# enrollment
switch(config-trustpoint-est)# renew lifetime 98
switch(config-trustpoint-est)# server 192.0.2.123 port 8443 path-segment /certs-eng proxy
system
switch(config-trustpoint-est)# client-trustpoint bootstrap_trustpoint
switch(config-trustpoint)# rsakeypair engineering-est-kp 4096
```

Related Commands

Command	Description
enrollment	Enable the certificate enrollment functionality using the Enrollment over Secure Transport (EST) protocol.
management-method est	Enters EST configuration submode
renew lifetime	Configures when to start certificate renewal.
show crypto ca certificates	Displays installed switch identity certificates.

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.**

In the **clock timezone** command, ensure that the STD timezone is not set to a non-DST timezone. Similarly, ensure that the DST timezone is set in the **clock summer-time** command. Otherwise, the SAN telemetry receivers will be unable to correlate the analytics metric timestamps.

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 format

To set the clock format that is to be used in NX-OS, use the **clock format** command. To reset the clock format, use the **no** form of this command.

clock format { **12-hours** | **24-hours** | **show-timezone** { **debug** | **syslog** } }

Syntax Description

12-hours	Specifies to set the clock format to 12 hours.
24-hours	Specifies to set the clock format to 24 hours.
show-timezone debug	Specifies to display the configured timezone in debug messages.
show-timezone syslog	Specifies to display the configured timezone in syslog messages.

Command Default

Clock format is set to 24 hours.

Timezone is included in debug messages.

Timezone is included in syslog messages.

Command Modes

Configuration mode (config)

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

The following example displays how to set the clock format to 12 hours:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# clock format 12-hours
```

The following example displays how to reset the clock format to 24 hours:

```
switch# configure
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# no clock format 12-hours
```

Related Commands

Command	Description
show running-config	Displays the active configuration of the switch.

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 startup-config running-config

To copy the startup configuration to the running configuration, use the **copy startup-config running-config** command.

copy startup-config running-config

Command Default

None.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.5(1)	Added a warning to alert users about overwriting the running configuration with startup configuration.
1.3(4)	This command was introduced.

Examples

The following example displays how to copy the startup configuration to the running configuration:

```
switch# copy startup-config running-config
Warning: This command will overwrite the running-config with startup-config.
Do you wish to proceed anyway? (y/n) [n] y
Copy complete.
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration.

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.
input-errors	Configures the input errors counter 1.3.6.1.2.1.2.2.1.14.
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.
rx-datarate-burst	Configures the receive datarate burst counter.
sfp-rx-power-low-warn	Configures the SFP receive power low warning counter.
sfp-tx-power-low-warn	Configures the SFP transmit power low warning counter.
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-datarate-burst	Configures the transmit datarate burst counter.
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.
warning-signal-threshold *count1*	Configures the warning signal threshold.
alarm-signal-threshold *count2*	Configures the alarm signal threshold.
portguard congestion-signals	Configures the congestion signal.
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 *count3*	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 *count4*	Sets numerical warning threshold limit. The range is from 0 to184467440737095516l5.
alerts	Specify to configure alerts.
obfl	Sets OBFL alerts.

rmon	Sets RMON alerts.
syslog	Sets syslog alerts.
none	Clears all alerts.
datarate *count5*	Configures the datarate counter.
falling-threshold *count6*	Sets numerical lower threshold limit. The range is from 0 to18446744073709551615.
portguard DIRL	Sets the port guard action for Dynamic Ingress Rate Limiting (DIRL).
portguard FPIN	Sets the port guard action for Fabric Performance Impact Notifications (FPIN).
portguard cong-isolate-recover	Sets the port guard action to recover traffic when traffic congestion is detected on a port.
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
8.5(1)	Added the **input-errors**, **rx-datarate-burst**, **sfp-rx-power-low-warn**, **sfp-tx-power-low-warn**, **tx-datarate-burst**, **warning-signal-threshold**, **alarm-signal-threshold**, **portguard congestion-signals**, **alerts**, **datarate**, **DIRL**, **FPIN**, and **cong-isolate-recover** keywords.
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 certfcate and associated RSA key pair and CA certificate or certfcate 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
AANBADbGBsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
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 *hours*	Specifies timer to fetch crl from remote certstore. 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 *group-name*	Specifies LDAP server group. 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 **config-crypto-map-ip** config submode supports *security-association lifetime* in gigabytes. It doesn't support kilobytes or megabytes.

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.

Command	Description
crypto transform-set domain ipsec	Configures the transform set for an IPsec crypto map.
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.