

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



## CHAPTER 5

# D 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. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

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

## data-pattern-file

To configure data pattern file for a SAN tuner extension N port, use the **data-pattern-file** command in interface configuration submode. To remove data pattern file, use the **no** form of the command.

**data-pattern-file** *filename*

**no data-pattern-file**

<b>Syntax Description</b>	<i>filename</i>	Specifies the data pattern file name.
---------------------------	-----------------	---------------------------------------

<b>Defaults</b>	All zero pattern.
-----------------	-------------------

<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>	By default, an all-zero pattern is used as the pattern for data generated by the virtual N ports. You can optionally specify a file as the data pattern to be generated by selecting a data pattern file from one of three locations: the bootflash: directory, the volatile: directory, or the slot0: directory. This option is especially useful when testing compression over FCIP links. You can also use Canterbury corpus or artificial corpus files for benchmarking purposes.
-------------------------	---

<b>Examples</b>	The following example configures the data pattern file for an N port:
-----------------	---

```
switch# san-ext-tuner
switch(san-ext)# nwwn 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
switch(san-ext-nport)# data-pattern-file bootflash://DataPatternFile
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	nport pwwn	Configures SAN extension tuner N port pWWNs.
	san-ext-tuner	Enters SAN extension tuner configuration mode.
	show san-ext-tuner	Displays SAN extension tuner information.

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

## deadtime (radius group configuration)

To configure a periodic time interval where a nonreachable (nonresponsive) RADIUS server is monitored for responsiveness, use the **deadtime** command in RADIUS group configuration submode. To disable the monitoring of the nonresponsive server, use the **no** form of the command.

**deadtime** *time*

**no deadtime** *time*

<b>Syntax Description</b>	<i>time</i>	Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.
---------------------------	-------------	--

<b>Defaults</b>	Zero.
-----------------	-------

<b>Command Modes</b>	RADIUS group configuration submode.
----------------------	-------------------------------------

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

<b>Usage Guidelines</b>	<p>If the dead time interval for an individual RADIUS server is greater than zero (0), that value takes precedence over the value set for the server group.</p> <p>When the dead time interval is 0 minutes, RADIUS server monitoring is not performed unless the RADIUS server is part of a server group and the dead time interval for the group is greater than 0 minutes.</p>
-------------------------	---

<b>Examples</b>	The following example shows the <b>deadtime</b> command in RADIUS group configuration submode.
-----------------	--

```
switch# config terminal
switch(config)# aaa group server radius testgroup
switch(config-radius)# deadtime 10
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>radius-server deadtime</b>	Sets a time interval for monitoring a nonresponsive RADIUS server.
	<b>show radius-server</b>	Displays RADIUS server information.

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

## deadtime (tacacs+ group configuration)

To configure a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness, use the **deadtime** command in TACACS+ group configuration submode. To disable the monitoring of the nonresponsive server, use the **no** form of the command.

**deadtime** *time*

**no deadtime** *time*

### Syntax Description

<i>time</i>	Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.
-------------	--

### Defaults

Zero.

### Command Modes

TACACS+ group configuration submode.

### Command History

Release	Modification
3.0(1)	This command was introduced.

### Usage Guidelines

If the dead time interval for an individual TACACS+ server is greater than zero (0), that value takes precedence over the value set for the server group.

When the dead time interval is 0 minutes, TACACS+ server monitoring is not performed unless the TACACS+ server is part of a server group and the dead time interval for the group is greater than 0 minutes.

### Examples

The following example shows the **deadtime** command in TACACS+ group configuration submode.

```
switch# config terminal
switch(config)# aaa group server tacacs mygroup
switch(config-tacacs)# deadtime 5
```

### Related Commands

Command	Description
<b>tacacs-server</b>	Sets a time interval for monitoring a nonresponsive TACACS+ server.
<b>deadtime</b>	
<b>show tacacs-server</b>	Displays TACACS+ server information.

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

# delete

To delete a specified file or directory on a Flash memory device, use the **delete** command in EXEC mode.

```
delete { bootflash:filename | debug:filename | log:filename | modflash:filename | slot0:filename
        | volatile:filename }
```

## Syntax Description

<b>bootflash:</b>	Flash image that resides on the supervisor module.
<b>debug:</b>	Contains the debug files.
<b>log:</b>	Contains the two default logfiles. The file dmesg contains the kernel log-messages and the file messages contains the system application log-messages.
<b>modflash:</b>	Flash image that resides on a module.
<b>slot0:</b>	Flash image that resides on another module.
<b>volatile:</b>	Flash image that resides on the volatile file system.
<b>filename</b>	The name of the file to be deleted.

## Defaults

None.

## Command Modes

EXEC mode.

## Command History

Release	Modification
1.0(2)	This command was introduced.
2.1(1a)	Added <b>debug</b> , <b>log</b> , and <b>modflash</b> keywords.

## Usage Guidelines

When you delete a file, the software erases the file.

If you attempt to delete the configuration file or image specified by the CONFIG\_FILE or BOOTLDR environment variable, the system prompts you to confirm the deletion. Also, if you attempt to delete the last valid system image specified in the BOOT environment variable, the system prompts you to confirm the deletion.



### Caution

If you specify a directory, the **delete** command deletes the entire directory and all its contents.

## Examples

The following example deletes the file named test from the Flash card inserted in slot 0.

```
switch# delete slot0:test
Delete slot0:test? [confirm]
```

The following example deletes a file from a directory.

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

```
switch# delete dns_config.cfg
```

The following example deletes a file from an external CompactFlash (slot0).

```
switch# delete slot0:dns_config.cfg
```

The following example deletes the entire `my-dir` directory and all its contents:

```
switch# delete bootflash:my-dir
```

The following example deletes the entire user created `dk` log file on the active supervisor:

```
switch# delete log://sup-active/
log://sup-active/dk          log://sup-active/dmesg          log://sup-active/messages
switch# delete log://sup-active/dk
switch# dir log:
      31      Feb 04 18:22:03 2005  dmesg
  14223      Feb 04 18:25:30 2005  messages
```

Usage for log://sup-local

```
  35393536 bytes used
  174321664 bytes free
  209715200 bytes total
```

```
switch#
```

### Related Commands

Command	Description
<b>cd</b>	Changes the default directory or file system.
<b>dir</b>	Displays a list of files on a file system.
<b>show boot</b>	Displays the contents of the BOOT environment variable, the name of the configuration file pointed to by the CONFIG_FILE environment variable, the contents of the BOOTLDR environment variable, and the configuration register setting.

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

## delete ca-certificate

To delete certificate authority certificates, use the **delete ca-certificate** command in trust point configuration submode.

**delete ca-certificate**

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

**Defaults** None.

**Command Modes** Trust point configuration submode.

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

**Usage Guidelines** This command deletes the CA certificate or certificate chain corresponding to the trust point CA. As a result, the trust point CA is no longer trusted. If there is an identity certificate from the CA, you should delete it before attempting to delete the CA certificate. Doing so prevents the accidental deletion of a CA certificate when you have not yet deleted the identity certificate from that CA. This action may be necessary when you do not want to trust the CA any more for a reason such as the CA is compromised or the CA certificate is already expired, with the latter being a very rare event.



**Note**

The trust point configuration, certificates, and key pair configurations are made persistent only after saving to the startup configuration. To be consistent with this configuration behavior, the delete behavior is also the same. That is, the deletions are made persistent only after saving to the startup configuration.

Use the **copy running-config startup-config** command to make the certificate and key pair deletions persistent.

**Examples** The following example shows how to delete a certificate authority certificate.

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete ca-certificate
```

Related Commands	Command	Description
	<b>delete certificate</b>	Deletes the identity certificate.
	<b>delete crl</b>	Deletes the crl from the trustpoint.

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

## delete certificate

To delete the identity certificate, use the **delete certificate** command in trust point configuration submode.

**delete certificate [force]**

<b>Syntax Description</b>	<b>force</b>	Forces the deletion of the identity certificate.
<b>Defaults</b>	None.	
<b>Command Modes</b>	Trust point configuration submode.	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.0(1)	This command was introduced.

### Usage Guidelines

Use this command to delete the identity certificate from the trust point CA. This action may be necessary when the identity certificate expires or the corresponding key pair is compromised. Applications will be left without any identity certificate to use after the deletion of the last or the only identity certificate present. Accordingly, an error message is generated if the certificate being deleted is the last or only identity certificate present. If needed, the deletion can still be accomplished by forcing it using the force option.



#### Note

The trust point configuration, certificates, and key pair configurations are made persistent only after saving to the startup configuration. To be consistent with this configuration behavior, the delete behavior is also the same. That is, the deletions are made persistent only after saving to the startup configuration.

Use the **copy running-config startup-config** command to make the certificate and key pair deletions persistent.

### Examples

The following example shows how to delete the identity certificate.

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete certificate
```

The following example shows how to force the deletion of the identity certificate.

```
switch(config-trustpoint)# delete certificate force
```



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

Related Commands	Command	Description
	<b>delete ca-certificate</b>	Deletes the certificate authority certificate.
	delete crl	Deletes the crl from the trustpoint.

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

## delete crl

To delete the crl from the trustpoint, use the **delete crl** command in trust point configuration submode.

**delete crl**

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

**Defaults** None.

**Command Modes** Trust point configuration submode.

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

**Usage Guidelines** None.

**Examples** The following example shows how to delete the crl from the trustpoint.

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete crl
```

Related Commands	Command	Description
	<b>delete ca-certificate</b>	Deletes the certificate authority certificate.
	<b>delete certificate</b>	Deletes the identity certificate.

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

## deny (IPv6-ACL configuration)

To configure deny conditions for an IPv6 access control list (ACL), use the **deny** command in IPv6-ACL configuration submode. To remove the conditions, use the **no** form of the command.

```
deny {ipv6-protocol-number | ipv6}
    {source-ipv6-prefix/prefix-length | any | host source-ipv6-address}
    {dest-ipv6-prefix/prefix-length | any | host dest-ipv6-address}
    [log-deny]
```

```
deny icmp
    {source-ipv6-prefix/prefix-length | any | host source-ipv6-address}
    {dest-ipv6-prefix/prefix-length | any | host dest-ipv6-address}
    [icmp-type [icmp-code]]
    [log-deny]
```

```
deny tcp
    {source-ipv6-prefix/prefix-length | any | host source-ipv6-address}
    [source-port-operator source-port-number |
range source-port-number source-port-number]
    {dest-ipv6-prefix/prefix-length | any | host dest-ipv6-address}
    [dest-port-operator dest-port-number |
range dest-port-number dest-port-number]
    [established] [log-deny]
```

```
deny udp
    {source-ipv6-prefix/prefix-length | any | host source-ipv6-address}
    [source-port-operator source-port-number |
range source-port-number source-port-number]
    {dest-ipv6-prefix/prefix-length | any | host dest-ipv6-address}
    [dest-port-operator dest-port-number |
range dest-port-number dest-port-number]
    [log-deny]
```

```
no deny {ipv6-protocol-number | ipv6 | icmp | tcp | udp}
```

### Syntax Description

<i>ipv6-protocol-number</i>	Specifies an IPv6 protocol number. The range is 0 to 255.
<b>ipv6</b>	Applies the ACL to any IPv6 packet.
<i>source-ipv6-prefix/prefix-length</i>	Specifies a source IPv6 network or class of networks. The format is <i>X:X:X::X/n</i> .
<b>any</b>	Applies the ACL to any source or destination prefix.
<b>host</b> <i>source-ipv6-address</i>	Applies the ACL to the specified source IPv6 host address. The format is <i>X:X:X::X</i> .
<i>dest-ipv6-prefix/prefix-length</i>	Specifies a destination IPv6 network or class of networks. The format is <i>X:X:X::X/n</i> .
<b>host</b> <i>dest-ipv6-address</i>	Applies the ACL to the specified destination IPv6 host address. The format is <i>X:X:X::X</i> .
<b>log-deny</b>	For packets that are dropped, creates an informational log message about the packet that matches the entry. The message includes the input interface.

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

<code>icmp</code>	Applies the ACL to any Internet Control Message Protocol (ICMP) packet.
<code>icmp-type</code>	Specifies an ICMP message type. The range is 0 to 255.
<code>icmp-code</code>	Specifies an ICMP message code. The range is 0 255.
<code>tcp</code>	Applies the ACL to any TCP packet.
<code>source-port-operator</code>	Specifies an operand that compares the source ports of the specified protocol. The operands are <b>lt</b> (less than), <b>gt</b> (greater than), and <b>eq</b> (equals).
<code>source-port-number</code>	Specifies the port number of a TCP or UDP port. The number can be from 0 to 65535. A range requires two port numbers.
<code>udp</code>	Applies the ACL to any UDP packet.
<code>dest-port-operator</code>	Specifies an operand that compares the destination ports of the specified protocol. The operands are <b>lt</b> (less than), <b>gt</b> (greater than), and <b>eq</b> (equals).
<code>dest-port-number</code>	Specifies the port number of a TCP or UDP port. The number can be from 0 to 65535. A range requires two port numbers.
<code>range</code>	Specifies a range of ports to compare for the specified protocol.
<code>established</code>	Indicates an established connection, which is defined as a packet whose SYN flag is not set.

#### Defaults

None.

#### Command Modes

IPv6-ACL configuration submode.

#### Command History

Release	Modification
3.0(1)	This command was introduced.

#### Usage Guidelines

The following guidelines can assist you in configuring an IPv6-ACL. For complete information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

- You can apply IPv6-ACLs to VSAN interfaces, the management interface, Gigabit Ethernet interfaces on IPS modules and MPS-14/2 modules, and Ethernet PortChannel interfaces. However, if IPv6-ACLs are already configured in a Gigabit Ethernet interface, you cannot add this interface to a Ethernet PortChannel group.



#### Caution

Do not apply IPv6-ACLs to just one member of a PortChannel group. Apply IPv6-ACLs to the entire channel group.

- Use only the TCP or ICMP options when configuring IPv6-ACLs on Gigabit Ethernet interfaces.
- Configure the order of conditions accurately. Because the IPv6-ACL filters are applied sequentially to the IP flows, the first match determines the action taken. Subsequent matches are not considered. Be sure to configure the most important condition first. If no conditions match, the software drops the packet.

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

### Examples

The following example configures an IPv6-ACL called List1, enters IPv6-ACL submode, and adds an entry to deny TCP traffic from any source address to any destination address.

```
switch# config terminal
switch(config)# ipv6 access-list List1
switch(config-ipv6-acl)# deny tcp any any
```

The following example removes a deny condition set for any destination prefix on a specified UDP host.

```
switch# config terminal
switch(config)# ipv6 access-list List1
switch(config-ipv6-acl)# no deny udp host 2001:db8:200d::4000 any
```

The following example removes the IPv6-ACL called List1 and all its entries.

```
switch# config terminal
switch(config)# no ipv6 access-list List1
```

### Related Commands

Command	Description
<b>ipv6 access-list</b>	Configures an IPv6 ACL and enters IPv6-ACL configuration submode.
<b>permit</b>	Configures permit conditions for an IPv6 ACL.

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

## destination interface

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

```
destination interface {fc slot/port | fc-tunnel tunnel-id}
```

```
no destination interface {fc slot/port | fc-tunnel tunnel-id}
```

### Syntax Description

<b>fc slot/port</b>	Specifies the Fibre Channel interface ID at a slot and port.
<b>fc-tunnel tunnel-id</b>	Specifies the Fibre Channel tunnel interface ID.

### Defaults

Disabled.

### Command Modes

SPAN session configuration submode.

### Command History

Release	Modification
1.0(2)	This command was introduced.
1.2(1)	Added the <b>fc-tunnel</b> parameter.

### Usage Guidelines

The SPAN destination interface must be configured as SPAN destination port (SD port) mode using the **switchport** command before the interface can be associated with SPAN session as a destination interface.

### Examples

The following example shows how to configure an interface as a SPAN destination port (SD port), create a SPAN session, and then configure the interface fc3/13 as the SPAN destination interface.

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface fc3/13
switch(config-if)# switchport mode sd
switch(config)# span session 1
switch(config-span)# destination interface fc3/13
switch(config-span)# do show span session 1
switch(config-span)# show span session 1
Session 1 (inactive as destination is down)
  Destination is fc3/13
  No session filters configured
  No ingress (rx) sources
  No egress (tx) sources

switch(config-span)#
```

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

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>switchport</b>	Configures the switchport mode on the Fibre Channel interface.
	<b>span session</b>	Selects or configures the SPAN session and changes to SPAN configuration submode.
	<b>source</b>	Configures a SPAN source.
	<b>suspend</b>	Suspends a SPAN session.
	<b>show span session</b>	Displays specific information about a SPAN session

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

## destination-profile

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

```
destination-profile {profile-name | full-txt-destination | short-txt-destination | xml-destination}
  {alert-group {all | avanti | cisco-tac | environmental | inventory | license |
linecard-hardware | rmon | supervisor-hardware | syslog-group-port | system | test}}
```

```
no destination-profile {profile-name | full-txt-destination | short-txt-destination |
xml-destination} {alert-group {all | avanti | cisco-tac | environmental | inventory | license |
linecard-hardware | rmon | supervisor-hardware | syslog-group-port | system | test}}
```

### Syntax Description

<i>profile-name</i>	Specifies a user-defined user profile with a maximum of 32 alphanumeric characters.
<b>full-txt-destination</b>	Configures destination profile for plain text message.
<b>short-txt-destination</b>	(Optional) Configures a destination for a short text message.
<b>xml-destination</b>	(Optional) Configures destination profile for XML message.
<b>alert-group</b>	Specifies one or more of the alert groups
<b>all</b>	Specifies an alert group consisting of all Call Home messages.
<b>avanti</b>	Specifies an alert group consisting of events that are meant only for Avanti.
<b>cisco-tac</b>	Specifies an alert group consisting of events that are meant only for Cisco TAC.
<b>environmental</b>	Specifies an alert group consisting of power, fan, temperature-related events.
<b>inventory</b>	Specifies an alert group consisting of inventory status events.
<b>license</b>	Specifies an alert group consisting of license status events.
<b>linecard-hardware</b>	Specifies an alert group consisting of module-related events.
<b>rmon</b>	Specifies an alert group consisting of RMON status events.
<b>supervisor-hardware</b>	Specifies an alert group consisting of supervisor related events.
<b>syslog-port-group</b>	Specifies an alert group consisting of syslog port group status events.
<b>system</b>	Specifies an alert group consisting of software related events.
<b>test</b>	Specifies an alert group consisting of user-generated test events.

### Defaults

None.

### Command Modes

Call Home configuration submode.

### Command History

Release	Modification
1.0(2)	This command was introduced.



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

**Usage Guidelines**      None.

**Examples**              The following example configures full-text destination profiles.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# destination-profile full-txt-destination email-addr person@place.com
switch(config-callhome)# destination-profile full-txt-destination message-size 1000000
```

The following example configures short-text destination profiles.

```
switch(config-callhome)# destination-profile short-txt-destination email-addr person@place.com
switch(config-callhome)# destination-profile short-txt-destination message-size 100000
```

**Related Commands**

Command	Description
<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)

## device-alias (IVR fcdomain database configuration submode)

To map a device alias to a persistent FC ID for IVR, use the **device-alias** command in IVR fcdomain database configuration submode. To remove the mapping for the device alias, use the **no** form of the command.

**device-alias** *device-name fc-id*

**no device-alias** *device-name*

Syntax Description		
	<i>device-name</i>	Specifies the device name. Maximum length is 64 characters.
	<i>fc-id</i>	Specifies the FC ID for the device.

**Defaults** None.

**Command Modes** IVR fcdomain database configuration submode.

Command History	Release	Modification
	2.1(2)	This command was introduced.

**Usage Guidelines** Only one FC ID can be mapped to a device alias.

**Examples** The following example shows how to map the device alias to the persistent FC ID.

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# native-autonomous-fabric-num 20 native-vsan 30 domain 15
switch(config-fcdomain-fcid)# device-alias SampleName 0x123456
```

The following example shows how to remove the mapping between the device alias and the FC ID.

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# native-autonomous-fabric-num 20 native-vsan 30 domain 15
switch(config-fcdomain-fcid)# no device-alias SampleName
```

Related Commands	Command	Description
	<b>ivr fcdomain database autonomous-fabric-num</b>	Creates IVR persistent FC IDs.
	<b>native-autonomous-fabric-num</b>	Creates an IVR persistent FC ID database entry.
	<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)

## device-alias (SDV virtual device configuration submode)

To add a device alias to a virtual device, use the **device-alias** command in SDV virtual device configuration submode. To remove a device alias, use the **no** form of the command.

**device-alias** *device-name* [**primary**]

**no device-alias** *device-name* [**primary**]

Syntax	Description
<i>device-name</i>	Specifies the device name. Maximum length is 64 characters.
<b>primary</b>	Specifies the device as a primary device.

**Defaults** None.

**Command Modes** SDV virtual device configuration submode.

Command History	Release	Modification
	3.1(2)	This command was introduced.

**Usage Guidelines** None.

**Examples** The following example shows how to configure a virtual target alias name and how to

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# sdv virtual-device name sql vsan 1
switch(config-sdv-virt-dev)# device-alias group1 primary
```

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

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

## device-alias abort

To discard a Distributed Device Alias Services (device alias) Cisco Fabric Services (CFS) distribution session in progress, use the **device-alias abort** command in **configuration mode**.

### device-alias abort

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

**Defaults** None.

**Command Modes** Configuration mode.

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

**Usage Guidelines** None.

**Examples** The following example shows how to discard a device alias CFS distribution session in progress.

```
switch# config terminal
switch(config)# device-alias abort
```

Related Commands	Command	Description
	<b>device-alias database</b>	Configures and activates the device alias database.
	<b>device-alias distribute</b>	Enables CFS distribution for device aliases.
	<b>show device-alias</b>	Displays device alias information.

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

## device-alias commit

To apply the pending configuration pertaining to the Distributed Device Alias Services (device alias) Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **device-alias commit** command in configuration mode.

**device-alias commit**

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

**Defaults** None.

**Command Modes** Configuration mode.

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

**Usage Guidelines** None.

**Examples** The following example shows how to commit pending changes to the active DPVM database.

```
switch# config terminal
switch(config)# device-alias commit
```

Related Commands	Command	Description
	<b>device-alias database</b>	Configures and activates the device alias database.
	<b>device-alias distribute</b>	Enables CFS distribution for device aliases.
	<b>show device-alias</b>	Displays device alias information.

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

## device-alias database

To initiate a Distributed Device Alias Services (device alias) session and configure device alias database, use the **device-alias database** command. To deactivate the device alias database, use the **no** form of the command.

**device-alias database**

**no device-alias database**

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

**Defaults** Deactivated.

**Command Modes** Configuration mode.

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

**Usage Guidelines** The **device-alias database** command starts a device alias session that locks all the databases on all the switches in this fabrics. When you exit device alias database configuration submode, the device alias session ends and the locks are released.

You can only perform all modifications in the temporary device alias database. To make the changes permanent, use the **device-alias commit** command.

**Examples** The following example shows how to activate a device alias session and enter device alias database configuration submode;.

```
switch# config terminal
switch(config)# device-alias database
switch(config-device-alias-db) #
```

Related Commands	Command	Description
	<b>device-alias commit</b>	Commits changes to the temporary device alias database to the active device alias database.
	<b>show device-alias</b>	Displays device alias database information.

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

## device-alias distribute

To enable Cisco Fabric Services (CFS) distribution for Distributed Device Alias Services (device alias), use the **device-alias distribute** command. To disable this feature, use the **no** form of the command.

**device-alias distribute**

**no device-alias distribute**

### Syntax Description

This command has no other arguments or keywords.

### Defaults

Enabled.

### Command Modes

Configuration mode.

### Command History

Release	Modification
2.0(x)	This command was introduced.

### Usage Guidelines

Use the **device-alias commit** command to apply pending changes to the CFS distribution session.

### Examples

The following example shows how to enable distribution for device alias information.

```
switch# config terminal
switch(config)# device-alias distribute
```

### Related Commands

Command	Description
<b>device-alias commit</b>	Commits changes to the active device alias database.
<b>device-alias database</b>	Configures and activates the device alias database.
<b>show device-alias</b>	Displays device alias information.

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

## device-alias import fcalias

To import device alias database information from another VSAN, use the **device-alias import fcalias** command. To revert to the default configuration or factory defaults, use the **no** form of the command.

**device-alias import fcalias vsan** *vsan-id*

**no device-alias import fcalias vsan** *vsan-id*

<b>Syntax Description</b>	<i>vsan vsan-id</i>	Specifies the VSAN ID. The range is 1 to 4093.
<b>Defaults</b>	None.	
<b>Command Modes</b>	Configuration mode.	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	2.0(x)	This command was introduced.
<b>Usage Guidelines</b>	<p>You can import legacy device name configurations using this feature without losing data, if they satisfy the following restrictions:</p> <ul style="list-style-type: none"> <li>• Each fcalias has only one member.</li> <li>• The member type is supported by the device name implementation.</li> </ul> <p>If any name conflict exists, the fcalias are not imported. The device name database is completely independent from the VSAN dependent fcalias database.</p> <p>When the import operation is complete, the modified global fcalias table can distributed to all other switches in the physical fabric using the <b>device-alias distribute</b> command so that new definitions are available everywhere.</p>	
<b>Examples</b>	<p>The following example shows how to import device alias information.</p> <pre>switch# config terminal switch(config)# device-alias import fcalias vsan 10</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>device-alias database</b>	Configures and activates the device alias database.
	<b>device-alias distribute</b>	Distributes fcalias database changes to the fabric.
	<b>show device-alias</b>	Displays device alias database information.



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

## device-alias name

To configure device names in the device alias database, use the **device-alias name** command. To remove device names from the device alias database, use the **no** form of the command.

**device-alias name** *device-name* **pwwn** *pwwn-id*

**no device-alias name** *device-name*

Syntax Description	<i>device-name</i>	Specifies the device name. Maximum length is 64 characters.
	<i>pwwn pwwn-id</i>	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.

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

Command Modes	Device alias database configuration submode.
---------------	--

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

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

**Examples** The following example shows how to configure a device name alias entry in the device name database.

```
switch# config terminal
switch(config)# device-alias database
switch(config-device-alias-db)# device-alias name Device1 pwwn 21:00:00:20:37:6f:db:bb
```

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

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

## dir

To display the contents of the current directory or the specified directory, use the **dir** command in EXEC mode.

**dir** [**bootflash**:*module* | *directory-or-filename* | **debug**:*directory-or-filename* | **log**:*module* | *directory-or-filename* | **modflash**:*module* | *directory-or-filename* | **slot0**:*directory-or-filename* | **volatile**:*module* | *directory-or-filename*]

Syntax Description	
<b>bootflash</b> :	(Optional) Flash image that resides on the supervisor module.
debug:	(Optional) Provides information about the debug capture directory.
log:	(Optional) Provides information about the two default logfiles. The file dmesg contains the kernel log-messages and the file messages contains the system application log-messages.
modflash:	(Optional) Provides information about the flash image that resides in a module flash file directory.
slot0:	(Optional) Flash image that resides on another module.
<i>module</i>	(Optional) Module name and number.
<i>filename-or-directory</i>	(Optional) Name of the file or directory to display on a specified device. The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.
volatile:	Flash image on the volatile file system.

### Defaults

The default file system is specified by the **cd** command.

### Command Modes

EXEC mode.

### Command History

Release	Modification
1.2(1)	This command was introduced.
2.1(1a)	Added <b>debug</b> , <b>log</b> , and <b>modflash</b> keywords.

### Usage Guidelines

None.

### Examples

The following example shows how to list the files on the bootflash directory.

```
switch# dir bootflash:
40295206   Aug 05 15:23:51 1980  ilc1.bin
12456448   Jul 30 23:05:28 1980  kickstart-image1
12288     Jun 23 14:58:44 1980  lost+found/
27602159   Jul 30 23:05:16 1980  system-image1
12447232   Aug 05 15:08:30 1980  kickstart-image2
28364853   Aug 05 15:11:57 1980  system-image2
```

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

```
Usage for bootflash://sup-local
 135404544 bytes used
  49155072 bytes free
 184559616 bytes total
```

The following example shows how to list the files in the debug directory.

```
switch# dir debug:
Usage for debug://sup-local
      0 bytes used
 2097152 bytes free
 2097152 bytes total
switch#
```

The following example shows how to list the files in the log file directory.

```
switch# dir log:
   31      Feb 05 05:00:57 2005  dmesg
 8445      Feb 06 10:34:35 2005  messages
```

```
Usage for log://sup-local
 35196928 bytes used
 174518272 bytes free
 209715200 bytes total
switch#
```

### Related Commands

Command	Description
cd	Changes the default directory or file system.
delete	Deletes a file on a Flash memory device.

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

# disable

To disable the Call Home function, use the **disable** command in Call Home configuration submode.

**disable**

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

**Defaults** None.

**Command Modes** Call Home configuration submode.

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

**Usage Guidelines** To enable the Call Home function, use the **enable** command.

**Examples** The following example shows how to disable the Call Home function.

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

Related Commands	Command	Description
	<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)**

## discover

To initiate the discovery of hosts, use the **discover** command. To disable this feature, use the **no** form of the command.

**discover host** *host port* **target** *target port* **vsan** *vsan id* **fabric** *fabric name*

**no discover**

### Syntax Description

<b>host</b> <i>host port</i>	Identifies the host port WWN. The format is <i>hh:hh:hh:hh:hh:hh:hh:hh</i> .
<b>target</b> <i>target port</i>	Identifies the target port WWN. The format is <i>hh:hh:hh:hh:hh:hh:hh:hh</i> .
<b>vsan</b> <i>vsan id</i>	Selects the VSAN identifier. The range is 1 to 4093.
<b>fabric</b> <i>fabric name</i>	Specifies the fabric for discovery. The maximum lengthmaximum length is 32 characters.

### Defaults

None.

### Command Modes

Cisco SME cluster configuration submode.

### Command History

Release	Modification
3.2(2)	This command was introduced.

### Usage Guidelines

None.

### Examples

The following example discovers a host and specifies a target, a VSAN, and a fabric for discovery:

```
switch# config t
switch(config)# sme cluster clustername1
switch(config-sme-cl)# discover host 20:00:00:00:c9:49:28:47 target
21:01:00:e0:8b:29:7e:0c vsan 2345 fabric sw-xyz
```

The following example disables the discovery feature:

```
switch# config t
switch(config)# sme cluster clustername1
switch(config-sme-cl)# no discover
```

### Related Commands

Command	Description
<b>show sme cluster</b>	Displays information about the Cisco SME cluster.

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

## discover custom-list

Command	Description
<b>show sme cluster</b>	Displays information about the Cisco SME cluster.

To selectively initiate discovery for specified domain IDs in a VSAN, use the **discover custom-list** command in EXEC mode.

```
discover custom-list {add | delete} vsan vsan-id fcid fc-id
```

### Syntax Description

<b>add</b>	Add a targets to the customized list.
<b>delete</b>	Deletes a target from the customized list.
<b>vsan</b> <i>vsan-id</i>	Discovers SCSI targets for the specified VSAN ID. The range is 1 to 4093.
<b>fcip</b> <i>fc-id</i>	Discovers SCSI targets for the specified FCID. The format is <i>0xhhhhhhh</i> , where <i>h</i> is a hexadecimal digit.

### Defaults

None.

### Command Modes

EXEC mode.

### Command History

Release	Modification
1.1(1)	This command was introduced.

### Usage Guidelines

None.

### Examples

The following example selectively initiates discovery for the specified VSAN and FCID.

```
switch# discover custom-list add vsan 1 fcid 0X123456
```

The following example deletes the specified VSAN and FCID from the customized list.

```
switch# discover custom-list delete vsan 1 fcid 0X123456
```

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

## discover scsi-target

To discover SCSI targets on local storage to the switch or remote storage across the fabric, use the **discover scsi-target** command in EXEC mode.

```
discover scsi-target { custom-list | local | remote | vsan vsan-id fcid fc-id } os { aix | all | hpux | linux | solaris | windows } [lun | target]
```

Syntax	Description
<b>custom-list</b>	Discovers SCSI targets from the customized list.
<b>local</b>	Discovers local SCSI targets.
<b>remote</b>	Discovers remote SCSI targets.
<b>vsan</b> <i>vsan-id</i>	Discovers SCSI targets for the specified VSAN ID. The range is 1 to 4093.
<b>fcid</b> <i>fc-id</i>	Discovers SCSI targets for the specified FCID. The format is <i>0xhhhhhhh</i> , where <i>h</i> is a hexadecimal digit.
<b>os</b>	Discovers the specified operating system.
<b>aix</b>	Discovers the AIX operating system
<b>all</b>	Discovers all operating systems
<b>hpux</b>	Discovers the HPUX operating system
<b>linux</b>	Discovers the Linux operating system
<b>solaris</b>	Discovers the Solaris operating system
<b>windows</b>	Discovers the Windows operating system
<b>lun</b>	Discovers SCSI targets and LUNs.
<b>target</b>	Discovers SCSI targets.

**Defaults** None.

**Command Modes** EXEC mode.

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

**Usage Guidelines** On-demand discovery only discovers Nx ports present in the name server database that have registered a FC4 Type = SCSI\_FCP.

**Examples** The following example shows how to discover local targets assigned to all OSs.

```
switch# discover scsi-target local os all
discovery started
```

The following example shows how to discover remote targets assigned to the Windows OS.

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

```
switch# discover scsi-target remote os windows  
discovery started
```

The following example shows how to discover SCSI targets for the specified VSAN (1) and FCID (0x9c03d6).

```
switch# discover scsi-target vsan 1 fcid 0x9c03d6  
discover scsi-target vsan 1 fcid 0x9c03d6  
VSAN:      1 FCID: 0x9c03d6 PWWN: 00:00:00:00:00:00:00:00  
PRLI RSP: 0x01 SPARM: 0x0012...
```

The following example begins discovering targets from a customized list assigned to the Linux operating system.

```
switch# discover scsi-target custom-list os linux  
discovery started
```



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

# distribute

To enable distribution of the Call Home function using CFS, use the **distribute** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

**distribute**

**no distribute**

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

**Defaults** None.

**Command Modes** Call Home configuration submode.

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

**Usage Guidelines** None.

**Examples** The following example shows how to enable distribution of the Call Home function using CFS.

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

Related Commands	Command	Description
	<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)**

## do

Use the **do** command to execute an EXEC-level command from any configuration mode or submode.

**do** *command*

<b>Syntax Description</b>	<i>command</i>	Specifies the EXEC command to be executed.
---------------------------	----------------	--

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

<b>Command Modes</b>	All configuration modes.	
----------------------	--------------------------	--

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	3.4(1)	Modified the command output for 3.4(1) release.
1.1(1)	This command was introduced.	

<b>Usage Guidelines</b>	Use this command to execute EXEC commands while configuring your switch. After the EXEC command is executed, the system returns to the mode from which you issued the <b>do</b> command.
-------------------------	--

<b>Examples</b>	The following example shows how to execute the EXEC commands:
-----------------	---

```
switch(config)# port-monitor name cisco
switch(config-port-monitor)# do
switch(config-port-monitor)#
```

The following example disables the **terminal session-timeout** command using the **do** command in configuration mode:

```
switch(config)# do terminal session-timeout 0
switch(config)#
```

The following example creates, enables, and displays the interface from configuration mode:

```
switch(config)# int fc 3/1
switch(config-if)# no shut
switch(config-if)# do show interface fc 3/1
fc3/1 is trunking
  Hardware is Fibre Channel
  Port WWN is 20:81:00:05:32:00:4a:9e
  Peer port WWN is 20:43:00:0c:88:00:4a:e2
  Admin port mode is auto, trunk mode is on
  Port mode is TE
  Port vsan is 1
  Speed is 2 Gbps
  Transmit B2B Credit is 0
  Receive B2B Credit is 255
  Receive data field Size is 2112
```

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

```
Beacon is turned off
Trunk vsans (admin allowed and active) (1-10)
Trunk vsans (up) (1-10)
Trunk vsans (isolated) ()
Trunk vsans (initializing) ()
5 minutes input rate 504 bits/sec, 63 bytes/sec, 0 frames/sec
5 minutes output rate 344 bits/sec, 43 bytes/sec, 0 frames/sec
69390 frames input, 4458680 bytes
  0 discards, 0 errors
  0 CRC, 0 unknown class
  0 too long, 0 too short
69458 frames output, 3086812 bytes
  0 discards, 0 errors
2 input OLS, 1 LRR, 0 NOS, 2 loop inits
1 output OLS, 1 LRR, 1 NOS, 1 loop inits
```

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

## dpvm abort

To discard a dynamic port VSAN membership (DPVM) Cisco Fabric Services (CFS) distribution session in progress, use the **dpvm abort** command in **configuration mode**.

### dpvm abort

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

**Defaults** None.

**Command Modes** Configuration mode.

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

**Usage Guidelines** To use this command, DPVM must be enabled using the **dpvm enable** command.

**Examples** The following example shows how to discard a DPVM CFS distribution session in progress.

```
switch# config terminal
switch(config)# dpvm abort
```

Related Commands	Command	Description
	<b>dpvm database</b>	Configures the DPVM database.
	dpvm distribute	Enables CFS distribution for DPVM.
	dpvm enable	Enables DPVM.
	show dpvm	Displays DPVM information.

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

## dpvm activate

To activate the dynamic port VSAN membership (DPVM) configuration database, use the **dpvm activate** command. To deactivate the DPVM configuration database, use the **no** form of the command.

**dpvm activate [force]**

**no dpvm activate [force]**

Syntax Description	force	Forces the activation or deactivation if conflicts exist between the configured DPVM database and the active DPVM database.
--------------------	-------	---

Defaults	Deactivated.
----------	--------------

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

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

Usage Guidelines	<p>To use this command, DPVM must be enabled using the <b>dpvm enable</b> command.</p> <p>Activation might fail if conflicting entries are found between the configured DPVM database and the currently activated DPVM database. You can ignore the conflicts using the <b>force</b> option.</p>
------------------	--

Examples	The following example shows how to activate the DPVM database.
----------	--

```
switch# config terminal
switch(config)# dpvm activate
```

The following example shows how to deactivate the DPVM database.

```
switch# config terminal
switch(config)# no dpvm activate
```

Related Commands	Command	Description
	<b>dpvm database</b>	Configures the DPVM database.
	<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)*

## dpvm auto-learn

To enable the automatic learning feature (autolearn) for the active dynamic port VSAN membership (DPVM) database, use the **dpvm auto-learn** command. To disable this feature, use the **no** form of the command.

**dpvm auto-learn**

**no dpvm auto-learn**

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

**Defaults** Disabled.

**Command Modes** Configuration mode.

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

**Usage Guidelines** To use this command, DPVM must be enabled using the **dpvm enable** command. When autolearn is enabled, the system automatically creates the DPVM database by learning about devices currently logged or newly logged devices with a VSAN. This is a quick way to create the DPVM database, which can later be edited. Autolearn features include the following:

- An autolearned entry is created by adding the device PWWN and VSAN to the active DPVM database.
- The active DPVM database must be present when autolearning is enabled.
- Autolearned entries can be deleted from the active DPVM database by the user until autolearning is disabled. Autolearned entries are not permanent in the active DPVM database until autolearning is disabled.
- If a device logs out when autolearning is enabled, the device entry is deleted from the active DPVM database.
- If a particular device logs into the switch multiple times through different ports, then only the VSAN corresponding to last login is associated with the device.
- Autolearn entries do not override previously configured activate entries.

**Examples** The following example shows how to enable autolearning for the DPVM database.

```
switch# config terminal
switch(config)# dpvm auto-learn
```

The following example shows how to disable autolearning for the DPVM database.

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

```
switch# config terminal  
switch(config)# no dpvm auto-learn
```

**Related Commands**

<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)***

## dpvm commit

To apply the pending configuration pertaining to the dynamic port VSAN membership (DPVM) Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **dpvm commit** command.

### dpvm commit

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

**Defaults** None.

**Command Modes** Configuration mode.

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

**Usage Guidelines** To use this command, DPVM must be enabled using the **dpvm enable** command.

**Examples** The following example shows how to commit changes to the DPVM database.

```
switch# config terminal
switch(config)# dpvm commit
```

Related Commands	Command	Description
	dpvm distribute	Enables CFS distribution for DPVM.
	<b>dpvm enable</b>	Enables DPVM.
	show dpvm	Displays DPVM information.



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

## dpvm database

To activate and configure the dynamic port VSAN membership (DPVM) database, use the **dpvm database** command. To deactivate the database, use the **no** form of the command.

**dpvm database**

**no dpvm database**

### Syntax Description

This command has no other arguments or keywords.

### Defaults

Deactivated.

### Command Modes

Configuration mode.

### Command History

Release	Modification
2.0(x)	This command was introduced.

### Usage Guidelines

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

The DPVM database consists of a series of device mapping entries. Each entry consists of device pWWN or nWWN along with the dynamic VSAN to be assigned. Use the **nwwn** command or **pwwn** command to add the entries to the DPVM database. This database is global to the whole switch (and fabric) and is not maintained for each VSAN.

### Examples

The following example shows how to activate the DPVM database and enter DPVM database configuration submenu.

```
switch# config terminal
switch(config)# dpvm database
switch(config-dpvm-db)#
```

### Related Commands

Command	Description
<b>dpvm enable</b>	Enables DPVM.
nwwn (DPVM database configuration submenu)	Adds entries to the DPVM database using the nWWN.
pwwn (DPVM database configuration submenu)	Adds entries to the DPVM database using the pWWN.
show dpvm	Displays DPVM database information.

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

## dpvm database copy active

To copy the active dynamic port VSAN membership (DPVM) database to the config DPVM database, use the **dpvm database copy active** command.

### dpvm database copy active

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

**Defaults** Disabled.

**Command Modes** EXEC mode.

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

**Usage Guidelines** To use this command, DPVM must be enabled using the **dpvm enable** command.

The following circumstances may require the active database to be copied to the config database:

- When the autolearned entries are only added to the active database.
- When the config database or entries in the config database are accidentally deleted.



**Note**

If you want to copy the DPVM database and fabric distribution is enabled, you must first commit the changes.

**Examples** The following example shows how to copy the active DPVM database to the config DPVM database.

```
switch# dpvm database copy active
```

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

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

## dpvm database diff

To display the active dynamic port VSAN membership (DPVM) database, use the **dpvm database diff** command.

**dpvm database diff {active | config}**

Syntax Description	active	config
	Displays differences in the DPVM active database compared to the DPVM config database.	Displays differences in the DPVM config database compared to the DPVM active database.

**Defaults** Deactivated.

**Command Modes** Configuration mode.

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

**Usage Guidelines** To use this command, DPVM must be enabled using the **dpvm enable** command.

**Examples** The following example displays the differences in the DPVM active database when compared with the DPVM config database.

```
switch# dpvm database diff active
Legend: "+" New Entry, "-" Missing Entry, "*" Possible Conflict Entry
-----
- pwnn 44:22:33:44:55:66:77:88 vsan 44
* pwnn 11:22:33:44:55:66:77:88 vsan 11
```

The following example displays the differences in the DPVM config database when compared with the DPVM active database.

```
switch# dpvm database diff config
Legend: "+" New Entry, "-" Missing Entry, "*" Possible Conflict Entry
-----
- pwnn 44:22:33:44:55:66:77:88 vsan 44
* pwnn 11:22:33:44:55:66:77:88 vsan 11
```

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

**Related Commands**

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

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

## dpvm distribute

To enable Cisco Fabric Services (CFS) distribution for dynamic port VSAN membership (DPVM), use the **dpvm distribute** command. To disable this feature, use the **no** form of the command.

**dpvm distribute**

**no dpvm distribute**

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

**Defaults** Enabled.

**Command Modes** Configuration mode.

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

**Usage Guidelines** To use this command, DPVM must be enabled using the **dpvm enable** command. Temporary changes to the DPVM database must be committed to the active DPVM database using the **dpvm commit** command before being distributed to the fabric.

**Examples** The following example shows how to disable distribution for the DPVM database.

```
switch# config terminal
switch(config)# no dpvm distribute
```

The following example shows how to enable distribution for the DPVM database.

```
switch# config terminal
switch(config)# dpvm distribute
```

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

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

## dpvm enable

To enable dynamic port VSAN membership (DPVM), use to **dpvm enable** command. To disable DPVM, use the **no** form of the command.

**dpvm enable**

**no dpvm enable**

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

**Defaults** Disabled.

**Command Modes** Configuration mode.

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

**Usage Guidelines** The configuration and verification commands for DPVM are only available when DPVM is enabled on the switch. When you disable this feature, all related configurations are automatically discarded.

**Examples** The following example shows how to enable DPVM.

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

Related Commands	Command	Description
	dpvm activate	Activates the DPVM database.
	<b>dpvm database</b>	Configures the DPVM database.
	show dpvm	Displays DPVM database information.

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

## dscp

To configure a differentiated services code point (DSCP) in a QoS policy map class, use the **dscp** command in EXEC mode. To disable this feature, use the **no** form of the command.

**dscp** *value*

**no dscp** *value*

Syntax Description	<i>value</i>
	Configures the DSCP value. The range is 0 to 63. DSCP value 46 is reserved.

Defaults	The default DSCP value is 0.
----------	------------------------------

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

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

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

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

Examples	The following example configures a DSCP value of 56 in QoS policy classMap1.
----------	--

```
switch(config-pmap)# class classMap1
switch(config-pmap-c)# dscp 56
switch(config-pmap-c)#
```

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

## duplicate-message throttle

To enable throttling of duplicate Call Home alert messages, use the **duplicate-message throttle** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

**duplicate-message throttle**

**no duplicate-message throttle**

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

**Defaults** Enabled.

**Command Modes** Call Home configuration submode.

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

**Usage Guidelines** The rate of throttling is a maximum of thirty messages in 2 hours.

**Examples** The following example shows how to enable throttling of duplicate Call Home alert messages.

```
switch# config terminal
switch(config)# callhome
switch(config-callhome)# duplicate-message throttle
```

Related Commands	Command	Description
	<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.