



## CHAPTER 4

# C Commands

---

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

***Send documentation comments to mdsfeedback-doc@cisco.com***

# callhome

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

## callhome

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

**Defaults** Disabled.

**Command Modes** Configuration mode.

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

**Usage Guidelines** 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:

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

```
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
<b>alert-group</b>	Customizes a Call Home alert group with user-defined <b>show</b> commands.
<b>callhome test</b>	Sends a dummy test message to the configured destination(s).
<b>show callhome</b>	Displays configured Call Home information.

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

# callhome test

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

**callhome test** [**inventory**]

<b>Syntax Description</b>	<b>inventory</b> (Optional) Sends a dummy Call Home inventory.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	1.0(2)	This command was introduced.

<b>Usage Guidelines</b>	You can simulate a message generation by issuing a <b>callhome test</b> command.
-------------------------	--

<b>Examples</b>	The following example sends a test message to the configured destination(s):
	<pre>switch# <b>callhome test</b> trying to send test callhome message successfully sent test callhome message</pre>
	The following example sends a test inventory message to the configured destination(s):
	<pre>switch# <b>callhome test inventory</b> trying to send test callhome message successfully sent test callhome message</pre>

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>callhome</b>	Configures Call Home functions.
	<b>show callhome</b>	Displays configured Call Home information.

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

## cd

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

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

<b>Syntax Description</b>	<i>directory</i>	(Optional) Name of the directory on the file system.
	<b>bootflash:</b>	URI or alias of the bootflash or file system.
	<b>slot0:</b>	URI or alias of the slot0 file system.
	<b>volatile:</b>	URI or alias of the volatile file system.

<b>Defaults</b>	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.

<b>Command Modes</b>	EXEC mode
----------------------	-----------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	1.0(2)	This command was introduced.

<b>Usage Guidelines</b>	For all EXEC commands that have an optional file system argument, the system uses the file system specified by the <b>cd</b> command when you omit the optional file system argument. For example, the <b>dir</b> 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 <b>cd</b> command.
-------------------------	---

<b>Examples</b>	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:/
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>copy</b>	Copies any file from a source to a destination.
	<b>delete</b>	Deletes a file on a flash memory device.
	<b>dir</b>	Displays a list of files on a file system.
	<b>pwd</b>	Displays the current setting of the <b>cd</b> command.
	<b>show file systems</b>	Lists available file systems and their alias prefix names.
	<b>undelete</b>	Recovers a file marked deleted on a Class A or Class B flash file system.

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

## 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

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

### Defaults

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)#
```

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

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 gigabitethernet 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**

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

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

## 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.

---

**Defaults** 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 reenables CFS distribution:

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



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

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

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

## cfs ipv4 distribute

To enable Cisco Fabric Services (CFS) distribution over IPv4 for applications that want to use this feature, use the **cfs ipv4** 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.

### Defaults

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 has 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 reenab CFS IPv4 distribution:

```
switch# config terminal
```

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

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

**Related Commands**

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

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

## 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

<i>ipv4-address</i>	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.
---------------------	--

### Defaults

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 keep-alive 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
```

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

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

**Related Commands**

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

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

## 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.

**Defaults** 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 has 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 reenab CFS IPv6 distribution:

```
switch# config terminal
```

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

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

**Related Commands**

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

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

# 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	<i>ipv6-address</i>	Specifies an IPv6 multicast address or CFS distribution over IPv6. The IPv6 Admin scope range is [ff15::/16, ff18::/16].
--------------------	---------------------	--

Defaults	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 keep-alive 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
```



***Send documentation comments to mdsfeedback-doc@cisco.com***

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

**Related Commands**

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

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

## 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

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

### Defaults

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
```

***Send documentation comments to mdsfeedback-doc@cisco.com***

```
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 will be moved to default region.  
Are you sure? (y/n) [n] y
```

**Related Commands**

Command	Description
<b>show cfs regions</b>	Displays all configured applications with peers.

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

## 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.

### Defaults

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
<b>show cfs static peers</b>	Displays configured static peers with status.

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

## 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.

### Defaults

Enabled.

### Command Modes

Interface configuration submode.

### Command History

Release	Modification
2.0(x)	This command was introduced.

### Usage Guidelines

This command determines the protocol behavior 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
<b>show interface port-channel</b>	Displays PortChannel interface information.

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

## 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

<i>port-channel number</i>	Specifies the PortChannel number. The range is 1 to 256.
<b>force</b>	Specifies the PortChannel to add a port using the force option.

### Defaults

None.

### Command Modes

Interface configuration mode.

### Command History

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

### Usage Guidelines

The auto mode support is not available after 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
<b>show interface port-channel</b>	Displays the PortChannel interface information.

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

## 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

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

### Defaults

None.

### Command Modes

Configuration mode.

### Command History

Release	Modification
1.3(1)	This command was introduced.

### Usage Guidelines

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

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

---

**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
<b>show csimserver</b>	Displays configured CIM settings and parameters.



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

## cimserver clearcertificate

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

**cimserver clearcertificate**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	Configuration mode.
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.3(1a)	This command was introduced.

<b>Usage Guidelines</b>	You need not specify the certificate name.
-------------------------	--

<b>Examples</b>	<p>The following example shows how to clear the cimserver certificate:</p> <pre>switch# <b>config</b> Enter configuration commands, one per line. End with CNTL/Z. switch(config)# <b>cimserver clearcertificate</b></pre>
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show cimserver certificate name</b>	Displays cimserver certificate file name.

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

## cimserver loglevel

To configure the cimserver loglevel filter, use the **cimserver loglevel** command in configuration mode.

**cimserver loglevel** *filter value*

Syntax Description	<i>filter value</i>	<p>1—Specifies the cimserver log filter levels. The range is 1 to 5.</p> <p>2—Sets the current value for the log level property to trace.</p> <p>3—Sets the current value for the log level property to information.</p> <p>4—Sets the current value for the log level property to warning.</p> <p>5—Sets the current value for the log level property to severe.</p> <p>6—Sets the current value for the log level property to fatal.</p>
--------------------	---------------------	--

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

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

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

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

Examples	<p>The following example displays the cimserver log level:</p> <pre>switch# <b>config</b> Enter configuration commands, one per line. End with CNTL/Z. switch(config)# <b>cimserver loglevel 2</b> Current value for the property logLevel is set to "INFORMATION" in CIMServer.</pre>
----------	--

Related Commands	Command	Description
	<b>show cimserver logs</b>	Displays the cimserver logs.

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

## 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	<i>class-map-name</i>	Selects the QoS policy class map to configure.
--------------------	-----------------------	--

Defaults	Disabled
----------	----------

Command Modes	QoS policy map configuration submode
---------------	--------------------------------------

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

Usage Guidelines	<p>Before you can configure a QoS policy map class you must complete the following:</p> <ul style="list-style-type: none"> <li>• Enable the QoS data traffic feature using the <b>qos enable</b> command.</li> <li>• Configure a QoS class map using the <b>qos class-map</b> command.</li> <li>• Configure a QoS policy map using the <b>qos policy-map</b> command.</li> </ul> <p>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.</p>
------------------	--

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

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# qos enable
switch(config)# qos class-map class-map1
switch(config)# qos policy-map policyMap1
switch(config-pmap)# class class-map1
switch(config-pmap-c)#
```

Related Commands	Command	Description
	<b>dscp</b>	Configures the DSCP in the QoS policy map class.
	<b>qos class-map</b>	Configures a QoS class map.
	<b>qos enable</b>	Enables the QoS data traffic feature on the switch.
	<b>qos policy-map</b>	Configures a QoS policy map.

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

Command	Description
<b>priority</b>	Configures the priority in the QoS policy map class.
<b>show qos</b>	Displays the current QoS settings.

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

## clear accounting log

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

**clear accounting log**

<b>Syntax Description</b>	This command has no other arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	Release	Modification
	2.0(x)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	The following example clears the accounting log:
	switch# <b>clear accounting session</b>

<b>Related Commands</b>	Command	Description
	<b>show accounting log</b>	Displays the accounting log contents.

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

# 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.

**Defaults** 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.

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

## clear asic-cnt

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

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

<b>Syntax Description</b>	<b>all</b>	Clears the counter for all device types.
	<b>device-id</b>	Clears the counter for device type device ID.
	<b>list-all-devices</b>	Lists all device types.

**Defaults** None.

**Command Modes** EXEC mode.

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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#
```

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

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
              |             10
              |             1
X-Bus IO       |             1
Power Mngmnt Epld |          25
module-4#
```

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



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

## clear callhome session

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

**clear callhome session**

<b>Syntax Description</b>	This command has no other arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	2.0(x)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	The following example shows how to clear the Call Home session configuration and locks:  switch# <b>clear callhome session</b>
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show callhome</b>	Displays Call Home information.

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

## 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

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

### Defaults

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
<b>cdp</b>	Configures global or interface-specific CDP settings and parameters.
<b>show cdp</b>	Displays configured CDP settings and parameters.

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

## clear cores

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

**clear cores**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	Release	Modification
	1.0(2)	This command was introduced.

<b>Usage Guidelines</b>	The system software keeps the last few cores per service and per slot and clears all other cores present on the active supervisor module.
-------------------------	---

<b>Examples</b>	The following example shows how to clear all core dumps for the switch:  switch# <b>clear cores</b>
-----------------	---

<b>Related Commands</b>	Command	Description
	<b>show cores</b>	Displays core dumps that have been made.

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

## 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* }

<b>Syntax Description</b>	<b>all</b>	Clears all interface counters.
	<b>interface</b>	Clears interface counters for the specified interface. See the Usage Guidelines for the interface type and their numbers.
	<i>number</i>	Specifies the number of the slot or interface being cleared.

**Defaults** None.

**Command Modes** EXEC mode.

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	1.0(2)	This command was introduced.

**Usage Guidelines** The following table lists the keywords and number ranges for the **clear counters** interface types:

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

This command clears counter 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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show interface</b>	Displays interface information.

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

## clear counters (SAN extension N port configuration mode)

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

**clear counters**

<b>Syntax Description</b>	This command has no other arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	SAN extension N port configuration submode.
----------------------	---

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	2.0(x)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	<p>The following example shows how to clear SAN extension tuner N port counters:</p> <pre>switch# <b>san-ext-tuner</b> switch(san-ext)# <b>nwwn 10:00:00:00:00:00:00</b> switch(san-ext)# <b>nport pwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2</b> switch(san-ext-nport)# <b>clear counters</b></pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show san-ext-tuner</b>	Displays SAN extension tuner information.

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

## 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*]

<b>Syntax Description</b>	<i>tunnel-id</i> (Optional) Specifies a tunnel ID. The range is 1 to 2147483647.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	2.0(x)	This command was introduced.

<b>Usage Guidelines</b>	To use this command, the IKE protocol must be enabled using the <b>crypto ike enable</b> command. If the tunnel ID is not specified, all IKE tunnels are cleared.
-------------------------	--

<b>Examples</b>	The following example shows how to clear all IKE tunnels:  switch# <b>clear crypto ike domain ipsec sa</b>
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>crypto ike domain ipsec</b>	Configures IKE information.
	<b>crypto ike enable</b>	Enables the IKE protocol.
	<b>show crypto ike domain ipsec</b>	Displays IKE information for the IPsec domain.

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

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

Defaults	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 <b>crypto ipsec enable</b> command.
------------------	---

Examples	The following example shows how to clear a security association for an interface:  switch# <b>clear crypto sa domain ipsec interface gigabitethernet 1/2 inbound sa 1</b>
----------	---

Related Commands	Command	Description
	<b>show crypto sad</b> <b>domain ipsec</b>	Displays IPsec security association database information.

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

## clear debug-logfile

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

**clear debug-logfile** *filename*

<b>Syntax Description</b>	<i>filename</i>	The name (restricted to 80 characters) of the log file to be cleared. The maximum size of the log file is 1024 bytes.
<b>Defaults</b>	None.	
<b>Command Modes</b>	EXEC mode.	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	1.0(2)	This command was introduced.
<b>Examples</b>	<p>The following example shows how to clear the debug logfile:</p> <pre>switch# clear debug-logfile debuglog</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	show debug logfile	Displays the log file contents.



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

## clear device-alias

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

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

Syntax Description	session	Clears session information.
	statistics	Clears device alias statistics.

Defaults	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# <b>clear device-alias session</b>
----------	---

Related Commands	Command	Description
	<b>show device-alias</b>	Displays device alias database information.

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

## clear dpvm

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

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

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

**Defaults** None.

**Command Modes** EXEC mode.

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>dpvm enable</b>	Enables DPVM.
	<b>show dpvm</b>	Displays DPVM database information.

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

## clear dpvm merge statistics

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

**clear dpvm merge statistics**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	Configuration mode.
----------------------	---------------------

<b>Command History</b>	Release	Modification
	NX-OS 4.1(1b)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	The following example shows how to clear the DPVM merge statistics:
-----------------	---

<pre>switch#(config)# <b>clear dpvm merge statistics</b></pre>
<pre>switch#(config)#</pre>

<b>Related Commands</b>	Command	Description
	<b>show dpvm merge statistics</b>	Displays the DPVM merge statistics.

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

## 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	<b>vsan</b> <i>vsan-id</i>	Specifies the FICON-enabled VSAN. The ID of the VSAN is from 1 to 4093.
--------------------	----------------------------	---

Defaults	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# <b>clear fabric-binding statistics vsan 1</b>
----------	---

Related Commands	Command	Description
	<b>show fabric-binding efmd statistics</b>	Displays existing fabric binding statistics information.

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

## clear fcanalyzer

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

**clear fcanalyzer**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC.
----------------------	-------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	1.0(2)	This command was introduced.

<b>Usage Guidelines</b>	This command clears only the list of configured hosts. Existing connections are not terminated.
-------------------------	---

<b>Examples</b>	The following example shows how to clear the entire list of configured hosts for remote capture: <pre>switch# clear fcanalyzer</pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	show fcanalyzer	Displays the list of hosts configured for a remote capture.

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

## 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*

<b>Syntax Description</b>	<b>aggregated</b>	(Optional) Clears the Fibre Channel flow aggregated statistics.
	<b>module</b>	Clears the statistics for a specified module.
	<i>module-number</i>	Specifies the module number.
	<b>index</b>	Clears the Fibre Channel flow counters for a specified flow index.
	<i>flow-number</i>	Specifies the flow index number.

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

<b>Command Modes</b>	EXEC.
----------------------	-------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show fcflow</b>	Displays the fcflow statistics.

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

## 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	<b>vsan</b> <i>vsan-id</i>	Clears FCS statistics for a specified VSAN ranging from 1 to 4093.
--------------------	----------------------------	--

Defaults	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
	<b>show fcns statistics</b>	Displays the name server statistics.

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

## 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	<b>vsan</b> <i>vsan-id</i>	FCS statistics are to be cleared for a specified VSAN ranging from 1 to 4093.
--------------------	----------------------------	---

Defaults	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# <b>clear fcs statistics vsan 10</b>

Related Commands	Command	Description
	<b>show fcs statistics</b>	Displays the fabric configuration server statistics information.



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

## clear fctimer session

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

**clear fctimer session**

<b>Syntax Description</b>	This command has no other arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	2.0(x)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	The following example shows how to clear fctimer session:  switch# <b>clear fctimer session</b>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	show fctimer	Displays fctimer information.

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

## 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]*

<b>Syntax Description</b>	<i>vt vt-pwwn</i>	Specify the VT pWWN for the configuration to be deleted.
	<i>local-switch-only</i>	(Optional) The configuration is deleted locally only.

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.2(1)	This command was introduced.

<b>Usage Guidelines</b>	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.

<b>Examples</b>	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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show fc-redirect active-configs</b>	Displays all active configurations on the switch.

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

## 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

<b>Syntax Description</b>	This command has no other arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.2(1)	This command was introduced.

<b>Usage Guidelines</b>	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.
-------------------------	---

<b>Examples</b>	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#
```

 clear fc-redirect decommission-switch

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

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

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

## 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	<b>vsan</b> <i>vsan-id</i>	Specifies the FICON-enabled VSAN. The ID of the VSAN is from 1 to 4093.
	<b>allegiance</b>	(Optional) Clears the FICON device allegiance.
	<b>timestamp</b>	(Optional) Clears the FICON VSAN specific timestamp.

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

Command Modes	EXEC mode.
---------------	------------

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

Usage Guidelines	The <b>clear ficon vsan</b> <i>vsan-id</i> <b>allegiance</b> command aborts the currently executing session.
------------------	--

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

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

The following example clears the VSAN clock for VSAN 20:

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

Related Commands	Command	Description
	<b>show ficon</b>	Displays configured FICON details.

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

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

Defaults	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# <b>clear fspf counters vsan 1</b>
	The following example clears FSPF statistics specific to the Fibre Channel interface in VSAN 1, Slot 9 Port 32:  switch# <b>clear fspf counters vsan 1 interface fc 9/32</b>

Related Commands	Command	Description
	<b>show fspf</b>	Displays global FSPF information for a specific VSAN.

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

## 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.

#### Defaults

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

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

## 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*

<b>Syntax Description</b>	<i>list-name</i> Specifies the IP access list name (maximum 64 characters).				
<b>Defaults</b>	None.				
<b>Command Modes</b>	EXEC.				
<b>Command History</b>	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>1.1(1)</td><td>This command was introduced.</td></tr> </table>	Release	Modification	1.1(1)	This command was introduced.
Release	Modification				
1.1(1)	This command was introduced.				
<b>Examples</b>	<p>The following example clears the counters for an IP access list:</p> <pre>switch# clear ip access-list counters adminlist</pre>				
<b>Related Commands</b>	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td><b>show ip access-list</b></td><td>Displays IP access list information.</td></tr> </table>	Command	Description	<b>show ip access-list</b>	Displays IP access list information.
Command	Description				
<b>show ip access-list</b>	Displays IP access list information.				



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

## 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	<b>address</b>	Clears fcflow aggregated statistics.
	<i>ip-address</i>	Enters the peer IP address.
	<b>interface</b> <b>gigabitethernet</b>	Specifies the Gigabit Ethernet interface.
	<i>module-number</i>	Specifies the slot and port of the Gigabit Ethernet interface.

Defaults	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
```

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

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

**Defaults** 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#
```

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

## 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*]

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

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.2(1)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	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#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ips stats fabric interface</b>	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.

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

## clear ipv6 access-list

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

**clear ipv6 access-list** [*list-name*]

<b>Syntax Description</b>	<b>access-list</b>	Displays a summary of access control lists (ACLs).
	<i>list-name</i>	(Optional) Specifies the name of the ACL. The maximum size is 64.

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.1(0)	This command was introduced.

<b>Usage Guidelines</b>	You can use the <b>clear ipv6 access-list</b> command to clear IPv6-ACL statistics.
-------------------------	---

<b>Examples</b>	The following example displays information about an IPv6-ACL:
-----------------	---

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ipv6 access-list</b>	Configures an IPv6-ACL.
	<b>show ipv6</b>	Displays IPv6 configuration information.

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

## clear ipv6 neighbors

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

**clear ipv6 neighbors**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.1(0)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	The following example flushes the IPv6 neighbor cache table:
	<pre>switch# clear ipv6 neighbors switch#</pre>

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ipv6 nd</b>	Configures IPv6 neighbor discovery commands.
	<b>show ipv6 neighbors</b>	Displays IPv6 neighbors configuration information.

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

## 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.

**Defaults** 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
	<b>islb abort</b>	Discards a pending iSLB configuration.
	<b>show islb cfs-session status</b>	Displays iSLB session details.
	<b>show islb pending</b>	Displays an iSLB pending configuration.
	<b>show islb pending-diff</b>	Displays iSLB pending configuration differences.
	<b>show islb session</b>	Displays iSLB session information.
	<b>show islb status</b>	Displays iSLB CFS status.
	<b>show islb vrrp</b>	Displays iSBL VRRP load balancing information.

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

## clear ivr fcdomain database

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

**clear ivr fcdomain database**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	2.1(2)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	The following example clears all IVR fcdomain database information:
	switch# <b>clear ivr fcdomain database</b>

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ivr fcdomain database</b>	Displays IVR fcdomain database entry information.

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

## 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**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.0(1)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	<p>The following example clears the ivr service-group database:</p> <pre>switch# clear ivr service-group database</pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ivr service-group database</b>	Displays an IVR service group database.



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

## 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**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC.
----------------------	-------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	1.3(1)	This command was introduced.

<b>Examples</b>	The following example clears all configured IVR information:  switch# <b>clear ivr zone database</b>
-----------------	--

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

## clear license

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

**clear license** *filename*

Syntax Description	<i>filename</i>	Specifies the license file to be uninstalled.
--------------------	-----------------	---

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

Command Modes	EXEC.
---------------	-------

Command History	Release	Modification
	1.3(2)	This command was introduced.

Examples	<p>The following example clears a specific license:</p> <pre>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=&lt;LicFileID&gt;san_extn2.lic&lt;/LicFileID&gt;&lt;LicLineID&gt;1&lt;/LicLineID&gt; \     SIGN=67CB2A8CCAC2  Do you want to continue? (y/n) <b>y</b> Clearing license ..done switch#</pre>
----------	---

Related Commands	Command	Description
	<b>show license</b>	Displays license information.

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

## clear line

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

**clear line** *vtty-name*

Syntax Description	<i>vtty-name</i> Specifies the VTY name (maximum 64 characters).
--------------------	--

Defaults	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
	<b>show line</b>	Displays line information.

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

## clear logging

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

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

Syntax Description		
<b>logfile</b>		Clears log file messages.
<b>nvr</b> am		Clears NVRAM logs.
<b>onboard</b> <i>information</i>		Clears onboard failure logging (OBFL) information. The types of information include <b>boot-up</b> time, <b>cpu-hog</b> , <b>device-version</b> , <b>endtime</b> , <b>environmental-history</b> , <b>error-stats</b> , <b>exception-log</b> , <b>interrupt-stats</b> , <b>mem-leak</b> , <b>miscellaneous-error</b> , <b>module</b> , <b>obfl-history</b> , <b>obfl-log</b> , <b>register-log</b> , <b>stack-trace</b> , <b>starttime</b> , <b>status</b> , and <b>system-health</b> .
<b>module</b> <i>slot</i>		(Optional) Clears OBFL information for a specified module.
<b>session</b>		Clears a logging session.

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

<b>Command Modes</b>	EXEC.
----------------------	-------

Command History	Release	Modification
	1.0(2)	This command was introduced.
	3.0(1)	Added the <b>onboard</b> , <b>module</b> and <b>session</b> options.

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

```
switch# clear logging logfile
```

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

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

Related Commands	Command	Description
	<b>show logging</b>	Displays logging information.

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

## 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.

Defaults	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.

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

## clear port-security

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

```
clear port-security {database auto-learn {interface fc slot/port | port-channel port} | session | statistics} vsan vsan-id
```

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

**Defaults** None.

**Command Modes** EXEC mode.

Command History	Release	Modification
	1.2(1)	This command was introduced.
	2.0(x)	Added the <b>session</b> 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
```

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

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

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

## 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*}

<b>Syntax Description</b>	<b>all</b>	Deletes all of the log files.
	<b>pid</b>	Deletes the log files of a specific process.
	<i>pid-number</i>	Specifies the process ID, which must be from 0 to 2147483647.

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	1.0(2)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	<p>The following example shows how to clear all of the log files on the switch :</p> <pre>switch# clear processes log all</pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show processes</b>	Displays the detailed running or log information of processes or high availability applications.



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

## clear qos statistics

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

**clear qos statistics**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	1.0(2)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	The following example shows how to clear the quality of service counters:
-----------------	---

```
switch# clear qos statistics
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	show qos statistics	Displays the current QoS settings, along with a number of frames marked high priority.

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

## clear radius-server statistics

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

**clear radius-server statistics** *{name}*

<b>Syntax Description</b>	<i>name</i> Specifies the RADIUS name or IP address.
---------------------------	--

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

<b>Command Modes</b>	Configuration mode.
----------------------	---------------------

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

<b>Usage Guidelines</b>	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)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>tacacs+ enable</b>	Enables TACACS+.

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

## clear radius session

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

**clear radius session**

<b>Syntax Description</b>	This command has no other arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	2.0(x)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	The following example shows how to clear RADIUS session:  switch# <b>clear radius session</b>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show radius</b>	Displays RADIUS CFS distribution status and other details.

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

## 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

<b>history</b>	Clears RLIR link incident history.
<b>recent</b>	Clears recent link incidents.
<b>interface</b> <i>fc slot/port</i>	Clears entries for a specified interface.
<b>bay</b> <i>port</i>   <b>ext</b> <i>port</i>	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.
<b>portnumber</b> <i>port-number</i>	Displays the port number for the link incidents.
<b>statistics</b>	Clears RLIR statistics.
<b>vsan</b> <i>vsan-id</i>	Specifies the VSAN ID for which the RLIR statistics are to be cleared.

### Defaults

None.

### Command Modes

EXEC mode.

### Command History

Release	Modification
1.3(1)	This command was introduced.
3.1(2)	Added the <b>interface bay</b>   <b>ext</b> 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
```

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

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.

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

## 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.

**Defaults** 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
	<b>clear rmon all-alarms</b>	Clears all the 32-bit and 64-bit RMON alarms.
	<b>clear rmon hcalarms</b>	Clears all the 64-bit RMON alarms.
	<b>clear rmon log</b>	Clears RMON log information.

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

## 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**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.3(1a)	This command was introduced.

<b>Usage Guidelines</b>	You must save the changes to startup configuration to make them permanent.
-------------------------	--

<b>Examples</b>	The following example clears all the 32-bit and 64-bit RMON alarms from the running configuration: <pre>switch# clear rmon all-alarms switch#</pre>
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear rmon alarms</b>	Clears all the 32-bit RMON alarms.
	<b>clear rmon hcalarms</b>	Clears all the 64-bit RMON alarms.
	<b>clear rmon log</b>	Clears RMON log information.

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

## 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.

**Defaults** 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
	<b>clear rmon all-alarms</b>	Clears all the 32-bit and 64-bit RMON alarms.
	<b>clear rmon alarms</b>	Clears all the 32-bit RMON alarms.
	<b>clear rmon log</b>	Clears RMON log information.



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

## clear rmon log

To clear all entries from RMON log on the switch, use the **clear rmon log** command.

**clear rmon log**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.3(1a)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	The following example clears all entries from RMON log on the switch:
	<pre>switch# clear rmon log switch#</pre>

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear rmon alarm</b>	Clears all the 32-bit RMON alarms.
	<b>clear rmon hcalarms</b>	Clears all the 64-bit RMON alarms.
	<b>clear rmon all-alarms</b>	Clears all the 32-bit and 64-bit RMON alarms.

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

## 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.

**Defaults** 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.

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

## 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	<i>vsan-id</i>	Specifies a VSAN where the RSCN session should be cleared. The ID of the VSAN is from 1 to 4093.
--------------------	----------------	--

Defaults	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# <b>clear rscn session vsan 1</b>
----------	---

Related Commands	Command	Description
	<b>rscn</b>	Configures an RSCN.
	<b>show rscn</b>	Displays RSCN information.

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

## 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

<b>vsan</b>	The RSCN statistics are to be cleared for a VSAN.
<b><i>vsan-id</i></b>	The ID for the VSAN for which you want to clear RSCN statistics.

### Defaults

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
<b>show rscn</b>	Displays RSCN information.

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

## 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		
<i>slot-number</i>		Specifies the Storage Services Module (SSM) module number. The range is 1 through 13.
<b>avt</b> <i>avt-pwwn</i>		Removes the appliance virtual target (AVT) pWWN. The format is <i>hh:hh:hh:hh:hh:hh:hh:hh</i> .
<b>lun</b> <i>avt-lun</i>		(Optional) Removes the appliance virtual target (AVT) LUN. The format is <i>0xhhhh[:hhhh[:hhhh[:hhhh]]]</i> .
<b>itl</b> <i>target-pwwn</i> <i>host-pwwn</i>		Removes the SANTap Initiator Target LUN (ITL) triplet. The format of the <i>target-pwwn</i> and the <i>host-pwwn</i> is <i>hh:hh:hh:hh:hh:hh:hh:hh</i> .
<b>session</b> <i>session-id</i>		Removes a session. The range for session ID is 0 through 2147483647.

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

Command History	Release	Modification
	3.0(1)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	The following example shows how to remove a SANTap session:
-----------------	---

```
switch# clear santap module 13 session 2020
```

Related Commands	Command	Description
	<b>santap module</b>	Configures the mapping between the Storage Services Module (SSM) and the VSAN where the appliance is configured.
	<b>show santap module</b>	Displays the configuration and statistics of the SANTap feature.

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

## 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*

<b>Syntax Description</b>	<i>slot</i>	Displays SANTap configuration for a module in the specified slot.
<b>Defaults</b>	None.	
<b>Command Modes</b>	EXEC mode.	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.2(1)	This command was introduced.
<b>Usage Guidelines</b>	None.	
<b>Examples</b>	<p>The following example shows how to clear the SANTap configuration for a slot 2:</p> <pre>switch# clear ssm-nvram santap module 2</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	ssm enable feature	Enables the SANTap feature on the SSM.

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

## clear scheduler logfile

To clear the command scheduler logfile, use the **clear scheduler logfile** command.

**clear scheduler logfile**

<b>Syntax Description</b>	This command has no other arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	2.0(x)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	The following example shows how to clear the command scheduler logfile:
	switch# <b>clear scheduler logfile</b>

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show scheduler</b>	Displays command scheduler information.

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

## clear screen

To clear the terminal screen, use the **clear screen** command in EXEC mode.

**clear screen**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	1.0(2)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	<p>The following example shows how to clear the terminal screen:</p> <pre>switch# <b>clear screen</b></pre>
-----------------	---



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

## 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*

<b>Syntax Description</b>	<b>flow-id</b> <i>flow-id</i>	Configures the SCSI flow identification number.
<b>Defaults</b>	None.	
<b>Command Modes</b>	EXEC mode.	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	2.0(2)	This command was introduced.
<b>Usage Guidelines</b>	None.	
<b>Examples</b>	The following example shows how to clear the SCSI flow statistics counters for SCSI flow ID 3:  switch# <b>clear scsi-flow statistics flow-id 3</b>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>scsi-flow flow-id</b>	Configures the SCSI flow services.
	<b>show scsi-flow</b>	Displays SCSI flow configuration and status.

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

## 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*}

<b>Syntax Description</b>	<b>database</b>	Clears the SDV database.
	<b>vsan</b> <i>vsan-id</i>	Specifies the number of the VSAN. The range is 1 to 4093.
	<b>session</b>	Clears the SDV session.
	<b>statistics</b>	Clears the SDV statistics.

**Defaults** None.

**Command Modes** EXEC mode.

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>sdv enable</b>	Enables or disables SAN device virtualization.
	<b>show sdv statistics</b>	Displays SAN device virtualization statistics.

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

## clear snmp hostconfig

To clear all SNMP hosts from the running configuration, use the **clear snmp hostconfig** command.

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.3(1a)	This command was introduced.

<b>Usage Guidelines</b>	You must save the changes to startup configuration to make them permanent:
-------------------------	--

<b>Examples</b>	The following example clears the SNMP host list. <pre>switch# clear snmp hostconfig switch#</pre>
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	show snmp host	Displays the SNMP status and setting information.

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

## clear ssh hosts

To clear trusted SSH hosts, use the **clear ssh hosts** command in EXEC mode.

**clear ssh hosts**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	1.2(1)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	<p>The following example shows how to clear reset-reason information from NVRAM and volatile storage:</p> <pre>switch# <b>clear ssh hosts</b></pre>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ssh hosts</b>	Displays SSH host information.

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

## 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**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	Release	Modification
	1.3(2a)	This command was introduced.

<b>Usage Guidelines</b>	Use this command as follows for these switches:
	<ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li></ul>

<b>Examples</b>	The following example shows how to clear trusted SSH hosts:
	<pre>switch# clear system reset-reason</pre>

<b>Related Commands</b>	Command	Description
	<b>show system reset-reason</b>	Displays system reset-reason information.

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

## clear tacacs-server statistics

To clear TACACS server statistics, use the **clear tacacs-server statistics** command.

**clear tacacs-server statistics** *{name}*

<b>Syntax Description</b>	<i>name</i> Specifies the TACACS name or IP address.				
<b>Defaults</b>	None.				
<b>Command Modes</b>	EXEC mode.				
<b>Command History</b>	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>NX-OS 4.2(1)</td><td>This command was introduced.</td></tr> </table>	Release	Modification	NX-OS 4.2(1)	This command was introduced.
Release	Modification				
NX-OS 4.2(1)	This command was introduced.				
<b>Usage Guidelines</b>	None.				
<b>Examples</b>	<p>The following example shows how to clear the tacacs server statistics:</p> <pre>switch(config)# <b>clear tacacs-server statistics 10.64.65.57</b> switch(config)#</pre>				
<b>Related Commands</b>	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td><b>tacacs+ enable</b></td><td>Enables TACACS+.</td></tr> </table>	Command	Description	<b>tacacs+ enable</b>	Enables TACACS+.
Command	Description				
<b>tacacs+ enable</b>	Enables TACACS+.				

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

## clear tacacs+ session

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

**clear tacacs+ session**

<b>Syntax Description</b>	This command has no other arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	2.0(x)	This command was introduced.

<b>Usage Guidelines</b>	To use this command, TACACS+ must be enabled using the <b>tacacs+ enable</b> command.
-------------------------	---

<b>Examples</b>	The following example shows how to clear the TACACS+ session:  switch# <b>clear tacacs+ session</b>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show tacacs+</b>	Displays TACACS+ CFS distribution status and other details.
	<b>tacacs+ enable</b>	Enables TACACS+.

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

## 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**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	NX-OS 5.0 and later releases	This command was deprecated.
	1.3(5)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	<p>The following example shows how to clear a TL port ALPA cache:</p> <pre>switch# clear tlport alpa-cache</pre>
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show tlport alpa-cache</b>	Displays TL port alpa-cache information.



***Send documentation comments to mdsfeedback-doc@cisco.com***

## clear user

To clear trusted SSH hosts, use the **clear user** command in EXEC mode.

**clear user** *username*

Syntax Description	<i>username</i>	Specifies the user name to clear.
--------------------	-----------------	-----------------------------------

Defaults	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# <b>clear user vsam</b>
----------	--

Related Commands	Command	Description
	<b>show users</b>	Displays user information.

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

## 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		
<b>statistics</b>		Clears global VRRP statistics.
<b>ipv4</b>		(Optional) Clears IPv4 virtual router statistics.
<b>ipv6</b>		(Optional) Clears IPv6 virtual router statistics.
<b>vr number</b>		Clears specific virtual router statistics and specifies a VR number from 1 to 255.
<b>interface</b>		Clears an interface.
<b>gigabitethernet slot/port</b>		Clears a specified Gigabit Ethernet interface.
<b>mgmt 0</b>		Specifies the management interface.
<b>port-channel port-channel-id</b>		Clears a specified PortChannel interface. The ID of the PortChannel interface is from 1 to 128.
<b>vsan vsan-id</b>		Clears a specified VSAN. The ID of the VSAN is from 1 to 4093.

**Defaults** None.

**Command Modes** EXEC mode.

Command History	Release	Modification
	1.0(2)	This command was introduced.
	3.0(1)	Added the <b>ipv4</b> and <b>ipv6</b> 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
	<b>show vrrp</b>	Displays VRRP configuration information.
	<b>vrrp</b>	Enables VRRP.

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

## 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

<b>database</b>	Clears zone server database information.
<b>lock</b>	Clears a zone server database lock.
<b>statistics</b>	Clears zone server statistics.
<b>lun-zoning</b>	Clears LUN-zoning related statistics.
<b>read-only-zoning</b>	Clears read-only zoning related statistics.
<b>vsan</b>	Clears zone information for a VSAN.
<i>vsan-id</i>	The ID of the VSAN is from 1 to 4093.

### Defaults

None.

### Command Modes

EXEC mode.

### Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the <b>lock</b> 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
<b>show zone</b>	Displays zone information for any configured interface.

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

## 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

<i>command</i>	Specifies an alias command name. The maximum size is 30 characters.
<i>definition</i>	Specifies the alias command definition. The maximum size is 80 characters.

### Defaults

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.

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

### 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
<b>alias</b>	Displays the default alias command for <b>show cli alias</b> .
<b>show cli alias</b>	Displays all configured aliases.

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

## 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

<i>name</i>	Specifies a variable name. The maximum size is 31 characters.
<i>value</i>	Specifies a variable value. The maximum size is 80.

### Defaults

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
```

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

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).

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

## 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

<i>name</i>	Specifies a variable name. The maximum size is 31 characters.
<i>value</i>	Specifies a variable value. The maximum size is 80.

### Defaults

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
<b>show cli variables</b>	Displays all CLI variables (persistent, session and system).



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

# 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		
<b>summer-time</b>		Specifies the name of the time zone in summer.
<i>summer-time-name</i>		Specifies the name of the daylight savings time zone, ranging from 1 to 8 characters.
<i>start-week</i> <i>end-week</i>		Specifies the starting week and ending week, ranging from 1 (week 1) to 5 (week 5).
<i>start-day</i> <i>end-day</i>		Specifies the starting day and ending day, ranging from 1 to 8 characters (Sunday to Saturday).
<i>start-month</i> <i>end-month</i>		Specifies the starting month and ending month, ranging from 1 to 8 characters (January to December).
<i>start-time</i> <i>end-time</i>		Specifies the starting time and ending time, ranging from 00:00 to 23:59.
<i>offset-minutes</i>		Specifies the daylight savings time offset, ranging from 1 to 1440 minutes.
<b>timezone</b>		Specifies the name of the time zone.
<i>timezone-name</i>		Specifies the name of the time zone, ranging from 1 to 8 characters.
<i>hours-offset</i>		Specifies the offset time in hours, ranging from 0 to 23. Include a dash before the number; for example, -23.
<i>minutes-offset</i>		Specifies the offset time in minutes, ranging from 0 to 59. Include a dash before the number; for example, -59.

## Defaults

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 <b>timezone</b> .

## Usage Guidelines

The appropriate daylight savings time zone name should be specified. If it is not, the default name is used.

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

Specify the *hours-offset argument* with a dash before the number; for example, **-23** . Specify the *minutes-offset argument* with a dash before the number; for example, **-59**.

### Examples

The following example shows how to set Pacific Daylight Time starting on Sunday in the second week of March at 2:00 A.M. and ending on Sunday in the first week of November at 2:00 A.M:

```
switch# config t
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# config t
switch(config)# clock timezone PST 0 0
```

### Related Commands

Command	Description
<b>clock set</b>	Changes the time on the switch.
<b>show clock</b>	Displays the current date and time.
<b>show run</b>	Displays changes made to the time zone configuration along with other configuration information.

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

## clock set

To change the system time on a Cisco MDS 9000 Family switch, use the **clock set** command in EXEC mode.

**clock set** *HH:MM:SS DD Month YYYY*

Syntax Description	<i>HH:</i>	The two-digit time in hours in military format (15 for 3 p.m.).
	<i>MM:</i>	The two-digit time in minutes (58).
	<i>SS</i>	The two-digit time in seconds (15).
	<i>DD</i>	The two-digit date (12).
	<i>Month</i>	The month in words (August).
	<i>YYYY</i>	The four-digit year (2002).

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

<b>Command Modes</b>	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
```

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

## cloud discover

To initiate manual, on-demand cloud discovery, use the **cloud discover** command.

**cloud discover** [**interface** { **gigabitethernet** *slot/port* | **port-channel** *port-channel-number* }]

<b>Syntax Description</b>	<b>interface</b>	(Optional) Specifies an interface for cloud discovery.
	<b>gigabitethernet</b> <i>slot/port</i>	(Optional) Specifies a Gigabit Ethernet interface.
	<b>port-channel</b> <i>port-channel-number</i>	(Optional) Specifies a PortChannel interface. The range for the PortChannel number is 1 to 256.

**Defaults** None.

**Command Modes** EXEC mode.

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.0(1)	This command was introduced.

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

**Examples** The following example 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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>cloud discovery</b>	Configures cloud discovery.
	<b>cloud-discovery enable</b>	Enables discovery of cloud memberships.
	<b>show cloud discovery</b>	Displays discovery information about the cloud.
	<b>show cloud membership</b>	Displays information about members of the cloud.

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

## 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

<b>auto</b>	Enables auto fabric discovery.
<b>fabric distribute</b>	Enables cloud discovery fabric distribution.
<b>message icmp</b>	Configures Internet Control Message Protocol (ICMP) as the method for sending a discovery message.

### Defaults

Auto.

### Command Modes

Configuration mode.

### Command History

Release	Modification
3.0(1)	This command was introduced.

### 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 discovery auto
```

The following example enables auto cloud discovery fabric distribution:

```
switch(config)# cloud discovery fabric distribute
```

The following example disables auto cloud discovery fabric distribution:

```
switch(config)# no cloud discovery fabric distribute
```

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

Related Commands	Command	Description
	<b>cloud discover</b>	Initiates manual, on-demand cloud discovery.
	<b>cloud-discovery enable</b>	Enables discovery of cloud memberships.
	<b>show cloud discovery</b>	Displays cloud discovery information.
	<b>show cloud membership</b>	Displays information about members of the cloud.

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

## 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**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Defaults</b>	Disabled.
-----------------	-----------

<b>Command Modes</b>	Configuration mode.
----------------------	---------------------

Command History	Release	Modification
	3.0(1)	This command was introduced.

<b>Usage Guidelines</b>	This command is not supported on the Cisco MDS 9124 switch.
-------------------------	---

<b>Examples</b>	The following example enables discovery of cloud memberships:  switch# <b>config terminal</b> Enter configuration commands, one per line. End with CNTL/Z. switch(config)# <b>cloud-discovery enable</b>
	The following example disables discovery of cloud memberships:  switch(config)# <b>no cloud-discovery enable</b>

Related Commands	Command	Description
	<b>cloud discover</b>	Initiates manual, on-demand cloud discovery.
	<b>cloud discovery</b>	Configures cloud discovery.
	<b>show cloud</b>	Displays cloud discovery and membership information.

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

# cluster

To configure a cluster feature, use the **cluster** command.

## cluster enable

Syntax Description	enable	Enables or disables a cluster.
--------------------	--------	--------------------------------

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

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

Command History	Release	Modification
	3.2(2)	This command was introduced.
	NX-OS 4.1(1c)	The <b>cluster</b> command is replaced by the <b>feature</b> command.

Usage Guidelines	Starting from Cisco NX-OS 4.x Release, the <b>cluster</b> command is replaced by the <b>feature</b> command.
------------------	--

Examples	The following example enables the Cisco SME clustering:
----------	---

```
switch# config terminal
switch(config)# cluster enable
switch(config)#
```



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

## 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	
<b>code-page</b>	Configures code page on a FICON-enabled VSAN
<b>brazil</b>	Configures the <b>brazil</b> EBCDIC format.
<b>france</b>	Configures the <b>france</b> EBCDIC format.
<b>international-5</b>	Configures the <b>international-5</b> EBCDIC format.
<b>italy</b>	Configures the <b>italy</b> EBCDIC format.
<b>japan</b>	Configures the <b>japan</b> EBCDIC format.
<b>spain-latinamerica</b>	Configures the <b>spain-latinamerica</b> EBCDIC format.
<b>uk</b>	Configures the <b>uk</b> EBCDIC format.
<b>us-canada</b>	Configures the <b>us-canada</b> EBCDIC format.

**Defaults** 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
```

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

Related Commands	Command	Description
	<b>ficon vsan</b> <i>vsan-id</i>	Enables FICON on the specified VSAN.
	<b>show ficon</b>	Displays configured FICON details.

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

# 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.

**Defaults** 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
	<b>callhome</b>	Configures the Call Home function.
	<b>callhome test</b>	Sends a dummy test message to the configured destination(s).
	<b>show callhome</b>	Displays configured Call Home information.

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

## 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**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	DMM job configuration submode.
----------------------	--------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.2(1)	This command was introduced.

<b>Usage Guidelines</b>	You need to configure server HBA ports, storage ports, and job attributes before you commit the job.
-------------------------	--

<b>Examples</b>	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)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show dmm job</b>	Displays job information.
	<b>show dmm srvr-vt-login</b>	Enables DMM.

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

## 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

<i>customer-id</i>	Configures the service contract ID of the customer. Allows up to 64 characters for the contract number.
--------------------	---

### Defaults

None.

### Command Modes

Call Home configuration submode.

### Command History

Release	Modification
1.0(2)	This command was introduced.

### Usage Guidelines

None.

### Examples

The following example shows how to configure the 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
<b>callhome</b>	Configures the Call Home function.
<b>callhome test</b>	Sends a dummy test message to the configured destination(s).
<b>show callhome</b>	Displays configured Call Home information.

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

# configure terminal

To enter the configuration mode, use the **configure terminal** command in EXEC mode.

**configure terminal**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	1.0(2)	This command was introduced.

<b>Usage Guidelines</b>	None.
-------------------------	-------

<b>Examples</b>	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)#
```

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

## copy

To save a backup of the system software, use the **copy** command in EXEC mode.

**copy** *source-URL destination-URL*

### Syntax Description

<i>source-URL</i>	The location URL or alias of the source file or directory to be copied.
<i>destination-URL</i>	The destination URL or alias of the copied file or directory.

The following table lists the aliases for source and destination URLs.

<b>running-config</b>	Specifies the configuration currently running on the switch. The <b>system:running-config</b> keyword represents the current running configuration file.
<b>startup-config</b>	Specifies the configuration used during initialization (startup). You can copy the startup configuration from NVRAM. The <b>nvram:startup-config</b> keyword represents the configuration file used during initialization.
<b>bootflash:</b>	Specifies the location for internal bootflash memory.
<b>log:</b>	Specifies the location for the log file system.
<b>slot0:</b>	Specifies the location for the CompactFlash memory or PCMCIA card.
<b>volatile:</b>	Specifies the location for the volatile file system.
<b>system:</b>	Specifies the location for system memory, which includes the running configuration.
<b>fabric</b>	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 <b>copy running-config startup-config fabric</b> .
<b>tftp:</b>	Specifies the location for a Trivial File Transfer Protocol (TFTP) network server. The syntax for this alias is <b>tftp:[//location]/directory/filename</b> .
<b>ftp:</b>	Specifies the location for a File Transfer Protocol (FTP) network server. The syntax for this alias is <b>ftp:[//location]/directory/filename</b> .
<b>scp:</b>	Specifies the location for a secure copy (scp) network server. The syntax for this alias is <b>scp:[//location]/directory/filename</b> .
<b>sftp:</b>	Specifies the location for a Secure Trivial File Transfer Protocol (SFTP) network server. The syntax for this alias is <b>sftp:[//location]/directory/filename</b> .
<b>log:</b>	Specifies the location for log files stored in the same directory.
<b>debug:</b>	Specifies the location for the debug files stored in the debug partition.
<b>nvram:</b>	Specifies the switch NVRAM.
<b>core:</b>	Specifies the location of the cores from any switching or supervisor module to an external flash (slot 0) or a TFTP server.
<i>filename</i>	The name of the flash file.
<i>sup-1</i>	The number of the supervisor module, where sup-1 is the slot 5 supervisor (active) and sup-2 is the slot 6 supervisor (standby).
<b>sup-2</b>	

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

### Defaults

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 <b>fabric</b> 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
```



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

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
```

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

Related Commands	Command	Description
	<b>cd</b>	Changes the default directory or file system.
	<b>dir</b>	Displays a list of files on a file system.
	<b>reload</b>	Reloads the operating system.
	<b>show version</b>	Displays the version of the running configuration file.

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

## 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	<i>source-URL</i>	The location URL or alias of the source file or directory to be copied.
	<i>destination-URL</i>	The destination URL or alias of the copied file or directory.

The following table lists the aliases for source and destination URLs.

<b>bootflash:</b>	Specifies the location for internal bootflash memory.
<b>slot0:</b>	Specifies the location for the CompactFlash memory or PCMCIA card.
<b>volatile:</b>	Specifies the location for the volatile file system.
<i>filename</i>	Specifies the name of the license file with a.tar extension.

Defaults	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, <b>cd bootflash:</b> ) and verify the available space (for example, <b>dir bootflash:</b> ).
	We recommend backing up your license files immediately after installing them and just before issuing a <b>write erase</b> command.

Examples	The following example saves a file called Enterprise.tar to the bootflash: directory:
	<pre>switch# copy licenses bootflash:/Enterprise.tar Backing up license done</pre>

Related Commands	Command	Description
	<b>cd</b>	Changes the default directory or file system.
	<b>dir</b>	Displays a list of files on a file system.
	<b>install license</b>	Installs a license file.

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

## 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**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	EXEC mode.
----------------------	------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.0(1)	This command was introduced.

<b>Usage Guidelines</b>	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 <b>copy</b> command instead.
-------------------------	--

<b>Examples</b>	The following example copies the contents of the SSM NVRAM to the standby Supervisor 2 module: switch# <b>copy ssm-nvram standby-sup</b>
-----------------	---

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>copy</b>	Saves a backup of the system software.

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

# CRLLookup

To set the CRLLookup, use the **CRLLookup** command. To disable this feature, use the **no** form of the command.

**crlookup attribute-name** *attribute-name* **search-filter** *string* **base-DN** *string*

**no crlookup attribute-name** *attribute-name* **search-filter** *string* **base-DN** *string*

<b>Syntax Description</b>	<b>attribute-name</b>	Specifies LDAP attribute name. The maximum size is 128 characters.
	<i>attribute-name</i>	
	<b>search-filter</b>	Specifies LDAP search filter. The maximum length is 128 characters.
	<i>string</i>	Specifies search map search filter . The maximum length is 128 characters.
	<b>base-DN</b>	Configure base DN to be used for search operation. The Maximum length is 63 characters.
	<i>string</i>	Specifies search map base DN name. The Maximum length is 63 characters.

**Defaults** None.

**Command Modes** Configuration mode.

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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
```

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

**Related Commands**

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

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

## 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*

<b>Syntax Description</b>	<i>trustpoint-label</i>	Specifies the name of the trust point. The maximum size is 64 characters.
<b>Defaults</b>	None.	
<b>Command Modes</b>	Configuration mode.	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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 it 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.

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

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
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAk1O
MRIwEAYDVQQLIExlLYXJuYXRha2ExEjAQBGNVBACTCUJhbmdbbG9yZTEOMAwGA1UE
ChMFQ2lzy28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBGNVBAMTCUFwYXJuYSBD
QTAEFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWVufuZGt1QGNpc2NvLmNvbTELMakGA1UEBhMCSU4xEjAQBGNVBAGTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECXMKbmV0c3RvcnFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHZluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAGiXT2ASFuUOwQ1iDM8rO/41jf8RxxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVROTAQH/BAUwAwEB/zAdBgNVHQ4EFgQUUjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVROfBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYYSUyMENBLmNybdAwoC6gLIYqZmlsZTovL1xccc3N1LTA4XENlcnRFbnJv
bGxcQXBhcm5hJTlwaQ0EuY3JsbGAGCSsGAQQBgjcVAQQDAGEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaNgLh0AFcT0rEyuYt/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
<b>crypto ca trustpoint</b>	Configures the trust point.
<b>show crypto ca certificates</b>	Displays configured trust point certificates.
<b>show crypto ca trustpoints</b>	Displays trust point configurations.



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

## 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*

<b>Syntax Description</b>	<i>trustpoint-label</i>	Specifies the name of the trust point. The maximum size is 64 characters.
	<i>source-file</i>	Specifies the location of the CRL in the form <b>bootflash:filename</b> . The maximum size is 512.

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

<b>Command Modes</b>	Configuration mode.
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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.

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

---

**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
<b>revocation-check</b>	Configures trust point revocation check methods.
<b>show crypto ca crl</b>	Displays configured certificate revocation lists (CRL).

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

## 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	<i>trustpoint-label</i>	Specifies the name of the trust point. The maximum size is 64 characters.
--------------------	-------------------------	---

Defaults	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
```

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

```

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-----
MIIBQzCCARQCAQAwHDEaMBGGA1UEAxMRVnVnYXNjby5jb20wgZ8wDQYJ
KoZIHvcNAQEBAQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxBLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVksCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCsQGSib3DQEJ
DjEpMccwJQYDVVR0RAQH/BBswGYIRVnVnYXNjby5jb22HBKwWH6IwDQYJ
KoZIHvcNAQEBAQADgYEAKT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6U188nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----

```

#### Related Commands

Command	Description
<b>crypto ca import trustpoint-label certificate</b>	Imports the identity certificate obtained from the CA to the trust point.
<b>crypto key generate rsa</b>	Generates an RSA key pair.
<b>rsa keypair</b>	Configures and associates the RSA key pair details to a trust point.
<b>show crypto key mypubkey rsa</b>	Displays all RSA public key configurations.

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

## 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 export***trustpoint-label pkcs12 destination-file-url pkcs12-password*

Syntax Description		
<i>trustpoint-label</i>		Specifies the name of the trust point. The maximum size is 64 characters.
<b>pkcs12</b> <i>destination-file-url</i>		Specifies a destination file in <b>bootflash:filename</b> format. The maximum size is 512 characters.
<i>pkcs12-password</i>		Specifies the password to be used to protect the RSA private key in the exported file. The maximum size is 64 characters.

**Defaults** 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
	<b>crypto ca import</b> <i>trustpoint-label</i> <b>certificate</b>	Imports the identity certificate obtained from the CA to the trust point.
	<b>crypto ca import</b> <i>trustpoint-label</i> <b>pkcs12</b>	Imports the identity certificate and associated RSA key pair and CA certificate (chain) to a trust point.
	<b>crypto key generate</b> <b>rsa</b>	Generates an RSA key pair.

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

Command	Description
<b>rsakeypair</b>	Configures and associates the RSA key pair details to a trust point.
<b>show crypto key mypubkey rsa</b>	Displays any RSA public key configurations.

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

## 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

<i>trustpoint-label</i>	Specifies the name of the trust point. The maximum size is 64 characters.
<b>pkcs12</b> <i>source-file-url</i>	Specifies a source file in <b>bootflash:filename</b> format. The maximum size is 512 characters.
<i>pkcs12-password</i>	Specifies the password that was used to protect the RSA private key in the imported PKCS#12 file. The maximum size is 64 characters.

### Defaults

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 certificate and associated RSA key pair and CA certificate or certificate 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.

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

### 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-----
MIEADCCA6qgAwIBAgIKCj00oQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIB3DQEJARYRYW1hbmRrZUBjaXNjb5jb20xCzAJBgNVBAYTAklOMRIwEAYD
VQQIEw1LYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdbhG9yZTEOMAwGA1UEChMFQ21z
Y28xEzARBgNVBAStCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTEeMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBWxGjAYBgNVBAMTEVZlZ2FzLTlEu
Y21zY28uY29tMIGfMA0GCSqGSIB3DQEBAAQAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjkJSICdpLfK5eJSmNCQujGpzcKsZPFxjF2UoiyeCYE8y1ncWyw5E08rJ47
glxr42/si9IRib/8udU/cj9jSSfKK56koa7xWYA8rDfz8jMCnIM4WlaY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMTMS5jaXNjb5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMGcgQwgcGAFCCo8kaDG6wjTEVNjskYUBoLFmxoYGW
pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWVfZGt1QGNpc2NvLmNvbTELMakGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFRYTEtESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDaXNjbzETMBEGA1UECXMkbnV0c3RvcnFnZTESMBAGA1UEAxMjQXBh
cm5hIEENBghAFYNKJrLQZ1E9JEiWMrR16MGsGA1UdHwRkMGiWlQAsOCqGKGh0dHA6
Ly9zc2UtMDgvdQ2VydeVucm9sbC9BcGFybmElmJBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDcBbigYIKwYBBQUH
AQEEfjB8MDSGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRFbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNyda9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XENlcnRFbnJvbGwvc3NlLTA4X0FwYXJuYSUyMENBLmNydaDANBgkqhkiG9w0BAQUF
AANBAdBgGBSbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
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
<b>crypto ca enroll</b>	Generates a certificate signing request for a trust point.
<b>crypto ca export trustpoint-label pkcs12</b>	Exports the RSA key pair and associated certificates of a trust point.
<b>crypto key generate rsa</b>	Generates the RSA key pair.
<b>rsa keypair</b>	Configures trust point RSA key pair details.
<b>show crypto ca certificates</b>	Displays the identity and CA certificate details.
<b>show crypto key mypubkey rsa</b>	Displays any RSA public key configurations.



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

## 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	<i>certificate-file</i>	Specifies the certificate filename in the form <b>bootflash:filename</b> . The maximum size is 512 characters.
--------------------	-------------------------	--

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

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

Command History	Release	Modification
	3.0(1)	This command was introduced.

Usage Guidelines	The <b>crypto ca test verify</b> 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	<p>The following example shows how to verify a certificate file. Verify status code 0 means the verification is successful.</p> <pre>switch(config)# <b>crypto ca test verify bootflash:id1.pem</b> verify status oode:0 verify error msg:</pre>
----------	--

Related Commands	Command	Description
	<b>show crypto ca certificates</b>	Displays configured trust point certificates.

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

## crypto ca lookup

To configure the type of certstore that PKI will use for authentication, use the **crypto ca lookup** command in configuration mode. To disable this feature, use the **no** form of the command.

**crypto ca lookup** { **both** | **local** | **remote** }

Syntax Description	<b>both</b>	Specifies both local and remote certstore.
	<b>local</b>	Specifies local certstore.
	<b>remote</b>	Specifies remote certstore.

**Defaults** 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
	<b>show crypto ssh-auth-map</b>	displays mapping filters applied for SSH authentication.

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

## 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		
<b>crl-refresh-time</b>		Specifies timer to fetch crl from remote certstore.
<i>hours</i>		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.
<b>server-group</b>		Specifies LDAP server group.
<i>group-name</i>		Specifies LDAP server group name. The maximum size is 64 characters.

**Defaults** 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
	<b>show crypto ssh-auth-map</b>	displays mapping filters applied for SSH authentication.

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

## 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*

<b>Syntax Description</b>	<i>trustpoint-label</i>	Specifies the name of the trust point. The maximum size is 64 characters.
---------------------------	-------------------------	---

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

<b>Command Modes</b>	Configuration mode.
----------------------	---------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.0(1)	This command was introduced.

<b>Usage Guidelines</b>	<p>Trust points have the following characteristics:</p> <ul style="list-style-type: none"> <li>• A trust point corresponds to a single CA, which an MDS switch trusts for peer certificate verification for any application.</li> <li>• A CA must be explicitly associated to a trust point using the CA authentication process using the <b>crypto ca authenticate</b> command.</li> <li>• 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.</li> <li>• A trust point is not restricted to a specific application.</li> <li>• The MDS switch can optionally enroll with a trust point CA to get an indemnity certificate for itself.</li> </ul> <p>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.</p> <p>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.</p>
-------------------------	--

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

**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
<b>crypto ca authenticate</b>	Authenticates the certificate of the certificate authority.
<b>crypto ca enroll</b>	Generates a certificate signing request for a trust point.
<b>show crypto ca certificates</b>	Displays the identity and CA certificate details.
<b>show crypto ca trustpoints</b>	Displays trust point configurations.

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

## 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*

<b>Syntax Description</b>	<i>mapname</i> Specifies the name of the filter map. The maximum size is 64 characters.				
<b>Defaults</b>	None.				
<b>Command Modes</b>	Configuration mode.				
<b>Command History</b>	<table> <tr> <th>Release</th><th>Modification</th></tr> <tr> <td>NX-OS 5.0(1a)</td><td>This command was introduced.</td></tr> </table>	Release	Modification	NX-OS 5.0(1a)	This command was introduced.
Release	Modification				
NX-OS 5.0(1a)	This command was introduced.				
<b>Usage Guidelines</b>	None.				
<b>Examples</b>	<p>The following example shows how to display mapping filters applied for SSH authentication:</p> <pre>switch(config)# <b>crypto certificatemap mapname map1</b> switch(config-certmap-filter)#</pre>				
<b>Related Commands</b>	<table> <tr> <th>Command</th><th>Description</th></tr> <tr> <td><b>show crypto ssh-auth-map</b></td><td>displays mapping filters applied for SSH authentication.</td></tr> </table>	Command	Description	<b>show crypto ssh-auth-map</b>	displays mapping filters applied for SSH authentication.
Command	Description				
<b>show crypto ssh-auth-map</b>	displays mapping filters applied for SSH authentication.				

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

## 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.

Defaults	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
	<b>show crypto ssh-auth-map</b>	displays mapping filters applied for SSH authentication.

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

# 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

<b>gigabytes</b> <i>number</i>	Specifies a volume-based key duration in gigabytes. The range is 1 to 4095.
<b>kilobytes</b> <i>number</i>	Specifies a volume-based key duration in kilobytes. The range is 2560 to 2147483647.
<b>megabytes</b> <i>number</i>	Specifies a volume-based key duration in megabytes. The range is 3 to 4193280.
<b>seconds</b> <i>number</i>	Specifies a time-based key duration in seconds. The range is 120 to 86400.

## Defaults

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
<b>crypto ipsec enable</b>	Enables IPsec.
<b>set (IPsec crypto map configuration submode)</b>	Configures IPsec crypto map entry parameters.
<b>show crypto global domain ipsec</b>	Displays the global attributes for IPsec.



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

## crypto ike domain ipsec

To enter IKE configuration submode, use the **crypto ike domain ipsec** command.

**crypto ike domain ipsec**

<b>Syntax Description</b>	This command has no other arguments or keywords.
---------------------------	--

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

<b>Command Modes</b>	Configuration mode.
----------------------	---------------------

Command History	Release	Modification
	2.0(x)	This command was introduced.

<b>Usage Guidelines</b>	To configure IKE protocol attributes, IKE must be enabled using the <b>crypto ike enable</b> 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.

<b>Examples</b>	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
	<b>crypto ike enable</b>	Enables the IKE protocol.
	<b>show crypto ike domain ipsec</b>	Displays IKE information for the IPsec domain.

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

## 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	<i>sa-index</i>	Specifies the SA index. The range is 1 to 2147483647.
--------------------	-----------------	---

Defaults	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 <b>crypto ike enable</b> command.
 <b>Note</b>	This command is not supported on the Cisco MDS 9124 switch.

Examples	The following example rekeys an IKE crypto SA:  switch# <b>crypto ike domain ipsec rekey sa 100</b>
----------	---

Related Commands	Command	Description
	<b>crypto ike enable</b>	Enables the IKE protocol.
	<b>show crypto ike domain ipsec</b>	Displays IKE information for the IPsec domain.

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

## 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.

### Defaults

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.

### Examples

The following example shows how to enable the IKE protocol:

```
switch# config terminal
switch(config)# crypto ike enable
```

### Related Commands

Command	Description
<b>clear crypto ike domain ipsec sa</b>	Clears IKE protocol information clear IKE SAs.
<b>crypto ipsec enable</b>	Enables IPsec.
<b>show crypto ike domain ipsec</b>	Displays IKE information for the IPsec domain.

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

# 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.

## Defaults

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
<b>show crypto global domain ipsec</b>	Displays IPsec crypto global information.
<b>show crypto map domain ipsec</b>	Displays IPsec crypto map information.
<b>show crypto transform-set domain ipsec</b>	Displays IPsec crypto transform set information.

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

## 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	<b>label</b> <i>key-pair-label</i>	(Optional) Specifies the name of the key pair. The maximum size is 64 characters.
	<b>exportable</b>	(Optional) Configures the key pair to be exportable.
	<b>modulus</b> <i>key-pair-size</i>	(Optional) Specifies the size of the key pair. The size ranges from 512 to 2048.

Defaults	By default, the <b>key</b> is not exportable. The default <b>label</b> is switch FQDN. The default <b>modulus</b> is 512.
----------	---

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

Command History	<b>Release</b>	<b>Modification</b>
	3.0(1)	This command was introduced.

Usage Guidelines	<p>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.</p> <p>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.</p> <p>You can also configure an RSA key pair label. The default key pair label is FQDN.</p>
------------------	---

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
```

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

Related Commands	Command	Description
	crypto key zeroize rsa	Deletes RSA key pair configurations.
	rsa keypair	Configures trust point RSA key pair details.
	show crypto key mypubkey rsa	Displays information about configured RSA key pairs.

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

## 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

<i>key-pair-label</i>	Specifies the RSA key pair to delete. The maximum size is 64 characters.
-----------------------	--

### Defaults

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
```

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

Related Commands	Command	Description
	crypto key generate rsa	Configures an RSA key pair.
	rsa keypair	Configures trust point RSA key pair details.
	show crypto key mypubkey rsa	Displays information about configured RSA key pairs.



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

## 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

<i>map-name</i>	Specifies the map name. Maximum length is 63 characters.
<i>seq-number</i>	(Optional) Specifies the sequence number for the map entry. The range is 1 to 65535.

### Defaults

None.

### Command Modes

Configuration mode.

### Command History

Release	Modification
2.0(x)	This command was introduced.

### Usage Guidelines

To use this command, IPsec must be enabled using the **crypto ipsec enable** command.  
The sequence number determines the order in which IPsec crypto map entries are applied.

### Examples

The following example specifies entry 1 for IPsec crypto map IPsecMap and enters IPsec crypto map configuration mode:

```
switch# config terminal
switch(config)# crypto map domain ipsec IPsecMap 1
switch(config-crypto-map-ip)#
```

The following example deletes an IPsec crypto map entry:

```
switch# config terminal
switch(config)# no crypto map domain ipsec IPsecMap 1
```

The following example deletes the entire IPsec crypto map:

```
switch# config terminal
switch(config)# no crypto map domain ipsec IPsecMap
```

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

Related Commands	Command	Description
	crypto ipsec enable	Enables IPsec.
	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.

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

## 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

<i>map-name</i>	Specifies the map name. Maximum length is 63 characters.
-----------------	--

### Defaults

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
<b>crypto ipsec enable</b>	Enables IPsec.
<b>show crypto map domain ipsec</b>	Displays IPsec crypto map information.
<b>show interface</b>	Displays interface information.

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

## 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

<i>set-name</i>	Specifies the transform set name. Maximum length is 63 characters.
<b>esp-3des</b>	Specifies ESP transform using the 3DES cipher (128 bits).
<b>esp-des</b>	Specifies ESP transform using the DES cipher (56 bits).
<b>esp-aes-xcbc-mac</b>	Specifies ESP transform using AES-XCBC-MAC authentication.
<b>esp-md5-hmac</b>	Specifies ESP transform using MD5-HMAC authentication.
<b>esp-sha1-hmac</b>	Specifies ESP transform using SHA1-HMAC authentication.
<b>esp-aes</b>	Specifies ESP transform using the AES cipher (128 or 256 bits).
<b>128</b>	Specifies ESP transform using AES 128-bit cipher.
<b>256</b>	Specifies ESP transform using AES 256-bit cipher.
<b>ctr</b>	Specifies AES in counter mode.

### Defaults

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.

### 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.

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

### 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
<b>clear crypto sa domain ipsec</b>	Clears security associations.
<b>crypto ipsec enable</b>	Enables IPsec.
<b>show crypto transform-set domain ipsec</b>	Displays IPsec crypto transform set information.

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

## 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-id** *customer-id*

Syntax Description	<i>customer-id</i>	Specifies the customer ID. The maximum length is 64 alphanumeric characters in free format.
--------------------	--------------------	---

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

Command Modes	Call Home configuration submode.
---------------	----------------------------------

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

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

Examples	<p>The following example shows how to configure the customer ID in the Call Home configuration submode:</p> <pre>switch# <b>config terminal</b> Enter configuration commands, one per line. End with CNTL/Z. switch(config)# <b>callhome</b> switch(config-callhome)# <b>customer-id Customer1234</b></pre>
----------	---

Related Commands	Command	Description
	<b>callhome</b>	Configures the Call Home function.
	<b>callhome test</b>	Sends a dummy test message to the configured destination(s).
	<b>show callhome</b>	Displays configured Call Home information.