



# I Commands

---

- [identity](#), on page 4
- [ingress-sa](#), on page 6
- [initiator](#), on page 7
- [in-order-guarantee](#), on page 8
- [install all](#), on page 9
- [install clock-module](#), on page 15
- [install license](#), on page 17
- [install module bios](#), on page 18
- [install module epld](#), on page 19
- [install module loader](#), on page 21
- [install ssi](#), on page 22
- [interface](#), on page 24
- [interface fc](#), on page 26
- [interface fcip](#), on page 28
- [interface fc-tunnel](#), on page 31
- [interface gigabitethernet](#), on page 33
- [interface ioa](#), on page 35
- [interface iscsi](#), on page 36
- [interface mgmt](#), on page 38
- [interface port-channel](#), on page 39
- [interface sme](#), on page 41
- [interface sme \(Cisco SME cluster node configuration submode\)](#), on page 42
- [interface vsan](#), on page 44
- [intersight connection](#), on page 45
- [intersight proxy](#), on page 46
- [intersight trustpoint](#), on page 47
- [ioa cluster](#), on page 48
- [ioa site-local](#), on page 49
- [ioa-ping](#), on page 50
- [ip access-group](#), on page 52
- [ip access-list](#), on page 54
- [ip address \(FCIP profile configuration submode\)](#), on page 61
- [ip address \(interface configuration\)](#), on page 62

- [ip default-gateway](#), on page 63
- [ip default-network](#), on page 64
- [ip \(destination-group\)](#), on page 65
- [ip domain-list](#), on page 67
- [ip domain-lookup](#), on page 68
- [ip domain-name](#), on page 69
- [ip name-server](#), on page 70
- [ip route](#), on page 71
- [ip routing](#), on page 72
- [ip-compression](#), on page 73
- [ips netsim delay-ms](#), on page 75
- [ips netsim delay-us](#), on page 76
- [ips netsim drop nth](#), on page 77
- [ips netsim drop random](#), on page 79
- [ips netsim enable](#), on page 81
- [ips netsim max-bandwidth-kbps](#), on page 82
- [ips netsim max-bandwidth-mbps](#), on page 83
- [ips netsim qsize](#), on page 84
- [ips netsim reorder](#), on page 85
- [ipv6 access-list](#), on page 87
- [ipv6 address](#), on page 88
- [ipv6 enable](#), on page 89
- [ipv6 nd](#), on page 90
- [ipv6 route](#), on page 92
- [ipv6 routing](#), on page 94
- [ipv6 traffic-filter](#), on page 95
- [iscsi authentication](#), on page 96
- [iscsi duplicate-wwn-check](#), on page 98
- [iscsi dynamic initiator](#), on page 100
- [iscsi enable](#), on page 102
- [iscsi enable module](#), on page 103
- [iscsi import target fc](#), on page 104
- [iscsi initiator idle-timeout](#), on page 105
- [iscsi initiator ip-address](#), on page 106
- [iscsi initiator name](#), on page 108
- [iscsi interface vsan-membership](#), on page 109
- [iscsi save-initiator](#), on page 110
- [iscsi virtual-target name](#), on page 112
- [islb abort](#), on page 115
- [islb commit](#), on page 116
- [islb distribute](#), on page 117
- [islb initiator](#), on page 119
- [islb save-initiator](#), on page 121
- [islb virtual-target name](#), on page 123
- [islb vrrp](#), on page 125
- [islb zoneset activate](#), on page 127

- [isns](#), on page 128
- [isns distribute](#), on page 129
- [isns esi retries](#), on page 130
- [isns profile name](#), on page 131
- [isns reregister](#), on page 132
- [isns-server enable](#), on page 133
- [ivr aam pre-deregister-check](#), on page 134
- [ivr aam register](#), on page 135
- [ivr abort](#), on page 136
- [ivr commit](#), on page 137
- [ivr copy active-service-group user-configured-service-group](#), on page 138
- [ivr copy active-topology user-configured-topology](#), on page 139
- [ivr copy active-zoneset full-zoneset](#), on page 140
- [ivr copy auto-topology user-configured-topology](#), on page 141
- [ivr distribute](#), on page 142
- [ivr enable](#), on page 143
- [ivr fcdomain database autonomous-fabric-num](#), on page 144
- [ivr nat](#), on page 145
- [ivr refresh](#), on page 146
- [ivr service-group activate](#), on page 147
- [ivr service-group name](#), on page 148
- [ivr virtual-fcdomain-add](#), on page 150
- [ivr virtual-fcdomain-add2](#), on page 151
- [ivr vsan-topology](#), on page 152
- [ivr vsan-topology auto](#), on page 154
- [ivr vsan-topology database](#), on page 155
- [ivr withdraw domain](#), on page 157
- [ivr zone name](#), on page 158
- [ivr zone rename](#), on page 159
- [ivr zoneset](#), on page 160
- [ivr zoneset rename](#), on page 161

# identity

To configure the identity for the IKE protocol, use the **identity** command in IKE configuration submode. To delete the identity, use the **no** form of the command.

```
identity {address | hostname}
no identity {address | hostname}
```

## Syntax Description

<b>address</b>	Sets the IKE identity to be the IPv4 address of the switch.
<b>hostname</b>	Sets the IKE identity to be the host name of the switch.

## Command Default

None.

## Command Modes

IKE configuration submode.

## Command History

Release	Modification
3.0(1)	This command was introduced.

## Usage Guidelines

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

Before configuring a certificate for the switch, configure the host name and domain name, and set the identity to be the host name. This allows the certificate to be used for authentication.



**Note** The host name is the fully qualified domain name (FQDN) of the switch. To use the switch FQDN for the IKE identity, you must first configure both the switch name and the domain name. The FQDN is required for using RSA signatures for authentication. By default address is identified.

## Examples

The following example shows how to set the IKE identity to the IP address of the switch:

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# identity address
```

The following example shows how to delete the IKE identity:

```
switch(config-ike-ipsec)# no identity address
```

The following example shows how to set the IKE identity to the host name:

```
switch(config-ike-ipsec)# identity hostname
```

The following example shows how to delete the IKE identity:

```
switch(config-ike-ipsec)# no identity hostname
```

**Related Commands**

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

# ingress-sa

To configure the Security Association (SA) to the ingress hardware, use the **ingress-sa** command. To delete the SA from the ingress hardware, use the **no** form of the command.

**ingress-sa** *spi-number*  
**no ingress-sa** *spi-number*

## Syntax Description

<i>spi-number</i>	The range is from 256 to 4294967295.
-------------------	--------------------------------------

## Command Default

None.

## Command Modes

Configuration submenu.

## Command History

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

## Usage Guidelines

None.

## Examples

The following example shows how to configure the SA to the ingress hardware:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface fc 2/1 - 3
switch(config-if)# fcsp esp manual
switch(config-if-esp)# ingress-sa 258
switch(config-if-esp)#
```

## Related Commands

Command	Description
<b>show fcsp interface</b>	Displays FC-SP-related information for a specific interface.

# initiator

To configure the initiator version and address, use the **initiator** command IKE configuration submode. To revert to the default, use the **no** form of the command.

**initiator version** *version* **address** *ip-address*  
**no initiator version** *version* **address** *ip-address*

## Syntax Description

<i>version</i>	Specifies the protocol version number. The only valid value is 1.
<b>address</b> <i>ip-address</i>	Specifies the IP address for the IKE peer. The format is <i>A.B.C.D</i> .

## Command Default

IKE version 2.

## Command Modes

IKE configuration submode.

## Command History

Release	Modification
2.0(x)	This command was introduced.

## Usage Guidelines

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

## Examples

The following example shows how initiator information for the IKE protocol:

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# initiator version 1 address 10.1.1.1
```

## Related Commands

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

# in-order-guarantee

To enable in-order delivery, use the **in-order-guarantee** command in configuration mode. To disable in-order delivery, use the **no** form of the command.

**in-order-guarantee** [**vsan** *vsan-id*]  
**no in-order-guarantee** [**vsan** *vsan-id*]

<b>Syntax Description</b>	<table border="1"> <tr> <td><b>vsan</b> <i>vsan-id</i></td> <td>(Optional) Specifies a VSAN ID. The range is 1 to 4093.</td> </tr> </table>	<b>vsan</b> <i>vsan-id</i>	(Optional) Specifies a VSAN ID. The range is 1 to 4093.
<b>vsan</b> <i>vsan-id</i>	(Optional) Specifies a VSAN ID. The range is 1 to 4093.		

**Command Default** Disabled.

**Command Modes** Configuration mode.

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>1.3(4)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	1.3(4)	This command was introduced.
Release	Modification				
1.3(4)	This command was introduced.				

**Usage Guidelines** In-order delivery of data frames guarantees frame delivery to a destination in the same order that they were sent by the originator.

**Examples**

The following example shows how to enable in-order delivery for the entire switch:

```
switch# config terminal
switch(config) # in-order-guarantee
```

The following example shows how to disable in-order delivery for the entire switch:

```
switch(config) # no in-order-guarantee
```

The following example shows how to enable in-order delivery for a specific VSAN:

```
switch(config) # in-order-guarantee vsan 3452
```

The following example shows how to disable in-order delivery for a specific VSAN:

```
switch(config) # no in-order-guarantee vsan 101
```

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>show in-order-guarantee</b></td> <td>Displays the in-order-guarantee status.</td> </tr> </tbody> </table>	Command	Description	<b>show in-order-guarantee</b>	Displays the in-order-guarantee status.
Command	Description				
<b>show in-order-guarantee</b>	Displays the in-order-guarantee status.				



# install all

To upgrade all modules in any Cisco MDS 9000 family switch, use the **install all** command. This upgrade can happen nondisruptively or disruptively depending on the current configuration of your switch.

**install all** [ {**asm-sfn** *file name* | **kickstart** | **ssi** | **system**} **URL**]

Syntax Description	
<b>asm-sfn</b> <i>filename</i>	(Optional) Upgrades the ASM image.
<b>kickstart</b>	(Optional) Upgrades the kickstart image.
<b>ssi</b>	(Optional) Upgrades the SSI image.
<b>system</b>	(Optional) Upgrades the system image.
<b>URL</b>	(Optional) Specifies the location URL of the source file to be installed.

The following table lists the aliases for *URL*.

<b>bootflash:</b>	Source location for internal bootflash memory.
<b>slot0:</b>	Source location for the CompactFlash memory or PCMCIA card.
<b>volatile:</b>	Source location for the volatile file system.
<b>tftp:</b>	Source location for a Trivial File Transfer Protocol (TFTP) network server. The syntax for this URL is <b>tftp: [[ //location ] /directory ] /filename.</b>
<b>ftp:</b>	Source location for a File Transfer Protocol (FTP) network server. The syntax for this URL is <b>ftp: [[ //location ] /directory ] /filename.</b>
<b>sftp:</b>	Source location for a Secure Trivial File Transfer Protocol (SFTP) network server. The syntax for this URL is <b>sftp: [[ //&lt;username@&gt;location ] /directory ] /filename.</b>
<b>scp:</b>	Source location for a Secure Copy Protocol (SCP) network server. The syntax for this URL is <b>scp: [[ //location ] /directory ] /filename.</b>
<i>image-filename</i>	The name of the source image file.

**Command Default** None.

**Command Modes** EXEC mode.

Command History	Release	Modification
	1.0(3)	This command was introduced.
	1.2(2)	Added the <b>asm-sfn</b> keyword and made all keywords optional.
	2.0(1b)	Added the <b>ssi</b> keyword.

**Usage Guidelines**

The **install all** command upgrades all modules in any Cisco MDS 9000 Family switch.



**Tip** During a software upgrade to Cisco MDS SAN-OS 3.1(3), all modules that are online are tested and the installation stops if any modules are running with a faulty CompactFlash. When this occurs, the switch can not be upgraded until the situation is corrected. A system message displays the module information and indicates that you must issue the **system health cf-crc-check module** CLI command to troubleshoot.

To copy a remote file, specify the entire remote path exactly as it is.



**Caution** If a switchover is required when you issue the **install all** command from a Telnet or SSH session, all open sessions are terminated. If no switchover is required, the session remains unaffected. The software issues a self-explanatory warning at this point and provides the option to continue or terminate the installation.

**Examples**

The following example displays the result of the **install all** command if the system and kickstart files are specified locally:

```
switch# install all sys bootflash:isan-1.3.1 kickstart bootflash:boot-1.3.1

Verifying image bootflash:/boot-1.3.1
[#####] 100% -- SUCCESS

Verifying image bootflash:/isan-1.3.1
[#####] 100% -- SUCCESS

Extracting "slc" version from image bootflash:/isan-1.3.1.
[#####] 100% -- SUCCESS

Extracting "ips" version from image bootflash:/isan-1.3.1.
[#####] 100% -- SUCCESS

Extracting "system" version from image bootflash:/isan-1.3.1.
[#####] 100% -- SUCCESS

Extracting "kickstart" version from image bootflash:/boot-1.3.1.
[#####] 100% -- SUCCESS

Extracting "loader" version from image bootflash:/boot-1.3.1.
[#####] 100% -- SUCCESS

Compatibility check is done:
Module  bootable      Impact  Install-type  Reason
-----  -
1       yes    non-disruptive  rolling
2       yes     disruptive     rolling  Hitless upgrade is not supported
3       yes     disruptive     rolling  Hitless upgrade is not supported
4       yes    non-disruptive  rolling
5       yes    non-disruptive  reset
6       yes    non-disruptive  reset

Images will be upgraded according to following table:
Module  Image      Running-Version  New-Version  Upg-Required
-----  -
1       slc        1.3(2a)         1.3(1)      yes
```



```

Module 6: Waiting for module online.
Jan 18 23:43:02 Hacienda %PORT-5-IF_UP: Interface mgmt0 is up
Jan 18 23:43:19 Hacienda %LICMGR-3-LOG_LIC_NO_LIC: No license(s) present for feature
FM_SERVER_PKG. Application(s) shutdown in 53 days.
Jan 18 23:43:19 Hacienda %LICMGR-3-LOG_LIC_NO_LIC: No license(s) present for feature
ENTERPRISE_PKG. Application(s) shutdown in 50 days.
Jan 18 23:43:19 Hacienda %LICMGR-3-LOG_LIC_NO_LIC: No license(s) present for feature
SAN_EXTN_OVER_IP. Application(s) shutdown in 50 days.
Jan 18 23:43:19 Hacienda %LICMGR-3-LOG_LICAPP_NO_LIC: Application port-security running
without ENTERPRISE_PKG license, shutdown in 50 days
Jan 18 23:43:19 Hacienda %LICMGR-4-LOG_LICAPP_EXPIRY_WARNING: Application Roles evaluation
license ENTERPRISE_PKG expiry in 50 days
Jan 18 23:44:54 Hacienda %BOOTVAR-5-NEIGHBOR_UPDATE_AUTOCOPY: auto-copy supported by neighbor,
starting...

Module 1: Non-disruptive upgrading.
[#          ] 0%Jan 18 23:44:56 Hacienda %MODULE-5-STANDBY_SUP_OK: Supervisor 5
is standby
Jan 18 23:44:55 Hacienda %IMAGE_DNLD-SLOT1-2-IMG_DNLD_STARTED: Module image download
process. Please wait until completion...
Jan 18 23:45:12 Hacienda %IMAGE_DNLD-SLOT1-2-IMG_DNLD_COMPLETE: Module image download
process. Download successful.
Jan 18 23:45:48 Hacienda %MODULE-5-MOD_OK: Module 1 is online
[#####] 100% -- SUCCESS

Module 4: Non-disruptive upgrading.
[#          ] 0%Jan 18 23:46:12 Hacienda %IMAGE_DNLD-SLOT4-2-IMG_DNLD_STARTED:
Module image download process. Please wait until completion...
Jan 18 23:46:26 Hacienda %IMAGE_DNLD-SLOT4-2-IMG_DNLD_COMPLETE: Module image download
process. Download successful.
Jan 18 23:47:02 Hacienda %MODULE-5-MOD_OK: Module 4 is online
[#####] 100% -- SUCCESS

Module 2: Disruptive upgrading.
...
-- SUCCESS

Module 3: Disruptive upgrading.
...
-- SUCCESS

Install has been successful.

MDS Switch
Hacienda login:

```

The following example displays the result of the **install all** command if the system and kickstart files are specified remotely:

```

switch# install all system
scp://user@171.69.16.26/tftpboot/HKrel/qa/vegas/final/m9500-sflek9-mz.1.3.2a.bin kickstart
scp://user@171.69.16.26/tftpboot/HKrel/qa/vegas/final/m9500-sflek9-kickstart-mz.1.3.2a.bin
For scp://user@171.69.16.26, please enter password:
For scp://user@171.69.16.26, please enter password:

Copying image from
scp://user@171.69.16.26/tftpboot/HKrel/qa/vegas/final/m9500-sflek9-kickstart-mz.1.3.2a.bin
to bootflash:///m9500-sflek9-kickstart-mz.1.3.2a.bin.
[#####] 100% -- SUCCESS

Copying image from
scp://user@171.69.16.26/tftpboot/HKrel/qa/vegas/final/m9500-sflek9-mz.1.3.2a.bin to

```

```

bootflash:///m9500-sflek9-mz.1.3.2a.bin.
[#####] 100% -- SUCCESS

Verifying image bootflash:///m9500-sflek9-kickstart-mz.1.3.2a.bin
[#####] 100% -- SUCCESS

Verifying image bootflash:///m9500-sflek9-mz.1.3.2a.bin
[#####] 100% -- SUCCESS

Extracting "slc" version from image bootflash:///m9500-sflek9-mz.1.3.2a.bin.
[#####] 100% -- SUCCESS

Extracting "ips" version from image bootflash:///m9500-sflek9-mz.1.3.2a.bin.
[#####] 100% -- SUCCESS

Extracting "system" version from image bootflash:///m9500-sflek9-mz.1.3.2a.bin.
[#####] 100% -- SUCCESS

Extracting "kickstart" version from image bootflash:///m9500-sflek9-kickstart-mz.1.3.2a.bin.
[#####] 100% -- SUCCESS

Extracting "loader" version from image bootflash:///m9500-sflek9-kickstart-mz.1.3.2a.bin.
[#####] 100% -- SUCCESS

```

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
1	yes	non-disruptive	rolling	
2	yes	disruptive	rolling	Hitless upgrade is not supported
3	yes	non-disruptive	rolling	
4	yes	non-disruptive	rolling	
5	yes	non-disruptive	reset	
6	yes	non-disruptive	reset	
7	yes	non-disruptive	rolling	
8	yes	non-disruptive	rolling	
9	yes	disruptive	rolling	Hitless upgrade is not supported

Images will be upgraded according to following table:

Module	Image	Running-Version	New-Version	Upg-Required
1	slc	1.3(1)	1.3(2a)	yes
1	bios	v1.1.0(10/24/03)	v1.0.8(08/07/03)	no
2	ips	1.3(1)	1.3(2a)	yes
2	bios	v1.1.0(10/24/03)	v1.0.8(08/07/03)	no
3	slc	1.3(1)	1.3(2a)	yes
3	bios	v1.1.0(10/24/03)	v1.0.8(08/07/03)	no
4	slc	1.3(1)	1.3(2a)	yes
4	bios	v1.1.0(10/24/03)	v1.0.8(08/07/03)	no
5	system	1.3(1)	1.3(2a)	yes
5	kickstart	1.3(1)	1.3(2a)	yes
5	bios	v1.1.0(10/24/03)	v1.0.8(08/07/03)	no
5	loader	1.2(2)	1.2(2)	no
6	system	1.3(1)	1.3(2a)	yes
6	kickstart	1.3(1)	1.3(2a)	yes
6	bios	v1.1.0(10/24/03)	v1.0.8(08/07/03)	no
6	loader	1.2(2)	1.2(2)	no
7	slc	1.3(1)	1.3(2a)	yes
7	bios	v1.1.0(10/24/03)	v1.0.8(08/07/03)	no
8	slc	1.3(1)	1.3(2a)	yes
8	bios	v1.1.0(10/24/03)	v1.0.8(08/07/03)	no
9	ips	1.3(1)	1.3(2a)	yes
9	bios	v1.1.0(10/24/03)	v1.0.8(08/07/03)	no

Do you want to continue with the installation (y/n)? [n]

<b>Command</b>	<b>Description</b>
<b>install module bios</b>	Upgrades the supervisor or switching module BIOS.
<b>install module loader</b>	Upgrades the bootloader on the active or standby supervisor or modules.
<b>show version</b>	Displays software image version information.

# install clock-module

To upgrade the EPLD images of the clock module on a Cisco MDS 9513 Switch Director, use the **install clock-module** command.

```
install clock-module [epld {bootflash: | slot0: | volatile:}]
```

Syntax Description	Parameter	Description
	<b>epld</b>	(Optional) Installs the clock module EPLD from the EPLD image.
	<b>bootflash:</b>	(Optional) Specifies the local URI containing EPLD image.
	<b>slot0:</b>	(Optional) Specifies the local URI containing EPLD image.
	<b>volatile:</b>	(Optional) Specifies the local URI containing EPLD image.

**Command Default** None.

**Command Modes** EXEC mode.

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

**Usage Guidelines** Use this command on the active supervisor to install the standby clock module EPLD from the specified EPLD image. After upgrading the clock module, power cycle the entire chassis for the change to take effect. It is not sufficient to reboot the chassis; you must turn the power off and on.



**Note** This command is supported only on the Cisco MDS 9513 Multilayer Switch Director.

## Examples

The following example upgrades the EPLD images for the clock module:

```
switch# install clock-module epld bootflash:m9000-epld-3.0.0.278.img
Len 3031343, CS 0x58, string MDS series EPLD image, built on Fri Nov 11 01:11:09 2005
EPLD Curr Ver New Ver
-----
Clock Controller 0x03 0x04
There are some newer versions of EPLDs in the image!
Do you want to continue (y/n) ? y
Proceeding to program Clock Module B.
Do you want to switchover Clock Modules after programming Clock Module B.
System Will Reset! y/n) ?n

|

Clock Module B EPLD upgrade is successful.
```

---

**Related Commands**

Command	Description
<b>show version clock-module epld</b>	Displays the current EPLD versions on the clock module.



# install license

To program the supervisor or switching module BIOS, use the **install license** command.

**install license** [**bootflash:** | **slot0:** | **volatile:**] *file-name*

## Syntax Description

<b>bootflash:</b>	(Optional) Specifies the source location for the license file.
<b>slot0:</b>	(Optional) Specifies the source location for the license file.
<b>volatile:</b>	(Optional) Specifies the source location for the license file.
<i>file-name</i>	Specifies the name of the license file.

## Command Default

None.

## Command Modes

EXEC mode.

## Command History

Release	Modification
1.2(1)	This command was introduced.

## Usage Guidelines

If a target filename is provided after the source URL, the license file is installed with that name. Otherwise, the filename in the source URL is used. This command also verifies the license file before installing it.

## Examples

The following example installs a file named license-file which resides in the bootflash: directory:

```
switch# install license bootflash:license-file
```

## Related Commands

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

# install module bios

To program the supervisor or switching module BIOS, use the **install module bios** command.

**install module** *module-number* **bios** {**system** [**bootflash:** | **slot0:** | **volatile:** *system-image*]}

## Syntax Description

<i>module-number</i>	Specifies the module number from slot 1 to 9 in a Cisco MDS 9500 Series switch. Specifies the module number from slot 1 to 2 in a Cisco MDS 9200 Series switch.
<b>system</b>	(Optional) Specifies the system image to use (optional). If system is not specified, the current running image is used.
<b>bootflash:</b>	(Optional) Specifies the source location for internal bootflash memory
<b>slot0:</b>	(Optional) Specifies the source location for the CompactFlash memory or PCMCIA card.
<b>volatile:</b>	(Optional) Specifies the source location for the volatile file system.
<i>system-image</i>	(Optional) Specifies the name of the system or kickstart image.

## Command Default

None.

## Command Modes

EXEC mode.

## Command History

Release	Modification
1.0(3)	This command was introduced.

## Usage Guidelines

If the BIOS is upgraded, you need to reboot to make the new BIOS effective. You can schedule the reboot at a convenient time so traffic will not be impacted.

The console baud rate automatically reverts to the default rate (9600) after any BIOS upgrade.

The URL is always the system image URL in the supervisor module, and points to the bootflash: or slot0: directories.

## Examples

The following example shows how to perform a nondisruptive upgrade for the system:

```
switch# install module 1 bios
Started bios programming .... please wait
###
BIOS upgrade succeeded for module 1
```

In this example, the switching module in slot 1 was updated.

# install module epld

To upgrade the electrically programmable logical devices (EPLDs) module, use the **install module epld** command. This command is only for supervisor modules, not switching modules.

**install module** *module-number* **epld** [**bootflash:** | **ftp:** | **scp:** | **sftp:** | **tftp:** | **volatile:**]

Syntax Description	
<i>module-number</i>	Enters the number for the standby supervisor modules or any other line card.
<b>bootflash:</b>	(Optional) Specifies the source location for internal bootflash memory.
<b>ftp</b>	(Optional) Specifies the local/remote URI containing EPLD image.
<b>scp</b>	(Optional) Specifies the local/remote URI containing EPLD image.
<b>sftp</b>	(Optional) Specifies the local/remote URI containing EPLD image.
<b>tftp</b>	(Optional) Specifies the local/remote URI containing EPLD image.
<b>volatile:</b>	(Optional) Specifies the source location for the volatile file system.

**Command Default** None.

**Command Modes** EXEC mode.

Command History	Release	Modification
	1.2(1)	This command was introduced.

**Usage Guidelines** Issue this command from the active supervisor module to update any other module.

If you forcefully upgrade a module that is not online, all EPLDs are forcefully upgraded. If the module is not present in the switch, an error is returned. If the module is present, the command process continues.

Do not insert or extract any modules while an EPLD upgrade or downgrade is in progress.

**Examples** The following example upgrades the EPLDs for the module in slot 2:

```
switch# install module 2 epld scp://user@10.6.16.22/users/dino/epld.img

The authenticity of host '10.6.16.22' can't be established.
RSA1 key fingerprint is 55:2e:1f:0b:18:76:24:02:c2:3b:62:dc:9b:6b:7f:b7.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.6.16.22' (RSA1) to the list of known hosts.
user@10.6.16.22's password:
epld.img          100% |*****| 1269 KB    00:00
Module Number                2
EPLD                        Curr Ver    New Ver
-----
Power Manager                0x06
XBUS IO                      0x07      0x08
```

```

UD chip Fix                0x05
Sahara                     0x05      0x05

Module 2 will be powered down now!!
Do you want to continue (y/n) ? y
\ <-----progress twirl
Module 2 EPLD upgrade is successful

```

The following example forcefully upgrades the EPLDs for the module in slot 2:

```

switch# install module 2 epld scp://user@10.6.16.22/epld-img-file-path

Module 2 is not online, Do you want to continue (y/n) ? y
cchetty@171.69.16.22's password:
epld.img                100% |*****| 1269 KB    00:00
\ <-----progress twirl
Module 2 EPLD upgrade is successful

```

### Related Commands

Command	Description
<b>show version epld</b>	Displays the available EPLD versions.
<b>show version modulenumbers epld</b>	Displays the current EPLD versions.

# install module loader

To upgrade the bootloader on either the active or standby supervisor module, use the **install module loader** command. This command is only for supervisor modules, not switching modules.

**install module** *module-number* **loader kickstart** [**bootflash:** | **slot0:** | **volatile:** *kickstart-image*]

Syntax Description	
<i>module-number</i>	Enters the module number for the active or standby supervisor modules (only slot 5 or 6).
<b>kickstart</b>	Specifies the kickstart image to use.
<b>bootflash:</b>	(Optional) Specifies the source location for internal bootflash memory
<b>slot0:</b>	(Optional) Specifies the source location for the CompactFlash memory or PCMCIA card.
<b>volatile:</b>	(Optional) Specifies the source location for the volatile file system.
<i>kickstart-image</i>	Specifies the name of the kickstart image.

**Command Default** None.

**Command Modes** EXEC mode.

Command History	Release	Modification
	1.0(3)	This command was introduced.

**Usage Guidelines** Before issuing the **install module loader** command, be sure to read the release notes to verify compatibility issues between the boot loader and the kickstart or system images.

If you install a loader version that is the same as the currently installed version, the loader will not be upgraded. When both the current version and the installed version are the same, use the **init system** command to force a loader upgrade.

## Examples

The following example shows how to perform a non disruptive upgrade for the system:

```
switch# install module 6 loader bootflash:kickstart_image
```

Related Commands	Command	Description
	<b>show version</b>	Verifies the output before and after the upgrade.

# install ssi

To perform a nondisruptive upgrade of the SSI image on an SSM, use the **install ssi** command.

```
install ssi {bootflash : | slot0 : | modflash : } file-name module slot
```

## Syntax Description

<b>bootflash:</b>	Specifies the source location for the SSI boot image file.
<b>slot0:</b>	Specifies the source location for the SSI boot image file.
<b>modflash:</b>	Specifies the source location for the SSI boot image file.
<i>file-name</i>	Specifies the SSI boot image filename.
<b>module</b> <i>slot</i>	Specifies the module slot number.

## Command Default

None.

## Command Modes

EXEC mode.

## Command History

Release	Modification
5.0(x)	This command has been deprecated (install ssi command is not supported for gen 2 card).
2.1(2)	This command was introduced.

## Usage Guidelines

You can use the **install ssi** command to upgrade or downgrade the SSI boot image if the SSM is only configured for Fibre Channel switching. If your SSM is configured for VSFN or Intelligent Storage Services, you must use the **boot** command to reconfigure the SSI boot variable and reload the module.

The **install ssi** command implicitly sets the SSI boot variable.



**Note** The SSM must be running EPLD version 2.1(2) to use the **install ssi** command. You must install the SSM on a Cisco MDS 9500 Series switch to update the EPLD.



**Note** The **install ssi** command does not support files located on the SSM modflash.

## Examples

The following example installs the SSI boot image on the module in slot 2:

```
switch# install ssi bootflash:lm9000-ek9-ssi-mz.2.1.2.bin module 2
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>boot</b>	Configures the boot variables.
<b>show boot</b>	Displays the current contents of boot variables.
<b>show module</b>	Verifies the status of a module.

# interface

To configure an interface on the Cisco MDS 9000 Family of switches, use the **interface** command in configuration mode.

```
interface {cpp {module-numberprocessor-numbervsan-id} | ethernet {slot number \ port-number} |
ethernet-port-channel ethernet-port-channel-number | fc {slot number | port number | fc-tunnel
tunnel-id} | mgmt | port-channel port-channel-number | vfc vfc-id | vfc port-channel vfc port-channel-id
| vsan vsan-id}
nointerface {cpp {module-numberprocessor-numbervsan-id} | ethernet {slot number \ port-number} |
ethernet-port-channel ethernet-port-channel-number | fc {slot number | port number | fc-tunnel
tunnel-id} | mgmt | port-channel port-channel-number | vfc vfc-id | vfc port-channel vfc port-channel-id
| vsan vsan-id}
```



**Note** On a Cisco Fabric Switch for HP c-Class BladeSystem and on a Cisco Fabric Switch for IBM BladeCenter, the syntax differs as follows:

## Syntax Description

<b>cpp</b>	Configures a Control Plane Process (CPP) interface.
<i>module-number</i>	Specifies the module number. The range is 1 to 10.
<i>processor-number</i>	Specifies the processor number. The range is from 1 to 1.
<i>vsan-id</i>	Specifies the VSAN ID. The range is from 1 to 4093.
<b>ethernet</b>	Specifies the Ethernet IEEE 802.3z.
<i>slot number / port number</i>	Specifies the Ethernet slot number and port number. Slot range is from 1 to 253 and port number range is from 1 to 128.
<b>ethernet-port-channel</b>	Ethernet Port Channel interface. The range is from 513 to 4096.
<i>ethernet-port-channel-number</i>	Specifies the Port Channel number. The range is from 513 to 4096.
<b>fc</b>	(Optional) Configures a Fiber Channel interface on an MDS 9000 Family switch (see the <b>interface fc</b> command).
<i>slot number / port number</i>	Specifies the slot number. The range is from 1 to 10. Specifies the FC slot number and port number. Slot range is from 1 to 10 and port number range is from 1 to 48.
<b>fc-tunnel</b>	Configures a Fiber Channel link interface (see the <b>interface fc-tunnel</b> command).
<i>tunnel-id</i>	Specifies the tunnel ID. The range is from 1 to 255.
<b>mgmt</b>	Configures a management interface (see the <b>interface mgmt</b> command).



<b>port-channel</b>	Configures a Port Channel interface (see the <b>interface port-channel</b> command).
<i>port-channel-number</i>	Specifies the Port Channel number. The range is from 1 to 256.
<b>vfc</b>	Specifies the Virtual FC interface.
<i>vfc-id</i>	Specifies the virtual interface ID or slot. The range is from 1 to 8192.
<b>vfc-port-channel</b>	Specifies the virtual FC port-channel interface
<i>vfc-port-channel-id</i>	Specifies the virtual interface ID. The range is from 513 to 4096.
<b>vsan</b>	Specifies the IPFC VSAN interface.
<i>vsan-id</i>	Specifies the VSAN ID. The range is from 1 to 4093.

**Command Default**

None.

**Command Modes**

Configuration mode.

**Command History**

Release	Modification
3.0(2)	This command was introduced.

**Usage Guidelines**

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

**interface fc1/1 - 5 , fc2/5 - 7**

The spaces are required before and after the dash ( - ) and before and after the comma ( , ).



**Note** For Cisco MDS 9500, 9700 and 9250i Series Switches support ethernet , vfc, vfc-port-channel and ethernet-port-channel commands.

**Examples**

The following example selects the mgmt 0 interface and enters interface configuration submode:

```
switch# config terminal
switch(config)# interface mgmt 0
```

**Related Commands**

Command	Description
<b>show interface</b>	Displays an interface configuration for a specified interface.

# interface fc

To configure a Fibre Channel interface on the Cisco MDS 9000 Family of switches, use the **interface fc** command in EXEC mode. To revert to defaults, use the **no** form of the command.

```
interface fc slot/port channel-group {group-id [force] | auto} fcdomain rcf-reject vsan vsan-id
fcsp
| fspf {cost link-cost vsan vsan-id | ficon portnumber portnumber | dead-interval seconds vsan
vsan-id | hello-interval seconds vsan vsan-id | passive vsan vsan-id | retransmit-interval seconds
vsan vsan-id}
nointerface fc slot/port channel-group {group-id [force] | auto} fcdomain rcf-reject vsan vsan-id
no fspf {cost link-cost vsan vsan-id | ficon portnumber portnumber | dead-interval seconds vsan
vsan-id | hello-interval seconds vsan vsan-id | passive vsan vsan-id | retransmit-interval seconds
vsan vsan-id}
```

## Syntax Description

<i>slot/port</i>	Specifies a slot number and port number.
<b>channel-group</b>	Add to or remove chaneel group from a Port Channel.
<i>group-id</i>	Specifies a Port Channel group number from 1 to 128.
<b>force</b>	(Optional) Forcefully adds a port.
<b>auto</b>	Enables autocreation of Port Channels.
<b>fcdomain</b>	Enters the interface submenu.
<b>rcf-reject</b>	Configures the rcf-reject flag.
<b>vsan vsan-id</b>	Specifies the VSAN ID. The range is 1 to 4093.
<b>fcsp</b>	Configures the FCSP for an interface.
<b>fspf</b>	Configures FSPF parameters.
<b>cost link-cost</b>	Configures FSPF link cost. The range is 1 to 30000.
<b>ficon</b>	Configures FICON parameters.
<b>portnumber portnumber</b>	Configures the FICON port number for this interface.
<b>dead-interval seconds</b>	Configures FSPF dead interval in seconds. The range is 2 to 65535.
<b>hello-interval seconds</b>	Configures FSPF hello-interval. The range is 1 to 65535.
<b>passive</b>	Enables or disables FSPF on the interface.
<b>retransmit-interval seconds</b>	Configures FSPF retransmit interface in seconds. The range is 1 to 65535.

## Command Default

Disabled.

**Command Modes**

Configuration mode.

**Command History**

Release	Modification
NX-OS 4.2(1)	Added fcsp keyword for the syntax description.
1.0(2)	This command was introduced.
2.0(x)	Added the <b>auto</b> option to the <b>channel-group</b> keyword.

**Usage Guidelines**

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

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

Use the **no shutdown** command to enable the interface.

The **channel-group auto** command enables autocreation of Port Channels. If autocreation of Port Channels is enabled for an interface, you must first disable this configuration before downgrading to earlier software versions or before configuring the interface in a manually configured channel group.

**Examples**

The following example configures ports 1 to 4 in Fibre Channel interface 9:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# int fc9/1 - 4
```

The following example enables the Fibre Channel interface:

```
switch# config terminal
switch(config)# interface fc1/1
switch(config-if)# no shutdown
```

The following example assigns the FICON port number to the selected Fibre Channel interface:

```
switch# config terminal
switch(config)# interface fc1/1
switch(config-if)# ficon portnumber 15
```

**Related Commands**

Command	Description
<b>show interface</b>	Displays an interface configuration for a specified interface.
<b>shutdown</b>	Disables and enables an interface.

# interface fcip

To configure a Fibre Channel over IP Protocol (FCIP) interface, use the **interface fcip** command. To disable a FCIP interface, use the **no** form of the command.

```
interface fcip interface_number bport bport-keepalives channel-group number [force] fcdomain
rcf-reject vsan vsan-id ficon portnumber portnumber|fspf {cost link-cost|dead-interval seconds
|hello-interval seconds|passive|retransmit-interval seconds} vsan vsan-id passive-mode peer-info
ipaddr ip-address [port number] qos control control-value data data-value special-frame peer-wnn
pwwn-id tcp-connections number time-stamp [acceptable-diff number] use-profile profile-id
no interface fcip interface_number bport bport-keepalives channel-group number [force] fcdomain
rcf-reject vsan vsan-id ficon portnumber portnumber fspf {cost link-cost|dead-interval seconds
|hello-interval seconds|passive|retransmit-interval seconds} vsan vsan-id qos control-value data
data-value passive-mode peer-info ipaddr ip-address [port number] special-frame peer-wnn
pwwn-id tcp-connections number time-stamp [acceptable-diff number] use-profile profile-id
```

## Syntax Description

<i>interface-number</i>	Configures the specified interface from 1 to 255.
<b>bport</b>	Sets the B port mode.
<b>bport-keepalives</b>	Sets the B port keepalive responses.
<b>channel-group number</b>	Specifies a PortChannel number from 1 to 128.
<b>force</b>	(Optional) Forcefully adds a port.
<b>fcdomain</b>	Enters the fcdomain mode for this FCIP interface
<b>rcf-reject</b>	Configures the rcf-reject flag.
<b>vsan vsan-id</b>	Specifies a VSAN ID. The range is 1 to 4093.
<b>ficon</b>	Configures FICON parameters.
<b>portnumber portnumber</b>	Configures the FICON port number for this interface.
<b>fspf</b>	Configures FSPF parameters.
<b>cost link-cost</b>	Enters FSPF link cost. The range is 1 to 30000.
<b>dead-interval seconds</b>	Specifies the dead interval in seconds. The range is 1 to 65535.
<b>hello-interval seconds</b>	Specifies FSPF hello-interval in seconds. The range is 1 to 65535.
<b>passive</b>	Enables or disables FSPF on the interface.
<b>retransmit-interval</b>	Specifies FSPF retransmit interface in seconds. The range is 1 to 65535.
<b>passive-mode</b>	Configures a passive connection.
<b>peer-info</b>	Configures the peer information.
<b>ipaddr ip-address</b>	Specifies the peer IP address.

<b>port</b> <i>number</i>	(Optional) Specifies the peer port number. The range is 1 to 65535.
<b>qos</b>	Configures the differentiated services code point (DSCP) value to mark all IP packets.
<b>control</b> <i>control-value</i>	Specifies the control value for DSCP.
<b>data</b> <i>data-value</i>	Specifies the data value for DSCP.
<b>special-frame</b>	Configures special frames.
<b>peer-wwn</b> <i>pwwn-id</i>	Specifies the peer WWN for special frames.
<b>switchport</b>	Configures switchport parameters.
<b>tcp-connections</b> <i>number</i>	Specifies the number of TCP connection attempts. Valid values are 1 or 2.
<b>time-stamp</b>	Configures the time stamp.
<b>acceptable-diff</b> <i>number</i>	(Optional) Specifies the acceptable time difference for time stamps. The range is 1 to 60000.
<b>use-profile</b> <i>profile-id</i>	Specifies the interface using an existing profile ID. The range is 1 to 255.

**Command Default**

Disabled.

**Command Modes**

Configuration mode.

**Command History**

Release	Modification
1.1(1)	This command was introduced.
1.3(1)	Added the <b>ficon portnumber</b> subcommand.
2.0(x)	Added the <b>qos</b> subcommand.

**Usage Guidelines**

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

```
interface fcip1space-space5space,spacefcip10space-space12space
```

**Examples**

The following example selects an FCIP interface and enters interface configuration submode:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface fcip 1
switch(config-if)#
```

The following example assigns the FICON port number to the selected FCIP interface:

```
switch# config terminal
switch(config)# interface fcip 51
switch(config-if)# ficon portnumber 234
```

---

**Related Commands**

Command	Description
<b>show interface fcip</b>	Displays an interface configuration for a specified FCIP interface.

# interface fc-tunnel

To configure a Fibre Channel tunnel and facilitate RSPAN traffic, use the **interface fc-tunnel** command. To remove a configured tunnel or revert to factory defaults, use the **no** form of the command.

**interface fc-tunnel** {*number destination ip-address* | **explicit-path** *path-name source ip-address*}  
**nointerface fc-tunnel** {*number destination ip-address* | **explicit-path** *path-name source ip-address*}

## Syntax Description

<i>number</i>	Specifies a tunnel ID range from 1 to 255.
<b>destination</b> <i>ip-address</i>	Maps the IP address of the destination switch.
<b>explicit-path</b> <i>path-name</i>	Specifies a name for the explicit path. Maximum length is 16 alphanumeric characters.
<b>source</b> <i>ip-address</i>	Maps the IP address of the source switch.

## Command Default

None.

## Command Modes

Configuration mode.

## Command History

Release	Modification
1.2(1)	This command was introduced.

## Usage Guidelines

None.

## Examples

The following example initiates the FC tunnel (100) in the source switch (switch S):

```
switch(config)# config terminal
switch(config)# interface fc-tunnel 100
switch(config-if)#
```

The following example maps the IP address of the source switch (switch S) to the FC tunnel (100):

```
switchS(config-if)# source 209.165.200.226
```

The following example maps the IP address of the destination switch (switch D) to the FC tunnel (100):

```
switch(config-if)# destination 209.165.200.227
```

The following example enables traffic flow through this interface:

```
switch(config-if)# no shutdown
```

The following example references the configured path in the source switch (switch S):

```
switch# config t
```

```
switch(config)# interface fc-tunnel 100  
switch(config)# explicit-path Path1
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>fc-tunnel explicit-path</b>	Configures a new or existing next-hop path.
<b>show interface fc-tunnel</b>	Displays an FC tunnel interface configuration for a specified interface.



# interface gigabitethernet

To configure an Gigabit Ethernet interface, use the **interface gigabitethernet** command. To revert to the default values, use the **no** form of the command.

**interface gigabitethernet** *slot/port* **cdp enable channel-group** *group-id* [**force**] **isns** *profile-name*  
**nointerfacegigabitethernet** *slot/port* **cdp enable channel-group isns** *profile-name*

Syntax Description		
	<i>slot/port</i>	Specifies a slot number and port number.
	<b>cdp enable</b>	Enables Cisco Discovery Protocol (CDP) configuration parameters.
	<b>channel-group</b> <i>group-id</i>	Adds to or removes from a PortChannel. The range is 1 to 128.
	<b>force</b>	(Optional) Forcefully adds a port.
	<b>isns</b> <i>profile-name</i>	Specifies the profile name to tag the interface. Maximum length is 64 characters.

**Command Default** Disabled.

**Command Modes** Configuration mode.

Command History	Release	Modification
	1.0(3a)	This command was introduced.
	1.1(1a)	Added the <b>channel-group</b> subcommand.
	1.3(1)	Added the <b>isns</b> subcommand.

**Usage Guidelines** You can specify a range of interfaces by issuing a command with the following example format:  
**interfacegigabitethernet1/1space-space2space,space gigabitethernet3/1space-space2**

## Examples

The following example configures the Gigabit Ethernet interface at slot 4 port 1:

```
switch# config terminal
switch(config)# interface gigabitethernet 4/1
switch(config-if)#
```

The following example enters a IP address and subnet mask for the selected Gigabit Ethernet interface:

```
switch(config-if)# ip address 209.165.200.226 255.255.255.0
```

The following example changes the IP maximum transmission unit (MTU) value for the selected Gigabit Ethernet interface:

```
switch(config-if)# switchport mtu 3000
```

The following example creates a VR ID for the selected Gigabit Ethernet interface, configures the virtual IP address for the VR ID (VRRP group), and assigns a priority:

```
switch(config-if)# vrrp 100
switch(config-if-vrrp)# address 209.165.200.226
switch(config-if-vrrp)# priority 10
```

The following example adds the selected Gigabit Ethernet interface to a channel group. If the channel group does not exist, it is created, and the port is shut down:

```
switch(config-if)# channel-group 10

gigabitethernet 4/1 added to port-channel 10 and disabled
please do the same operation on the switch at the other end of the port-channel, then do
"no shutdown" at both ends to bring them up.
```

#### Related Commands

Command	Description
<b>show interface</b>	Displays an interface configuration for a specified interface.

# interface ioa

To configure an IOA interface, use the **interface ioa** command. To disable this feature, use the **no** form of the command.

```
interface ioa {slot/port}
no interface ioa {slot/port}
```

<b>Syntax Description</b>	<i>slot /port</i>	Specifies IOA slot or port number. The range is from 1 to 16 for the slot and for the port. The range is from 1 to 4.
---------------------------	-------------------	---

**Command Default** None.

**Command Modes** Configuration mode.

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

**Usage Guidelines** None.

**Examples** The following example shows how to configure an IOA interface for a specific cluster:

```
switch(config)# interface ioa2/1

2009 May 19 18:33:08 sjc-sw2 %IOA-2-LOG_LIBBASE_SVC_LICENSE_ON_GRACE_PERIOD: (pid=8582) No
license. Feature will be shut down after a grace period of approximately 107 days

switch(config-if)# no shutdown
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show ioa cluster summary</b>	Displays the summary of all the IOA cluster.

# interface iscsi

To configure an iSCSI interface, use the **interface iscsi** command. To revert to default values, use the **no** form of the command.

**interface iscsi** *slot/port* **mode** {**pass-thru** | **store-and-forward** | **cut-thru**} **tcp qos** *value*  
**nointerface iscsi** *slot/port* **mode** {**pass-thru** | **store-and-forward** | **cut-thru**} **tcp qos** *value*

<i>slot/port</i>	Specifies a slot number and port number.
<b>mode</b>	Configures a forwarding mode.
<b>pass-thru</b>	Forwards one frame at a time.
<b>store-and-forward</b>	Forwards data in one assembled unit (default).
<b>cut-thru</b>	Forwards one frame at a time without waiting for the exchange to complete.
<b>tcp qos</b> <i>value</i>	Configures the differentiated services code point (DSCP) value to apply to all outgoing IP packets. The range is 0 to 63.

## Command Default

Disabled.

The TCP QoS default is 0.

The forwarding mode default is store-and-forward.

## Command Modes

Configuration mode.

## Command History

Release	Modification
1.3(1)	This command was introduced.
2.1(1)	Added the <b>cut-thru</b> option for the <b>mode</b> subcommand.

## Usage Guidelines

To configure iSCSI interface, enable iSCSI using the **iscsi enable** command.

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

```
interface iscsi space fc1/1space -space 5space ,space fc2/5space -space 7
```

## Examples

The following example enables the iSCSI feature:

```
switch# config t  
switch(config)# iscsi enable
```

The following example enables the store-and-forward mode for iSCSI interfaces 9/1 to 9/4:

```
switch(config)# interface iscsi 9/1 - 4  
switch(config-if)# mode store-and-forward
```

The following example reverts to using the default pass-thru mode for iSCSI interface 9/1:

```
switch(config)# interface iscsi 9/1  
switch(config-if)# mode pass-thru
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>iscsi enable</b>	Enables iSCSI.
<b>show interface</b>	Displays an interface configuration for a specified interface.

# interface mgmt

To configure a management interface, use the **interface mgmt** command in configuration mode.

**interface mgmt** *number*

## Syntax Description

<i>number</i>	Specifies the management interface number which is 0.
---------------	---

## Command Default

Disabled.

## Command Modes

Configuration mode.

## Command History

Release	Modification
1.0(2)	This command was introduced.

## Usage Guidelines

When you try to shut down a management interface(mgmt0), a follow-up message confirms your action before performing the operation. Use the **force** option to bypass this confirmation, if required.

## Examples

The following example configures the management interface, displays the options available for the configured interface, and exits to configuration mode:

```
switch# config terminal
switch(config)#
switch(config)# interface mgmt 0
switch(config-if)# exit
switch(config)#
```

The following example shuts down the interface without using the **force** option:

```
switch# config terminal
switch(config)# interface mgmt 0
switch(config-if)# shutdown
Shutting down this interface will drop all telnet sessions.
Do you wish to continue (y/n)? y
```

The following example shuts down the interface using the **force** option:

```
switch# config terminal
switch(config)# interface mgmt 0
switch(config-if)# shutdown force
switch(config-if)#
```

## Related Commands

Command	Description
<b>show interface mgmt</b>	Displays interface configuration for specified interface.

# interface port-channel

To configure a PortChannel interface, use the **interface port-channel** command. To remove this configuration, use the **no** form of the command.

```
interface port-channel number channel mode active fcdomain rcf-reject vsan vsan-id fspf [cost
link_cost | dead-interval seconds | ficon portnumber portnumber | hello-interval seconds | isns
profile-name | passive | retransmit-interval seconds]
no interface port-channel number
```

## Syntax Description

<i>number</i>	Specifies the PortChannel number. The range is 1 to 128.
<b>channel mode active</b>	Configures the channel mode for the PortChannel interface.
<b>fcdomain</b>	Specifies the interface submodule.
<b>rcf-reject</b>	Configures the rcf-reject flag.
<b>vsan</b>	Specifies the VSAN range.
<i>vsan-id</i>	Specifies the ID of the VSAN is from 1 to 4093.
<b>fspf</b>	Configures the FSPF parameters.
<b>cost</b>	(Optional) Configures the FSPF link cost.
<i>link_cost</i>	Specifies the FSPF link cost which is 1-30000.
<b>dead-interval</b>	(Optional) Configures the FSPF dead interval.
<i>seconds</i>	Specifies the dead interval (in seconds) from 2-65535.
<b>ficon</b>	(Optional) Configures the FICON parameters.
<b>portnumber</b> <i>portnumber</i>	(Optional) Configures the FICON port number for this interface.
<b>hello-interval</b>	(Optional) Configures FSPF hello-interval.
<i>seconds</i>	Specifies the hello interval (in seconds) from 1-65535.
<b>isns</b>	(Optional) Tags this interface to the Internet Storage Name Service (iSNS) profile.
<i>profile-name</i>	Specifies the profile name to tag the interface.
<b>passive</b>	(Optional) Enable/disable FSPF on the interface.
<b>retransmit-interval</b>	(Optional) Configures FSPF retransmit interface.
<i>seconds</i>	Specifies the retransmit interval (in seconds) from 1-65535.

## Command Default

Prior to Cisco MDS NX-OS Release 8.3(1), the CLI and the Device Manager create the PortChannel in On mode in the NPIV core switches and Active mode on the NPV switches. DCNM-SAN creates all PortChannels in Active mode.

From Cisco MDS NX-OS Release 8.4(1), the CLI and the Device Manager create the PortChannel in Active mode in the NPIV core switches.

### Command Modes

Configuration mode.

### Command History

Release	Modification
1.0(2)	This command was introduced.
1.3(1)	Added <b>channel mode active</b> subcommand.
8.4(1)	This command was modified to change the default PortChannel mode from On to Active.

### Usage Guidelines

Prior to Cisco MDS NX-OS Release 8.3(1), the CLI and the Device Manager create the PortChannel in On mode in the NPIV core switches and Active mode on the NPV switches. DCNM-SAN creates all PortChannels in Active mode. We recommend that you create PortChannels in Active mode.

From Cisco MDS NX-OS Release 8.4(1), the CLI and the Device Manager create the PortChannel in Active mode in the NPIV core switches.

### Examples

The following example enters configuration mode and configures a PortChannel interface:

```
switch# config terminal
switch(config)# interface port-channel 32
switch(config-if)#
```

The following example assigns the FICON port number to the selected PortChannel port:

```
switch# config terminal
switch(config)# interface Port-channel 1
switch(config-if)# ficon portnumber 234
```

### Related Commands

Command	Description
<b>show interface</b>	Displays interface configuration for specified interface.



## interface sme

To configure the Cisco SME interface on a switch, use the **interface sme** command. To remove the interface, use the **no** form of the command,

```
interface sme slot /port
no interface sme slot /port
```

### Syntax Description

<i>slot</i>	Identifies the number of the MPS-18/4 module slot.
<i>port</i>	Identifies the number of the Cisco SME port.

### Command Default

Disabled.

### Command Modes

Configuration mode.

### Command History

Release	Modification
3.2(2)	This command was introduced.

### Usage Guidelines

To use this command, clustering must be enabled using the **cluster enable** command and Cisco SME services must be activated using the sme enable command.

Once you have configured the interface, use the **no shutdown** command to enable the interface.

To delete the Cisco SME interface, you must first remove the switch from the cluster. Use the **no sme cluster** command to remove the switch from the cluster and then use the **no interface** command to delete the interface.

The interface commands are available in the (**config-if**) submode.

### Examples

The following example configures and enables the Cisco SME interface on the MPS-18/4 module slot and the default Cisco SME port:

```
switch# config terminal
switch(config)# interface sme 3/1
switch(config-if)# no shutdown
```

### Related Commands

Command	Description
<b>show interface sme</b>	Displays interface information.
<b>shutdown</b>	Enables or disables an interface.

# interface sme (Cisco SME cluster node configuration submode)

To add Cisco SME interface from a local or a remote switch to a cluster, use the **interface sme** command. To delete the interface, use the **no** form of the command.

```
interface sme {slot/port} [force]
no interface sme {slot/port} [force]
```

## Syntax Description

<i>slot</i>	Identifies the MPS-18/4 module slot.
<i>port</i>	Identifies the Cisco SME port.
<b>force</b>	(Optional) Forcibly clears the previous interface context in the interface.

## Command Default

Disabled.

## Command Modes

Cisco SME cluster node configuration submode.

## Command History

Release	Modification
3.2(2)	This command was introduced.

## Usage Guidelines

You have to first configure a node using the **fabric-membership** command before this command can be executed.

To use this command, clustering must be enabled using the **cluster enable** command and Cisco SME services must be activated using the **sme enable** command.

To delete the Cisco SME interface, first remove the switch from the cluster. Use the **no sme cluster** command to remove the switch from the cluster and then use the **no interface** command to delete the interface.

## Examples

The following example specifies the fabric to which the node belongs and then adds the Cisco SME interface (4/1) from a local switch using the force option:

```
switch# config terminal
switch(config)# sme cluster clustername1
switch(config-sme-cl)# node local
switch(config-sme-cl-node)# fabric-membership f1
switch(config-sme-cl-node)# interface sme 4/1 fabric sw-xyz
```

The following example specifies the fabric to which the node belongs and then adds the Cisco SME interface (4/1) from a remote switch using the force option:

```
switch# config terminal
switch(config)# sme cluster clustername1
switch(config-sme-cl)# node 171.71.23.33
switch(config-sme-cl-node)# fabric-membership f1
switch(config-sme-cl-node)# interface sme 4/1 fabric sw-xyz
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>fabric-membership</b>	Adds the node to a fabric.
<b>show interface</b>	Displays Cisco SME interface details.

# interface vsan

To configure a VSAN interface, use the **interface vsan** command. To remove a VSAN interface, use the **no** form of the command.

```
interface vsan vsan-id
no interface vsan vsan-id
```

## Syntax Description

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

## Command Default

Disabled.

## Command Modes

Configuration mode.

## Command History

Release	Modification
1.0(2)	This command was introduced.

## Usage Guidelines

None.

## Examples

The following example selects a VSAN interface and enters interface configuration submode:

```
switch# config terminal
switch(config)# interface vsan 1
switch(config-if)#
```

## Related Commands

Command	Description
<b>show interface</b>	Displays interface configuration for specified interface.

# intersight connection

To configure the DNS name for intersight connection on a switch, use the **intersight connection** command. Use the **no** form of this command to not configure the DNS name for intersight connection.

**intersight connection** *name*  
**no intersight connection** *name*

Syntax Description	connection	Specifies the destination name for intersight
	<i>name</i>	Specifies the destination host name

**Command Default** Disabled

**Command Modes** Configuration mode (config)

Command History	Release	Modification
	9.3(2)	This command was introduced.

**Usage Guidelines** None

**Examples** The following example shows how to enable the Intersight feature on a switch:

```
switch# configure terminal
switch(config)# intersight connection testconnect.starshipcloud.com
```

Related Commands	Command	Description
	<b>feature intersight</b>	Enables the feature intersight.
	<b>intersight proxy</b>	Configures the proxy server for intersight connection.
	<b>intersight trustpoint</b>	Configures the certificates for the intersight connection.
	<b>show system internal intersight info</b>	Displays the device connector information.
	<b>show system internal intersight connection state</b>	Displays the status of the connection of the devices.

# intersight proxy

To configure the proxy server for the intersight connection on a switch, use the **intersight proxy** command. Use the **no** form of this command to not configure the proxy server connection.

```
intersight proxy proxy-server port proxy-port
no intersight proxy proxy-server port proxy-port
```

## Syntax Description

<b>proxy</b>	Configure the proxy server, ipv4/ipv6/hostname.
<i>proxy-server</i>	IPv4 or IPv6 address or DNS name of proxy server
<b>port</b>	(Optional) Configure the proxy server port
<i>proxy-port</i>	(Optional) Proxy port number. The range is 1-65535. The default value is 8080.

## Command Default

Disabled

## Command Modes

Configuration mode (config)

## Command History

Release	Modification
9.3(2)	This command was introduced.

## Usage Guidelines

None

## Examples

The following example shows how to enable the Intersight feature on a switch:

```
switch# configure terminal
switch(config)# intersight proxy proxy server proxy.esl.cisco.com port 8080
```

## Related Commands

Command	Description
<b>feature intersight</b>	Enables the feature intersight.
<b>intersight connection</b>	Configures the DNS name for the intersight connection.
<b>intersight trustpoint</b>	Configures the certificates for the intersight connection.
<b>show system internal intersight info</b>	Displays the device connector information.
<b>show system internal intersight connection state</b>	Displays the status of the connection of the devices.

# intersight trustpoint

To configure the certificates for intersight connection on a switch, use the **intersight trustpoint** command. Use the **no** form of this command to not configure the certificates for intersight connection.

**intersight trustpoint** *trustpoint-label*

**no intersight trustpoint** *trustpoint-label*

Syntax Description	trustpoint	Specifies the certificates for intersight
	<i>trustpoint-label</i>	Specifies the Crypto ca trustpoint label

**Command Default** Disabled

**Command Modes** Configuration mode (config)

Command History	Release	Modification
	9.3(2)	This command was introduced.

**Usage Guidelines** None

**Examples** The following example shows how to enable the Intersight feature on a switch:

```
switch# configure terminal
switch(config)# intersight trustpoint mds-stage-onprem
```

Related Commands	Command	Description
	<b>feature intersight</b>	Enables the feature intersight.
	<b>intersight proxy</b>	Configures the proxy server for intersight connection.
	<b>intersight connection</b>	Configures the DNS name for the intersight connection.
	<b>show system internal intersight info</b>	Displays the device connector information.
	<b>show system internal intersight connection state</b>	Displays the status of the connection of the devices.

# ioa cluster

To configure an IOA cluster, use the **ioa cluster** command. To disable this feature, use the **no** form of the command.

**ioa cluster** {*cluster name*}  
**no ioa cluster** {*cluster name*}

## Syntax Description

<i>cluster name</i>	Specifies an IOA cluster name.
---------------------	--------------------------------

## Command Default

None.

## Command Modes

Configuration mode.

## Command History

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

## Usage Guidelines

None.

## Examples

The following example shows how to configure an IOA cluster:

```
switch(config)# ioa cluster tape_vault
switch#(config-ioa-cl)#
```

## Related Commands

Command	Description
<b>show ioa cluster</b>	Displays detailed information of all the IOA cluster.



## ioa site-local

To configure an IOA site, use the **ioa site-local** command. To disable this feature, use the **no** form of the command.

```
ioa site-local {site name}
no ioa site-local {site name}
```

### Syntax Description

<i>site name</i>	Specifies an IOA site name. The maximum name length is restricted to 31 alphabetical characters.
------------------	--

### Command Default

None.

### Command Modes

Configuration mode.

### Command History

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

### Usage Guidelines

None.

### Examples

The following example shows how to configure an IOA local site:

```
switch# config t
switch(config)# ioa site-local SJC
switch#(config)#
```

### Related Commands

Command	Description
<b>ioa enable</b>	Enables or disables the I/O Accelerator.

# ioa-ping

To validate the connectivity between the master switch and the specified target device (for a specific flow), use the **ioa-ping** command.

**ioa-ping host** *hpwwn* **target** *tpwwn* **vsan** *vid* **interface** *if0*

## Syntax Description

<b>host</b>	Specifies the host address.
<i>hpwwn</i>	Specifies the host PWWN for the flow.
<b>target</b>	Specifies the target address.
<i>tpwwn</i>	Specifies the target PWWN for the flow.
<b>vsan</b>	Specifies the VSAN.
<i>vid</i>	Specifies the VSAN ID. The range is from 1 to 4093.
<b>interface</b>	Specifies the interface associated with the flow.
<i>if0</i>	Specifies the ioa interface for the flow over which the test unit ready commands will be sent.

## Command Default

Prompts for user input.

## Command Modes

EXEC mode.

## Command History

Release	Modification
NX-OS 6.2(5)	This command was introduced.

## Usage Guidelines

None.



**Note** **ioa-ping** will work from 6.2(5) onwards and the command has to be executed from IOA master switch only.

## Examples

The following example shows how to validate the connectivity between the master switch and the specified target device:

```
switch# ioa-ping host 10:00:00:00:11:a1:01:0a target 50:0a:09:80:11:4b:01:0a vsan 11 interface
ioa 1/1

1: Round Trip Time   inf msec Device status 0
2: Round Trip Time   inf msec Device status 0
3: Round Trip Time   inf msec Device status 0
4: Round Trip Time   inf msec Device status 0
5: Round Trip Time   inf msec Device status 0
```

```
5 transmitted, 5 received ,rtt min/avg/max = inf/ inf/ inf (msec)
switch#
```

**Related Commands**

Command	Description
<b>show ioa cluster</b>	Displays detailed information of all the IOA cluster.

# ip access-group

To apply an access list to an interface, use the **ip access-group** command in interface mode. Use the **no** form of this command to negate a previously issued command or revert to factory defaults.

**ip access-group** *access-list-name* [**in** | **out**]

## Syntax Description

<i>access-list-name</i>	Specifies the IP access list name. The maximum length is 64 alphanumeric characters and the text is case insensitive.
<b>in</b>	(Optional) Specifies that the group is for ingress traffic.
<b>out</b>	(Optional) Specifies that the group is for egress traffic.

## Command Default

The access list is applied to both ingress and egress traffic.

## Command Modes

Interface mode.

## Command History

Release	Modification
1.2(1)	This command was introduced.

## Usage Guidelines

The **ip access-group** command controls access to an interface. Each interface can only be associated with one access list. The access group becomes active immediately.

We recommend creating all rules in an access list, before creating the access group that uses that access list.

If you create an access group before an access list, the access list is created and all packets in that interface are dropped, because the access list is empty.

The access-group configuration for the ingress traffic applies to both local and remote traffic. The access-group configuration for the egress traffic applies only to local traffic. You can apply a different access list for each type of traffic.

## Examples

The following example creates an access group called `aclPermit` for both the ingress and egress traffic (default):

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip access-list aclPermit permit ip any any
switch(config)# interface GigabitEthernet 3/1
switch(config-if)# ip access-group aclPermit
```

The following example deletes the access group called `aclPermit`:

```
switch(config-if)# no ip access-group aclPermit
```

The following example creates an access group called `aclDenyTcp` (if it does not already exist) for ingress traffic:

```

switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip access-list aclDenyTcp deny tcp any any
switch(config)# interface gigabitethernet 3/1
switch(config-if)# ip access-group aclDenyTcp in

```

The following example deletes the access group called aclDenyTcp for ingress traffic:

```

switch(config-if)# no ip access-group aclDenyTcp in

```

The following example creates an access list called aclPermitUdp (if it does not already exist) for local egress traffic:

```

switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip access-list aclPermitUdp permit udp 192.168.32.0 0.0.7.255 any
switch(config)# interface gigabitethernet 3/1
switch(config-if)# ip access-group aclPermitUdp out

```

The following example removes the access list called aclPermitUdp for local egress traffic:

```

switch(config-if)# no ip access-group aclPermitUdp out

```

#### Related Commands

Command	Description
<b>ip access-list</b>	Configures IP access control lists.
<b>show ip access-list</b>	Displays the IP-ACL configuration information.

## ip access-list

IP access control lists can be used to filter IP packets through an interface. To configure IPv4 access control lists (ACLs), use the **ip access-list** command. To remove a line from an access list or completely remove the access list, use the corresponding **no** form of this command.

```
ip access-list name { permit | deny } protocol { any | src-ip src-mask } [ source-ports ]
{ any | dst-ip dst-mask } [ destination-ports ] [ options ]
no ip access-list name { permit | deny } protocol { any | src-ip src-mask } [ source-ports ]
{ any | dst-ip dst-mask } [ destination-ports ] [ options ]
no ip access-list name
```

where:

- *protocol*—{**icmp** | **ip** | **tcp** [**flags** {[**ack**] } {[**all**] } {[**fin**] } {[**psh**] } {[**rst**] } {[**syn**] } {[**urg**] }]} | **udp** | *protocol-num*}
- *source-ports*—[**eq port** {**dns** | **ftp** | **ftp-data** | **http** | **ntp** | **radius** | **sftp** | **smtp** | **snmp** | **snmp-trap** | **ssh** | **syslog** | **tacacs-ds** | **tacacs-plus** | **telnet** | **tftp** | **www** | **wbem-http** | **wbem-https** | *port-num*} | **gt port port-num-low** | **lt port port-num-high** | **range port port-num-low port-num-high**]
- *destination-ports*—[**eq port** {**dst\_dns** | **dst\_ftp** | **dst\_ftp-data** | **dst\_http** | **dst\_ntp** | **dst\_radius** | **dst\_sftp** | **dst\_smtp** | **dst\_snmp** | **dst\_snmp-trap** | **dst\_ssh** | **dst\_syslog** | **dst\_tacacs-ds** | **dst\_tacacs-plus** | **dst\_telnet** | **dst\_tftp** | **dst\_www** | **dst\_wbem-http** | **dst\_wbem-https** | *port-num*} | **gt port port-num-low** | **lt port port-num-high** | **range port port-num-low port-num-high**]
- *options*—[**established** | **icmp-type** {**echo** | **echo-reply** | **redirect** | **time-exceeded** | **unreachable** | **traceroute** | *icmp-msg-num*} | **icmp-code** *icmpcode-num*] [**tos** {**delay** | **throughput** | **reliability** | **monetary-cost** | **normal service**}] [**log-deny**]

### Syntax Description

<i>name</i>	Specifies an access list name. The maximum length is 28 alphanumeric characters.
<b>deny</b>	Drops the packet if the conditions match.
<b>permit</b>	Forwards the packet if the conditions match.
<i>protocol</i>	Specifies the name or number (integer range from 0 to 255) of an IP protocol. The IP protocol name can be <b>icmp</b> , <b>ip</b> , <b>tcp</b> , or <b>udp</b> .

<b>flags</b> <i>flag-set</i>	(Optional) Specifies TCP header flags to match. Multiple flags may be specified, separated by spaces.  The available flag names are:  <b>all</b> —Any TCP flag.  <b>psh</b> —The Push flag. It indicates the data should be immediately pushed through to the receiving user.  <b>fin</b> —The Finish flag. It is used to clear connections.  <b>rst</b> —Reset flag. It indicates that the receiver should delete the connection without further interaction.  <b>syn</b> —The Synchronize flag. It is used to establish connections.  <b>urg</b> —The Urgent flag. It indicates that the urgent field is meaningful and must be added to the segment sequence number.
<b>any</b>	Specifies any source or destination IP address. The <b>any</b> keyword is synonymous to the address 0.0.0.0 and wildcard mask 255.255.255.255.
<i>src-ip</i> <i>src-mask</i>	Specifies the network from which the packet is sent. Mask bits are <i>0</i> for match and <i>1</i> for don't care.
<i>dst-ip</i> <i>dst-mask</i>	Specifies the network to which the packet is to be sent. Mask bits are <i>0</i> for match and <i>1</i> for don't care.

<i>source-ports</i>	<p>Specifies a set of source ports to match.</p> <p>The syntax of this block is:</p> <p><i>operator port-set</i></p> <p>The following operators are available:</p> <ul style="list-style-type: none"><li><b>eq</b>— equal to</li><li><b>gt</b>— greater than and including</li><li><b>lt</b>— less than and including</li><li><b>range</b>— a range of source ports (inclusive)</li></ul> <p>The <i>port-set</i> is a single value for the <b>eq</b>, <b>gt</b>, <b>lt</b> operators and a pair of space separated ports, in low port high port order, for the <b>range</b> operator. Ports may be specified as a number or a name. The range for numbers is 0 to 65535.</p> <p>The available names are as follows.</p> <p>TCP:</p> <ul style="list-style-type: none"><li><b>ftp-data</b> (20)</li><li><b>ftp</b> (21)</li><li><b>ssh</b> (22)</li><li><b>telnet</b> (23)</li><li><b>smtp</b> (25)</li><li><b>tacacs-plus</b> (49)</li><li><b>tacacs-ds</b> (65)</li><li><b>www</b> (80)</li><li><b>sftp</b> (115)</li><li><b>http</b> (143)</li><li><b>radius</b> (1812)</li><li><b>wbem-http</b> (5988)</li><li><b>wbem-https</b> (5989)</li></ul> <p>UDP:</p> <ul style="list-style-type: none"><li><b>dns</b> (53)</li><li><b>tftp</b> (69)</li><li><b>ntp</b> (123)</li><li><b>snmp</b> (161)</li><li><b>snmp-trap</b> (162)</li><li><b>syslog</b> (514)</li></ul>
---------------------	---



<i>destination-ports</i>	<p>Specifies a set of destination ports to match.</p> <p>The syntax of this block is:</p> <p><i>operator port-set</i></p> <p>The following operators are available:</p> <ul style="list-style-type: none"> <li><b>eq</b>— equal to</li> <li><b>gt</b>— greater than and including</li> <li><b>lt</b>— less than and including</li> <li><b>range</b>— a range of source ports (inclusive)</li> </ul> <p>The <i>port-set</i> is a single value for the <b>eq</b>, <b>gt</b>, <b>lt</b> operators and a pair of space separated ports, in low port high port order, for the <b>range</b> operator. Ports may be specified as a number or a name. The range for numbers is 0 to 65535.</p> <p>The available names are as follows.</p> <p>TCP:</p> <ul style="list-style-type: none"> <li><b>dst_ftp-data</b> (20)</li> <li><b>dst_ftp</b> (21)</li> <li><b>dst_ssh</b> (22)</li> <li><b>dst_telnet</b> (23)</li> <li><b>dst_smtp</b> (25)</li> <li><b>dst_tacacs-plus</b> (49)</li> <li><b>dst_tacacs-ds</b> (65)</li> <li><b>dst_www</b> (80)</li> <li><b>dst_sftp</b> (115)</li> <li><b>dst_http</b> (143)</li> <li><b>dst_radius</b> (1812)</li> <li><b>dst_wbem-http</b> (5988)</li> <li><b>dst_wbem-https</b> (5989)</li> </ul> <p>UDP:</p> <ul style="list-style-type: none"> <li><b>dst_dns</b> (53)</li> <li><b>dst_tftp</b> (69)</li> <li><b>dst_ntp</b> (123)</li> <li><b>dst_snmp</b> (161)</li> <li><b>dst_snmp-trap</b> (162)</li> <li><b>dst_syslog</b> (514)</li> </ul>
--------------------------	--

<b>icmp-type</b> <i>icmp-value</i>	Optional) Specifies an ICMP message type to match. <i>icmp-value</i> may be a number or a name. The range for numbers is 0 to 255.  The names are:  <b>echo-reply</b> (0) <b>unreachable</b> (3) <b>redirect</b> (5) <b>echo</b> (8) <b>time-exceeded</b> (11) <b>traceroute</b> (30)
<b>icmp-code</b> <i>icmpcode-num</i>	(Optional) Specifies an ICMP message code to match as a number. The range of <i>icmpcode-num</i> is from 0 to 255.
<b>established</b>	(Optional) Indicates an established connection for the TCP protocol. A match occurs if the TCP datagram has the ACK, FIN, PSH, RST, or URG control bits set. The nonmatching case is that of the initial TCP datagram to form a connection.
<b>tos</b> <i>tos-value</i>	(Optional) Specifies the name of a type of service level to match.  The names are:  <b>normal-service</b> (0) <b>monetary-cost</b> (1) <b>reliability</b> (2) <b>throughput</b> (4) <b>delay</b> (8)
<b>log-deny</b>	(Optional) Logs an information level syslog message for each denied packet.

**Command Default** No IP access lists are configured.

**Command Modes** Configuration mode (config)

**Command History**

Release	Modification
1.2(1)	This command was introduced.

**Usage Guidelines** An ACL is applied to each packet, starting at the first ACL rule. Each subsequent rule in the ACL is applied until there is a match. No further rules are applied after this. If there is no match the default rule is applied. Thus, it is important that rules are configured in the right order to achieve the desired results. Generally, 'deny' rules should be configured before 'permit' rules to ensure packets are dropped before matching an unintended 'permit' rule.

IP ACLs use an address and a wildcard mask to specify a range of IP addresses. The mask is applied to the specified address where bits in the mask that are 0 mean the corresponding bits in the specified address are

used as written (they cannot change), including *0s*. Bits that are *1* in the mask mean the corresponding bits in the address may have any value (they can change and are *wild*). This is the inverse behaviour of subnet masks.

Using the **log-deny** option at the end of the individual ACL entries shows the ACL number and whether the packet was permitted or denied, in addition to port-specific information. This option causes an information logging message about the packet that matches the dropped entry (or entries).

If the ACL specified does not exist, it is created when you enter this command. If the ACL already exists, new configuration commands are added to the end of it.

Each interface has a default action that is used when all entries in an IP ACL have been checked and there is no match. For management and non-IPS Gigabit Ethernet interfaces, this is an implicit **deny ip any any** action at the end of the IP ACL which will drop the packet. For IP Storage (IPS) interfaces, this is an implicit **permit ip any any**, which allows any IPS traffic. You must explicitly add a **deny ip any any** rule at the end of IP ACL for IPS interfaces to match the behaviour of other interfaces.

**Table 1: Unsupported Keyword Combinations**

Protocol Keyword	Unsupported Keywords
<b>ip</b>	<b>eq</b> <b>established</b> <b>gt</b> <b>lt</b> <b>range</b> <b>icmp-type</b>
<b>icmp</b>	<b>eq</b> <b>established</b> <b>gt</b> <b>lt</b> <b>range</b>
<b>udp</b>	<b>established</b> <b>icmp-type</b>
<b>tcp</b>	<b>icmp-type</b>

## Examples

The following example configures an IP ACL called `aclPermit` and permits IP traffic from any source address to any destination address:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip access-list aclPermit permit ip any any
```

The following example removes the IP ACL called `aclPermit`:

```
switch# config terminal
```

Enter configuration commands, one per line. End with CNTL/Z.  
 switch(config)# **no ip access-list aclPermit**

The following example appends a rule to the IP ACL called aclPermit to deny TCP traffic from any source address to any destination address:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip access-list aclPermit deny tcp any any
```

The following example appends a rule to the IP ACL called aclPermitUdp that permits source addresses of 192.168.32.0 to 192.168.39.255. Subtracting 255.255.248.0 (subnet mask) from 255.255.255.255 yields 0.0.7.255:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip access-list aclPermitUdp permit udp 192.168.32.0 0.0.7.255 any
```

The following example appends a rule to the IP ACL called aclPermitIpToServer that permits all IP traffic from and to the specified networks:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip access-list aclPermitIpToServer permit ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
```

The following example appends a rule to the IP ACL called aclDenyTcpIpPrt5 that denies TCP traffic from port 5 and any source address in the range 1.2.3.0 to 1.2.3.255 to any destination:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/
switch(config)# ip access-list aclDenyTcpIpPrt5 deny tcp 1.2.3.0 0.0.0.255 eq port 5 any
```

The following example removes this entry from the IP ACL:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/
switch(config)# no ip access-list aclDenyTcpIpPrt5 deny tcp 1.2.3.0 0.0.0.255 eq port 5 any
```

**Related Commands**

Command	Description
<b>ip access-group</b>	Applies an IPv4 ACL to an interface.
<b>ipv6 access-list</b>	Configures an IPv6 access control list.
<b>show ip access-list</b>	Displays the configured IPv4 ACLs information.

## ip address (FCIP profile configuration submode)

To assign the local IP address of a Gigabit Ethernet interface to the FCIP profile, use the **ip address** command. To remove the IP address, use the **no** form of the command.

**ip address** *address*  
**no ip address** *address*

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

**Command Default** Disabled.

**Command Modes** FCIP profile configuration submode.

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

**Usage Guidelines** To create a FCIP profile, you must assign a local IP address of a Gigabit Ethernet interface to the FCIP profile.

**Examples** The following example assigns the local IP address of a Gigabit Ethernet interface to the FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)# ip address 209.165.200.226
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>interface fcip interface_number use-profile profile-id</b>	Configures the interface using an existing profile ID from 1 to 255.
	<b>show fcip profile</b>	Displays information about the FCIP profile.

# ip address (interface configuration)

To assign an IP address to a Gigabit Ethernet interface, use the **ip address** command in interface configuration submode. To remove the IP address, use the **no** form of the command.

**ip address** *address netmask*  
**no ip address** *address netmask*

## Syntax Description

<i>address</i>	Specifies the IP address.
<i>netmask</i>	Specifies the network mask.

## Command Default

None.

## Command Modes

Interface configuration submode.

## Command History

Release	Modification
1.1(2)	This command was introduced.

## Usage Guidelines

None.

## Examples

The following example assigns an IP address to a Gigabit Ethernet interface:

```
switch# config terminal
switch(config)# interface gigabitethernet 1/2
switch(config-profile)# ip address 10.5.1.1 255.255.0.0
```

## Related Commands

Command	Description
<b>interface fcip interface_number use-profile profile-id</b>	Configures the interface using an existing profile ID from 1 to 255.
<b>show fcip profile</b>	Displays information about the FCIP profile.
<b>show interface fcip</b>	Displays an interface configuration for a specified FCIP interface.

# ip default-gateway

To configure the IP address of the default gateway, use the **ip default-gateway** command. To disable the IP address of the default gateway, use the **no** form of the command.

**ip default-gateway** *destination-ip-address* [**interface cpp** *slot\_number/processor-number/vsan-id*]  
**no ip default-gateway** *destination-ip-address* [**interface cpp** *slot\_number/processor-number/vsan-id*]

## Syntax Description

<i>destination-ip-address</i>	Specifies the IP address,
<b>interface</b>	(Optional) Configures an interface.
<b>cpp</b>	(Optional) Specifies a virtualization IPFC interface.
<i>slot</i>	(Optional) Specifies a slot number of the ASM.
<i>processor-number</i>	(Optional) Specifies the processor number for the IPFC interface. The current processor number is always 1.
<i>vsan-id</i>	(Optional) Specifies the ID of the management VSAN. The range 1 to 4093.

## Command Default

None.

## Command Modes

Configuration mode.

## Command History

Release	Modification
1.0(2)	This command was introduced.

## Usage Guidelines

None.

## Examples

The following example configures the IP default gateway to 1.1.1.4:

```
switch# config terminal
switch(config)# ip default-gateway 1.1.1.4
```

## Related Commands

Command	Description
<b>show ip route</b>	Displays the IP address of the default gateway.

# ip default-network

To configure the IP address of the default network, use the **ip default-network** command in configuration mode. To disable the IP address of the default network, use the **no** form of the command.

**ip default-network** *ip-address*  
**no ip default-network** *ip-address*

## Syntax Description

<i>ip-address</i>	Specifies the IP address of the default network.
-------------------	--

## Command Default

None.

## Command Modes

Configuration mode.

## Command History

Release	Modification
1.0(2)	This command was introduced.

## Usage Guidelines

None.

## Examples

The following example configures the IP address of the default network to 1.1.1.4:

```
switch# config terminal
switch(config)# ip default-network 209.165.200.226
switch(config)# ip default-gateway 209.165.200.227
```

## Related Commands

Command	Description
<b>show ip route</b>	Displays the IP address of the default gateway.



# ip (destination-group)

To configure an IPv4 or IPv6 destination address for a destination group, use the **ip** command. To remove the destination address, use the **no** form of this command.

**{ip | ipv6} address address port number [protocol procedural-protocol encoding encoding-protocol]**

Syntax Description	Field	Description
	<b>address</b> <i>address</i>	Destination IPv4 or IPv6 address.
	<b>port</b> <i>number</i>	Destination port number.
	<b>protocol</b> <i>procedural-protocol</i>	Transport protocol. gRPC is the supported transport protocol.
	<b>encoding</b> <i>encoding-protocol</i>	Encoding format. Google Protocol Buffers (GPB) is the supported encoding format.

**Command Default** IP address is not configured for a destination group.

**Command Modes** Telemetry destination group configuration mode (conf-tm-dest)

Command History	Release	Modification
	8.3(1)	This command was introduced.

**Usage Guidelines** When the destination group is linked to a subscription node, telemetry data is sent to the IP address and port specified in the profile.

**Examples** This example shows how to configure an IPv4 and IPv6 address to a destination group with the default transport protocol and default encoding:

```
switch# configure
switch(config)# telemetry
switch(config-telemetry)# destination-group 100
switch(conf-tm-dest)# ip address 1.2.3.4 port 50003 protocol gRPC encoding GPB
switch(conf-tm-dest)# destination-group 100
switch(conf-tm-dest)# ipv6 address 1::1::1:1 port 50009 protocol gRPC encoding GPB
```

This example shows how to remove an IPv4 and IPv6 address from a destination group with the default transport protocol and default encoding:

```
switch# configure
switch(config)# telemetry
switch(config-telemetry)# destination-group 100
switch(conf-tm-dest)# no ip address 1.2.3.4 port 50003 protocol gRPC encoding GPB
switch(conf-tm-dest)# destination-group 100
switch(conf-tm-dest)# no ipv6 address 1::1::1:1 port 50009 protocol gRPC encoding GPB
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>destination-group</b>	Creates a destination group and enters destination group configuration mode.
<b>feature telemetry</b>	Enables the SAN Telemetry Streaming feature.
<b>show running-config telemetry</b>	Displays the existing telemetry configuration.
<b>show telemetry</b>	Displays telemetry configuration.
<b>telemetry</b>	Enters SAN Telemetry Streaming configuration mode.

# ip domain-list

To configure or un-configure one or more domain names, use the **ip domain-list** command in configuration mode. To disable the IP domain list, use the **no** form of the command.

**ip domain-list** *domain-name*  
**no ip domain-list** *domain-name*

## Syntax Description

<i>domain-name</i>	Specifies the domain name for the IP domain list. Maximum length is 80 characters.
--------------------	--

## Command Default

If there is a domain list, the default domain name is not used.

## Command Modes

Configuration mode.

## Command History

Release	Modification
1.0(2)	This command was introduced.

## Usage Guidelines

When “ping dino” is initiated, IP stack will append dino.cisco.com (whatever configured in domain-name) first for Name resolution. If that doesn’t succeed, it will try with domain-list.



**Note** If there is no domain list, the domain name that you specified with the **ip domain-name** global configuration command is used. More than one "**ip domain-list**" command can be entered and they will be tried in order.

## Examples

The following example configures the IP domain list:

```
switch# config terminal
switch(config)# ip domain-list juniper.com
```

## Related Commands

Command	Description
<b>ip domain-lookup</b>	Enables the DNS hostname to address translation.
<b>ip name-server</b>	Configures a list of name servers.
<b>show ip route</b>	Displays the IP address of the default gateway.

# ip domain-lookup

To enable the DNS hostname to address translation, use the **ip domain-lookup** command in configuration mode. Use the **no** form of this command to disable this feature.

**ip domain-lookup**  
**no ip domain-lookup**

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

**Command Default** Enabled.

**Command Modes** Configuration mode.

Release	Modification
1.0(2)	This command was introduced.

**Usage Guidelines** Instead of IP addresses, you can configure the switch using meaningful names. When names are configured the switch automatically looks up the name to get its corresponding IP address.



**Note** In addition to **ip domain-lookup**, other commands need to be entered as well such as "**ip name-server**" and optionally, "**ip domain-name**" and "**ip domain-list**".

## Examples

The following example configures a DNS server lookup feature:

```
switch# config terminal
switch(config)# ip domain-lookup
```

Command	Description
<b>show ip route</b>	Displays the IP address of the default gateway.
<b>ip name-server</b>	Configures a list of name servers.

# ip domain-name

To configure a domain name, use the **ip domain-name** command in configuration mode. To delete a domain name, use the **no** form of the command.

**ip domain-name** *domain-name*  
**no ip domain-name** *domain-name*

## Syntax Description

<i>domain-name</i>	Specifies the domain name.
--------------------	----------------------------

## Command Default

None.

## Command Modes

Configuration mode.

## Command History

Release	Modification
1.0(2)	This command was introduced.

## Usage Guidelines

When “**ping dino**” is initiated, IP stack will append dino.cisco.com (whatever configured in domain-name) first for name resolution. If that doesn’t succeed, it will try with **domain-list**.

## Examples

The following example configures a domain name:

```
switch# config terminal
switch(config)# ip domain-name cisco.com
```

## Related Commands

Command	Description
<b>ip-name server</b>	Configures one or more IP name servers.
<b>ip domain-list</b>	Configure or un-configure one or more domain names.
<b>ip domain-lookup</b>	Enables the DNS hostname to address translation.
<b>show ip route</b>	Displays the IP address of the default gateway.

## ip name-server

To configure one or more IP name servers, use the **ip name-server** command in configuration mode. To disable this feature, use the **no** form of the command.

**ip name-server** *ip-address*  
**no ip name-server** *ip-address*

### Syntax Description

<i>ip-address</i>	Specifies the IP address for the name server.
-------------------	---

### Command Default

The default is no name servers are configured and no IP name resolution is performed.

### Command Modes

Configuration mode.

### Command History

Release	Modification
1.0(2)	This command was introduced.

### Usage Guidelines

You can configure a maximum of six servers. By default, no server is configured.

### Examples

The following example configure a name server with an IP address of 209.165.200.226:

```
switch# config terminal
switch(config)# ip name-server 209.165.200.226
```

The following example specifies the first address (209.165.200.226) as the primary server and the second address (209.165.200.227) as the secondary server:

```
switch(config)# ip name-server 209.165.200.226 209.165.200.227
```

The following example deletes the configured server(s) and reverts to factory default:

```
switch(config)# no ip name-server
```

### Related Commands

Command	Description
<b>ip domain-lookup</b>	Enables the DNS hostname to address translation.
<b>ip domain-list</b>	Configure or un-configure one or more domain names.
<b>ip name-server</b>	Configures one or more IP name servers.
<b>show ip route</b>	Displays the IP address of the default gateway.

# ip route

To configure a static route, use the **ip route** command in configuration mode.

```
ip route ip-address subnet-mask [nexthop_ip-address] [interface {gigabitethernet slot /port |
mgmt 0 | port-channel channel-id | vsan vsan-id} | distance distance-number]
no ip route ip-address subnet-mask [nexthop_ip-address] [interface {gigabitethernet slot /port
| mgmt 0 | port-channel channel-id | vsan vsan-id} | distance distance-number]
```

## Syntax Description

<i>ip-address</i>	Specifies the IP address for the route.
<i>subnet-mask</i>	Specifies the subnet mask for the route.
<i>nexthop_ip-address</i>	(Optional) Specifies the IP address of the next hop switch.
<b>interface</b>	(Optional) Configures the interface associated with the route.
<b>gigabitethernet slot /port</b>	Specifies a Gigabit Ethernet interface at a port and slot.
<b>mgmt 0</b>	Specifies the management interface (mgmt 0).
<b>port-channel channel-id</b>	Specifies a PortChannel interface. The range is 1 to 128.
<b>vsan vsan-id</b>	Specifies a VSAN ID. The range is 1 to 4093.
<b>distance distance-number</b>	(Optional) Specifies the distance metric for this route. It can be from 0 to 32766.

## Command Default

None.

## Command Modes

Configuration mode.

## Command History

Release	Modification
1.0(2)	This command was introduced.

## Usage Guidelines

None.

## Examples

The following example shows how to configure a static route:

```
switch# config terminal
switch(config)# IP route 10.0.0.0 255.0.0.0 20.20.20.10 distance 10 interface vsan 1
```

## Related Commands

Command	Description
<b>show ip route</b>	Displays the IP address routes configured in the system.

# ip routing

To enable the IP forwarding feature, use the **ip routing** command in configuration mode. To disable this feature, use the **no** form of the command.

**ip routing**  
**no ip routing**

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

**Command Default** Disabled.

**Command Modes** Configuration mode.

Release	Modification
1.0(2)	This command was introduced.

**Usage Guidelines** None.

**Examples** The following example enables the IP forwarding feature:

```
switch# config terminal
switch(config)# ip routing
```

Command	Description
<b>show ip routing</b>	Displays the IP routing state.



# ip-compression

To enable compression on the FCIP link, use the **ip-compression** command in interface configuration submode. To disable compression, use the **no** form of the command.

**ip-compression** [**auto** | **mode1** | **mode2** | **mode3**]  
**no ip-compression** [**auto** | **mode1** | **mode2** | **mode3**]

## Syntax Description

<b>auto</b>	(Optional) Enables the automatic compression setting.
<b>mode1</b>	(Optional) Enables fast compression for the following high bandwidth links: PS-4 and IPS-8, less than 100 Mbps MPS-14/2, up to 1 Gbps
<b>mode2</b>	(Optional) Enables moderate compression for medium bandwidth links less than 25 Mbps.
<b>mode3</b>	(Optional) Enables compression for bandwidth links less than 10 Mbps.

## Command Default

Disabled.

## Command Modes

Interface configuration submode.

## Command History

Release	Modification
1.3(1)	This command was introduced.
2.0(x)	Changed the keywords from <b>high-throughput</b> and <b>high-comp-ratio</b> to <b>mode1</b> , <b>mode2</b> , and <b>mode3</b> .

## Usage Guidelines

When no compression mode is entered in the command, the default is **auto**.

The FCIP compression feature introduced in Cisco SAN-OS Release 1.3 allows IP packets to be compressed on the FCIP link if this feature is enabled on that link. By default the FCIP compression is disabled. When enabled, the software defaults to using the auto mode (if a mode is not specified).

With Cisco SAN-OS Release 2.0(1b) and later, you can configure FCIP compression using one of the following modes:

- **mode1** is a fast compression mode for high bandwidth links (> 25 Mbps).
- **mode2** is a moderate compression mode for moderately low bandwidth links (between 10 and 25 Mbps).
- **mode3** is a high compression mode for low bandwidth links (< 10 Mbps).
- **auto** (default) mode determines the appropriate compression scheme based on the bandwidth of the link (the bandwidth of the link configured in the FCIP profile's TCP parameters).

The IP compression feature behavior differs between the IPS module(s) and the MPS-14/2 module. While **mode2** and **mode3** perform software compression in both modules, **mode1** performs hardware-based compression in MPS-14/2 modules, and software compression in IPS-4 and IPS-8 modules.

In Cisco MDS SAN-OS Release 2.1(1a) and later, the **auto** mode option uses a combination of compression modes to effectively utilize the WAN bandwidth. The compression modes change dynamically to maximize the WAN bandwidth utilization.

---

**Examples**

The following example enables faster compression:

```
switch# config terminal  
switch(config) interface fcip 1  
switch(config-if) # ip-compression model
```

The following example enables automatic compression by default:

```
switch(config-if) # ip-compression
```

The following example disables compression:

```
switch(config-if) # no ip-compression
```

---

**Related Commands**

Command	Description
<b>show interface fcip</b>	Displays an interface configuration for a specified FCIP interface.

# ips netsim delay-ms

To delay packets that arrive at a specified Gigabit Ethernet interface specifying milliseconds, use the **ips netsim delay** command in SAN extension tuner configuration submode.

**ips netsim delay-ms** *milliseconds* **ingress** **gigabitethernet** *slot/port*

Syntax Description		
	<i>milliseconds</i>	Specifies the delay in milliseconds. The range is 0 to 150.
	<b>ingress</b>	Specifies the ingress direction.
	<b>gigabitethernet</b> <i>slot/port</i>	Specifies the the slot and port number of the Gigabit Ethernet interface.

**Command Default** Disabled.

**Command Modes** SAN extension tuner configuration submode.

Command History	Release	Modification
	3.1(1)	This command was introduced.

**Usage Guidelines** To use this command, you must enable the IP Network Simulator using the **ips netsim enable** command. This command introduces a delay for all packets entering the Gigabit Ethernet interface. Delay is unidirectional. To introduce delay in the opposite direction, use the slot and port number of the adjacent interface.

**Examples** The following example shows how to configure a delay of 50 milliseconds for packets entering Gigabit Ethernet interface 2/3:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
switch(config)# exit
switch#
switch# ips netsim delay-ms 50 ingress gigabitethernet 2/3
```

Related Commands	Command	Description
	<b>show ips netsim</b>	Displays a summary of the interfaces that are currently operating in network simulation mode.
	<b>ips netsim enable</b>	Enables the IP Network Simulator.

# ips netsim delay-us

To delay packets that arrive at a specified Gigabit Ethernet interface specifying microseconds, use the **ips netsim delay** command in SAN extension tuner configuration submenu.

**ipsnetsimdelay-us***microseconds***ingress****gigabitethernet***slot/port*

Syntax Description		
	<i>microseconds</i>	Specifies the delay in microseconds. The range is 0 to 150000.
	<b>ingress</b>	Specifies the ingress direction.
	<b>gigabitethernet</b> <i>slot/port</i>	Specifies the the slot and port number of the Gigabit Ethernet interface.

**Command Default** Disabled.

## Command Modes

SAN extension tuner configuration submenu.

## Command History

Release	Modification
3.1(1)	This command was introduced.

## Usage Guidelines

To use this command, you must enable the IP Network Simulator using the **ips netsim enable** command.

This command introduces a delay for all packets entering the Gigabit Ethernet interface. Delay is unidirectional. To introduce delay in the opposite direction, use the slot and port number of the adjacent interface.

## Examples

The following example shows how to configure a delay of 50 microseconds for packets entering Gigabit Ethernet interface 2/3:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
switch(config)# exit
switch#
switch# ips netsim delay-us 50 ingress gigabitethernet 2/3
```

## Related Commands

Command	Description
<b>ips netsim enable</b>	Enables the IP Network Simulator.
<b>show ips netsim</b>	Displays a summary of the interfaces that are currently operating in network simulation mode.

# ips netsim drop nth

To drop packets every nth packet at a specified Gigabit Ethernet interface, use the **ips netsim drop nth** command in SAN extension tuner configuration submode.

**ips netsim drop nth** *packet* {**burst** *burst-size* **ingress** **gigabitethernet** *slot/port* | **ingress** **gigabitethernet** *slot/port*}

## Syntax Description

<i>packet</i>	Specifies a specific packet to drop. The range is 0 to 10,000.
<b>burst</b> <i>burst-size</i>	Specifies the packet burst size. The range is 1 to 100.
<b>ingress</b>	Specifies the ingress direction.
<b>gigabitethernet</b> <i>slot/ port</i>	Specifies the the slot and port number of the Gigabit Ethernet interface.

## Command Default

Disabled.

## Command Modes

SAN extension tuner configuration submode.

## Command History

Release	Modification
3.1(1)	This command was introduced.

## Usage Guidelines

To use this command, you must enable the IP Network Simulator using the **ips netsim enable** command.

You can configure the IP Network Simulator to simulate packet drops (even when the queue is not full) randomly (specified as a percentage) or every Nth packet. Percentage is represented as the number of packets in 10,000. For example, if you want to drop one percent of packets, then specify it as 100 packets in 10,000. To simulate a realistic scenario for IP networks using random drops, the drop percentage should be between zero and one percent of packet drops in the specified traffic direction.

If you use the optional burst parameter, then a specified number of packets are dropped. If you do not specify the burst parameter, then only one packet is dropped. The burst limit for either random or Nth drops is 1 to 100 packets. Take the burst parameter into account when specifying the percentage of packets dropped. For example, if you select a random drop of 100 packets in 10,000 (or one percent) with a burst of 2, 200 packets (or two percent) in every 10,000 packets are dropped. Specifying 2 for burst doubles the packet drop.

## Examples

The following example shows how to configure an interface to drop every 100th packet, 2 packets at a time:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
switch(config)# exit
switch#
switch# ips netsim drop nth 100 burst 2 ingress gigabitethernet 2/3
```

---

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ips netsim enable</b>	Enables the IP Network Simulator.
<b>show ips netsim</b>	Displays a summary of the interfaces that are currently operating in network simulation mode.

# ips netsim drop random

To drop packets randomly at a specified Gigabit Ethernet interface, use the **ips netsim drop random** command in SAN extension tuner configuration submode.

**ips netsim drop random** *packet-percentage* {**burst** *burst-size* **ingress** **gigabitethernet** *slot/port* | **ingress** **gigabitethernet** *slot/port*}

## Syntax Description

<i>packet-percentage</i>	Specifies the percentage of packets dropped. The range is 0 to 10000.
<b>burst</b> <i>burst-size</i>	Specifies the packet burst size. The range is 1 to 100.
<b>ingress</b>	Specifies the ingress direction.
<b>gigabitethernet</b> <i>slot /port</i>	Specifies the the slot and port number of the Gigabit Ethernet interface.

## Command Default

Disabled.

## Command Modes

SAN extension tuner configuration submode.

## Command History

Release	Modification
3.1(1)	This command was introduced.

## Usage Guidelines

To use this command, you must enable the IP Network Simulator using the **ips netsim enable** command.

You can configure the IP Network Simulator to simulate packet drops (even when the queue is not full) randomly (specified as a percentage) or every Nth packet. Percentage is represented as the number of packets in 10,000. For example, if you want to drop one percent of packets, then specify it as 100 packets in 10,000. To simulate a realistic scenario for IP networks using random drops, the drop percentage should be between zero and one percent of packet drops in the specified traffic direction.

If you use the optional burst parameter, then a specified number of packets are dropped. If you do not specify the burst parameter, then only one packet is dropped. The burst limit for either random or Nth drops is 1 to 100 packets. Take the burst parameter into account when specifying the percentage of packets dropped. For example, if you select a random drop of 100 packets in 10,000 (or one percent) with a burst of 2, 200 packets (or two percent) in every 10,000 packets are dropped. Specifying 2 for burst doubles the packet drop.

## Examples

The following example shows how to configure an interface to drop one percent of packets:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
switch(config)# exit
switch#
switch# ips netsim drop random 100 burst 1 ingress gigabitethernet 2/3
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show ips netsim</b>	Displays a summary of the interfaces that are currently operating in network simulation mode.
<b>ips netsim enable</b>	Enables the IP Network Simulator.



# ips netsim enable

To enable two Gigabit Ethernet interfaces to operate in the network simulation mode, enter the **ips netsim enable** command in SAN extension tuner configuration submenu. To disable this feature, use the **no** form of the command.

```
ips netsim enable interface gigabitethernet slot/port gigabitethernet slot/port
no ips netsim enable interface gigabitethernet slot/port gigabitethernet slot/port
```

Syntax Description	Parameter	Description
	<b>interface</b>	Specifies that interfaces are enabled.
	<b>gigabitethernet</b> <i>slot/port</i>	Specifies the the slot and port number of the Gigabit Ethernet interface.

**Command Default** Disabled.

**Command Modes** SAN extension tuner configuration submenu.

Command History	Release	Modification
	3.1(1)	This command was introduced.

**Usage Guidelines** This command enables two Gigabit Ethernet interfaces to simulate network characteristics. The first interface specified is the ingress port and the second interface specified is the egress port. Ports must be adjacent and the ingress interface must be an odd-numbered port.

Interfaces configured with this command can no longer be used for FCIP or iSCSI. When the SAN extension tuner configuration submenu is turned off, any interface configured for network simulation reverts back to normal operation.

**Examples** The following example enables the IP Network Simulator and configures interfaces 2/3 and 2/4 for network simulation:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
switch(config)# exit
switch#
switch# ips netsim enable interface gigabitethernet 2/3 gigabitethernet 2/4
```

Related Commands	Command	Description
	<b>show ips netsim</b>	Displays a summary of the interfaces that are currently operating in network simulation mode.

## ips netsim max-bandwidth-kbps

To limit the bandwidth in kilobytes per second of a specified Gigabit Ethernet interface, use the **ips netsim max-bandwidth-kbps** command in SAN extension tuner configuration submode.

**ips netsim max-bandwidth-kbps** *bandwidth* **ingress** **gigabitethernet** *slot/port*

### Syntax Description

<i>bandwidth</i>	Specifies the bandwidth in kilobytes per second. The range is 1000 to 1000000.
<b>ingress</b>	Specifies the ingress direction.
<b>gigabitethernet</b> <i>slot/port</i>	Specifies the the slot and port number of the Gigabit Ethernet interface.

### Command Default

Disabled.

### Command Modes

SAN extension tuner configuration submode.

### Command History

Release	Modification
3.1(1)	This command was introduced.

### Usage Guidelines

To use this command, you must enable the IP Network Simulator using the **ips netsim enable** command.

### Examples

The following example shows how to limit the interface bandwidth to 4500 Kbps:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
switch(config)# exit
switch#
switch# ips netsim max-bandwidth-kbps 4500 ingress gigabitethernet 2/3
```

### Related Commands

Command	Description
<b>ips netsim enable</b>	Enables the IP Network Simulator.
<b>show ips netsim</b>	Displays a summary of the interfaces that are currently operating in network simulation mode.

# ips netsim max-bandwidth-mbps

To limit the bandwidth in megabytes per second of a specified Gigabit Ethernet interface, use the **ips netsim max-bandwidth-mbps** command in SAN extension tuner configuration submode.

**ips netsim max-bandwidth-mbps** *bandwidth* **ingress** **gigabitethernet** *slot/port*

Syntax Description		
	<i>bandwidth</i>	Specifies the bandwidth in megabytes per second. The range is 1 to 1000.
	<b>ingress</b>	Specifies the ingress direction.
	<b>gigabitethernet</b> <i>slot/port</i>	Specifies the the slot and port number of the Gigabit Ethernet interface.

**Command Default** Disabled.

**Command Modes** SAN extension tuner configuration submode.

Command History	Release	Modification
	3.1(1)	This command was introduced.

**Usage Guidelines** To use this command, you must enable the IP Network Simulator using the **ips netsim enable** command.

**Examples** The following example shows how to limit the interface bandwidth to 45 Mbps:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
switch(config)# exit
switch#
switch# ips netsim max-bandwidth-mbps 45 ingress gigabitethernet 2/3
```

Related Commands	Command	Description
	<b>ips netsim enable</b>	Enables the IP Network Simulator.
	<b>show ips netsim</b>	Displays a summary of the interfaces that are currently operating in network simulation mode.

# ips netsim qsize

To limit the size of the queue on a specified Gigabit Ethernet interface, use the **ips netsim qsize** command in SAN extension tuner configuration submenu.

**ips netsim qsize** *queue-size* **ingress** **gigabitethernet** *slot/port*

## Syntax Description

<i>queue-size</i>	Specifies the queue size. The range is 0 to 1000000.
<b>ingress</b>	Specifies the ingress direction.
<b>gigabitethernet</b> <i>slot /port</i>	Specifies the the slot and port number of the Gigabit Ethernet interface.

## Command Default

Disabled.

## Command Modes

SAN extension tuner configuration submenu.

## Command History

Release	Modification
3.1(1)	This command was introduced.

## Usage Guidelines

To use this command, you must enable the IP Network Simulator using the **ips netsim enable** command.

This command rate limits the size of the queue on a specified Gigabit Ethernet port. The recommended queue size for network simulation is 50000 to 150000. If the queue becomes full, packets are dropped.

## Examples

The following example shows how to limit the queue size to 75 KB:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
switch(config)# exit
switch#
switch# ips netsim qsize 75 ingress gigabitethernet 2/3
```

## Related Commands

Command	Description
<b>ips netsim enable</b>	Enables the IP Network Simulator.
<b>show ips netsim</b>	Displays a summary of the interfaces that are currently operating in network simulation mode.

# ips netsim reorder

To reorder packets entering a specified Gigabit Ethernet interface, use the **ips netsim reorder** command in SAN extension tuner configuration submode.

```
ipsnetsimreorder {nth packet distance dist-packet ingress gigabitethernet slot/port | nth packet ingress
gigabitethernet slot/port}
| {random percent distance dist-packet ingress gigabitethernet slot/port}
| random percent ingress gigabitethernet slot/port}
```

## Syntax Description

<b>nth packet</b>	Specifies a specific packet reordered. The range is 0 to 10,000.
<b>distance dist-packet</b>	Specifies the distance between the packet to be reordered and the packet at the head of the queue. The range is 1 to 10.
<b>ingress</b>	Specifies the ingress direction.
<b>gigabitethernet slot/port</b>	Specifies the the slot and port number of the Gigabit Ethernet interface.
<b>random percent</b>	Specifies the percentage of packets passed before a reorder. The range is 0 to 10,000.

## Command Default

Disabled.

## Command Modes

SAN extension tuner configuration submode.

## Command History

Release	Modification
3.1(1)	This command was introduced.

## Usage Guidelines

To use this command, you must enable the IP Network Simulator using the **ips netsim enable** command.

You can configure network simulator to reorder packets (even when the queue is not full) randomly (specified as a percentage) or every Nth packet. Percentage is represented as the number of packets in 10,000. For example, if you want to reorder one percent of packets, then specify it as 100 packets in 10,000. To simulate a realistic scenario for IP networks using random reordering, the percentage should be between zero and one percent of packet reordered in the specified traffic direction.

If you use the optional burst parameter, then the specified number of packets will be reordered. If you do not specify the burst parameter, then only one packet is reordered.

## Examples

The following example shows reordering at 50 percent with a distance limit of 5:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
```

```
switch(config)# exit
switch#
switch# ips netsim reorder random 50 distance 5 ingress gigabitethernet 2/3
```

The following example shows reordering of every 50th packet with a distance limit of 5:

```
switch# config terminal
switch(config)#
switch(config)# san-ext-tuner enable
switch(config)# exit
switch#
switch# ips netsim reorder nth 50 distance 5 ingress gigabitethernet 2/3
```

#### Related Commands

Command	Description
<b>ips netsim enable</b>	Enables the IP Network Simulator.
<b>show ips netsim</b>	Displays a summary of the interfaces that are currently operating in network simulation mode.

## ipv6 access-list

To configure an IPv6 access control list (ACL) and enter IPv6-ACL configuration submode, use the **ipv6 access-list** command in configuration mode. To discard an IPv6 ACL, use the **no** form of the command.

**ipv6 access-list** *list-name*  
**no ipv6 access-list** *list-name*

<b>Syntax Description</b>	<i>list-name</i> Specifies an IP access control list name. The maximum size is 64.
---------------------------	--

**Command Default** None.

**Command Modes** Configuration mode.

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

**Usage Guidelines** Before using the **ipv6 access-list** command to configure an IPv6 ACL on a switch, become familiar with the features of IPv6 and its extended addressing capabilities. In particular, it is important to understand the different types of IPv6 address formats, the IPv6 address prefix format, and the different IPv6 address types. For detailed information about IPv6.

### Examples

The following example configures an IPv6 access list called List1 and enters IPv6-ACL configuration submode:

```
switch # config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ipv6 access-list List1
switch(config-ipv6-acl)#
```

The following example removes the IPv6 access list called List1 and all of its entries:

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

<b>Related Commands</b>		
<b>ipv6 route</b>		Configures an IPv6 static route.
<b>ipv6 routing</b>		Enables IPv6 unicast routing.
<b>show ipv6 access-list</b>		Displays a summary of ACLs.
<b>show ipv6 route</b>		Displays the IPv6 static routes configured on the switch.
<b>show ipv6 routing</b>		Displays the IPv6 unicast routing configured on the switch.

# ipv6 address

To enable IPv6 processing and configure an IPv6 address on the interface, use the **ipv6 address** command in interface configuration submenu. To remove an IPv6 address, use the **no** form of the command.

**ipv6 address** *ipv6-address-prefix*  
**no ipv6 address** *ipv6-address-prefix*

## Syntax Description

<i>ipv6-address-prefix</i>	Specifies the IPv6 address prefix. The format is X:X:X::X/n .
----------------------------	---

## Command Default

None.

## Command Modes

Interface configuration submenu.

## Command History

Release	Modification
3.0(1)	This command was introduced.

## Usage Guidelines

You can use the **ipv6 address** command to enable IPv6 processing and configure the IPv6 address on the interface. An IPv6 address must be configured on an interface for the interface to forward IPv6 traffic.

Assigning a unicast address generates a link local address and implicitly enables IPv6.



**Note** The *ipv6-address-prefix* argument in the **ipv6 address** command must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons. A slash mark (/) precedes a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).

## Examples

The following example assigns a unicast IPv6 address to the interface and enables IPv6 processing on the interface:

```
switch#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#interface gigabitethernet 2/2
switch(config-if)#ipv6 address 2001:0DB8:800:200C::417A/64
```

## Related Commands

<b>ipv6 enable</b>	Enables IPv6 processing on the interface.
<b>ipv6 nd</b>	Configures IPv6 neighbor discovery commands on the interface.
<b>ipv6 traffic-filter</b>	Configures IPv6 ACLs to filter traffic for packets on the interface.
<b>show interface</b>	Displays interface configuration information.



# ipv6 enable

To enable IPv6 processing and configure an IPv6 link-local address on the interface, use the **ipv6 enable** command in interface configuration submenu. To disable IPv6 processing and remove the link-local address, use the **no** form of the command.

**ipv6 enable**  
**no ipv6 enable**

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

**Command Default** None.

**Command Modes** Interface configuration submenu.

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

**Usage Guidelines** When you enable IPv6 on an interface, a link local address is automatically assigned. This address is used for communication on the switch:

## Examples

The following example enables IPv6 processing on the interface:

```
switch#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#interface gigabitethernet 2/2
switch(config-if)#ipv6 enable
```

The following example disables IPv6 processing on the interface:

```
switch(config-if)# no ipv6 enable
```

Related Commands	Command	Description
	<b>ipv6 address</b>	Configures the IPv6 address and enables IPv6 processing.
	<b>ipv6 nd</b>	Configures IPv6 neighbor discovery commands on the interface.
	<b>ipv6 traffic-filter</b>	Configures IPv6 ACLs to filter traffic for packets on the interface.
	<b>show interface</b>	Displays interface configuration information.

# ipv6 nd

To configure IPv6 neighbor discovery commands on the interface, use the **ipv6 nd** command in interface configuration submode. To remove IPv6 neighbor discovery configuration commands, use the **no** form of the command.

**ipv6 nd** {**dad attempts** *number* | **reachable-time** *time* | **retransmission-time** *time*}  
**no ipv6 nd** {**dad attempts** *number* | **reachable-time** *time* | **retransmission-time** *time*}

## Syntax Description

<b>dad attempts</b> <i>number</i>	Configures duplicate address detection (DAD) attempts. The range is 0 to 15.
<b>reachable-time</b> <i>time</i>	Configures reachability time. Specifies the reachability time in milliseconds. The range is 1000 to 3600000.
<b>retransmission-time</b> <i>time</i>	Configures the retransmission timer. Specifies the retransmission time in milliseconds. The range is 1000 to 3600000.

## Command Default

DAD attempts: 0.  
 Reachable-time: 30000 milliseconds.  
 Retransmission-time: 1000 milliseconds.

## Command Modes

Interface configuration submode.

## Command History

Release	Modification
3.0(1)	This command was introduced.

## Usage Guidelines

A router must be able to determine the link-local address for each of its neighboring routers in order to ensure that the target address (the final destination) in a redirect message identifies the neighbor router by its link-local address. For static routing, the address of the next-hop router should be specified using the link-local address of the router; for dynamic routing, all IPv6 routing protocols must exchange the link-local addresses of neighboring routers.



**Note** A high number of DAD attempts (greater than 2) can delay address assignment.

For complete information about IPv6 neighbor discovery.

## Examples

The following example sets the duplicate address detection attempts count to 2:

```
switch# config terminal
switch(config)# interface gigabitethernet 2/2
switch(config-if)# ipv6 nd dad attempts 2
```

The following example sets the reachability time to 10000 milliseconds:

```
switch(config-if)# ipv6 nd reachability-time 10000
```

The following example sets the retransmission time to 20000 milliseconds:

```
switch(config-if)# ipv6 nd retransmission-time 20000
```

**Related Commands**

<b>ipv6 address</b>	Configures the IPv6 address and enables IPv6 processing.
<b>ipv6 enable</b>	Enables IPv6 processing on the interface.
<b>ipv6 traffic-filter</b>	Configures IPv6 ACLs to filter traffic for packets on the interface.
<b>show interface</b>	Displays interface configuration information.

## ipv6 route

To configure an IPv6 static route, use the **ipv6 route** command in configuration mode. To remove or disable an IPv6 static route, use the **no** form of the command.

**ipv6 route** *destination-address-prefix next-hop-address* [**distance** *distance-metric* | **interface** {**gigabitethernet** *slot/port* | **mgmt** *number* | **port-channel** *number* | **vsan** *vsan-id*}] [**distance** *distance-metric*]

**no ipv6 route** *destination-address-prefix next-hop-address* [**distance** *distance-metric* | **interface** {**gigabitethernet** *slot/port* | **mgmt** *number* | **port-channel** *number* | **vsan** *vsan-id*}] [**distance** *distance-metric*]

### Syntax Description

<i>destination-address-prefix</i>	Specifies the IPv6 destination address prefix. The format is <i>X:X:X::X/n</i> .
<i>next-hop-address</i>	Specifies the next hop IPv6 address. The format is <i>X:X:X::X</i> .
<b>distance</b>	(Optional) Configures an IPv6 route metric.
<i>distance-metric</i>	Specifies a distance metric for the specified route. The range is 0 to 32766.
<b>interface</b>	(Optional) Configures a next hop IPv6 address.
<b>gigabitethernet</b> <i>slot/port</i>	(Optional) Specifies a Gigabit Ethernet slot and port number.
<b>mgmt</b> <i>number</i>	(Optional) Specifies the management interface.
<b>port-channel</b> <i>number</i>	(Optional) Specifies a PortChannel number. The range is 1 to 128
<b>vsan</b> <i>vsan-id</i>	(Optional) Specifies an IPFC VSAN ID. The range is 1 to 4093.

### Command Default

None.

### Command Modes

Configuration mode.

### Command History

Release	Modification
3.0(1)	This command was introduced.

### Usage Guidelines

Before using the **ipv6 route** command to configure IPv6 features on a switch, become familiar with the features of IPv6 and its extended addressing capabilities. In particular, it is important to understand the different types of IPv6 address formats, the IPv6 address prefix format, and the different IPv6 address types.

## Examples

The following example configures a static default IPv6 route on a Gigabit Ethernet interface:

```
switch # config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ipv6 route ::/0 gigabitethernet 3/1
```

The following example configures a fully specified static route on a Gigabit Ethernet interface:

```
switch(config)# ipv6 route 2001:0DB8::/32 gigabitethernet 3/2
```

The following example configures a recursive static route to a specified next hop address:

```
switch(config)# ipv6 route 2001:0DB8::/32 2001:0DB8:2002::1
```

The following example configures a recursive static route to a specified next hop address, from which the output interface is automatically derived, and to a specified interface:

```
switch(config)# ipv6 route 2001:0DB8::/32 2001:0DB8:2002::1 gigabitethernet 3/2
```

The following example configures a static IPv6 route with an administrative distance of 20.

```
switch(config)# ipv6 route 2001:0DB8::/32 interface gigabitethernet 2/0 distance 20
```

## Related Commands

<b>ipv6 access-list</b>	Configures an IPv6 access control list (ACL) and enters IPv6-ACL configuration submode.
<b>ipv6 routing</b>	Enables IPv6 unicast routing.
<b>show ipv6 access-list</b>	Displays a summary of ACLs.
<b>show ipv6 route</b>	Displays the static IPv6 routes configured on the switch.
<b>show ipv6 routing</b>	Displays the IPv6 unicast routing configured on the switch.

# ipv6 routing

To enable IPv6 unicast routing, use the **ipv6 routing** command in configuration mode. To disable IPv6 unicast routing, use the **no** form of the command.

**ipv6 routing**  
**no ipv6 routing**

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

**Command Default** None.

**Command Modes** Configuration mode.

Release	Modification
3.0(1)	This command was introduced.

**Usage Guidelines** Before using the **ipv6 routing** command to configure IPv6 features on a switch, become familiar with the features of IPv6 and its extended addressing capabilities. In particular, it is important to understand the different types of IPv6 address formats, the IPv6 address prefix format, and the different IPv6 address types.

**Examples** The following example enables IPv6 routing:

```
switch # config terminal
switch(config)# ipv6 routing
```

The following example disables IPv6 routing:

```
switch(config)# no ipv6 routing
```

Related Commands	
<b>ipv6 access-list</b>	Configures an IPv6 access control list (ACL) and enters IPv6-ACL configuration submode.
<b>ipv6 route</b>	Configures a static IPv6 route.
<b>show ipv6 access-list</b>	Displays a summary of ACLs.
<b>show ipv6 route</b>	Displays the static IPv6 routes configured on the switch.
<b>show ipv6 routing</b>	Displays the IPv6 unicast routing configured on the switch.

## ipv6 traffic-filter

To configure IPv6 access control lists (ACLs) to filter traffic for packets on the interface, use the **ipv6 traffic-filter** command in interface configuration submenu. To remove an IPv6-ACL traffic filter on the switch, use the **no** form of the command.

```
ipv6 traffic-filter access-list-name {in | out}
no ipv6 traffic-filter access-list-name {in | out}
```

Syntax Description	
<i>access-list-name</i>	Specifies the name of an access control list for packets. The maximum size is 64 characters.
<b>in</b>	Configures inbound packets.
<b>out</b>	Configures outbound packets.

**Command Default** None.

**Command Modes** Interface configuration submenu.

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

**Usage Guidelines** None.

**Examples** The following example configures a traffic filter, called testfilter, for inbound packets:

```
switch# config terminal
switch(config)# interface gigabitethernet 2/2
switch(config-if)# ipv6 traffic-filter testfilter in
```

Related Commands	
<b>ipv6 address</b>	Configures the IPv6 address and enables IPv6 processing.
<b>ipv6 enable</b>	Enables IPv6 processing on the interface.
<b>ipv6 nd</b>	Configures IPv6 ACLs to filter traffic for packets on the interface.
<b>show interface</b>	Displays interface configuration information.

# iscsi authentication

To configure the default authentication method for iSCSI, use the **iscsi authentication** command. To revert to the default, use the **no** form of the command.

```
iscsi authentication {chap | chap-none | none | username username password [0 | 7] password}
no iscsi authentication {chap | chap-none | none | username}
```

## Syntax Description

<b>chap-none</b>	Configures either the CHAP or no authentication.
<b>chap</b>	Configures the Challenge Handshake Authentication Protocol (CHAP) authentication method.
<b>none</b>	Specifies that no authentication is required for the selected interface
<b>username</b> <i>username</i>	Assigns CHAP username to be used when switch is authenticated. Specifies the name of the user. Maximum length is 128 characters.
<b>password</b>	Configures the password for the username.
<b>0</b>	(Optional) Specifies that the password is a cleartext CHAP password.
<b>7</b>	(Optional) Specifies that the password is an encrypted CHAP password. The password is limited to 128 characters.
<i>password</i>	Specifies a password for the username. The password length is limited to 128 characters.

## Command Default

chap-none.

The default password is a cleartext password.

## Command Modes

Configuration mode.

## Command History

Release	Modification
1.1(1)	This command was introduced.
2.0(x)	Added the <b>username</b> option.

## Usage Guidelines

By default, the Cisco MDS 9000 Family switch accepts an iSCSI initiator with either no authentication or CHAP authentication. If CHAP authentication is always required, use the **iscsi authentication chap** command. If no authentication is always required, use the **iscsi authentication none** command.

Use the **chap-none** option to override the global configuration which might have been configured to allow only one option either CHAP or none but not both.





---

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

---

### Examples

The following example configures CHAP only for iSCSI authentication:

```
switch# config terminal  
switch(config)# iscsi authentication chap
```

### Related Commands

Command	Description
<b>show iscsi global</b>	Displays all iSCSI initiators configured by the user.

# iscsi duplicate-wwn-check

To check the current running configuration for conflicts between iSCSI initiators' static WWN allocation and what the system thinks is available in its WWN pool, use the **iscsi duplicate-wwn-check** command in configuration mode.

## iscsi duplicate-wwn-check

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

**Command Default** None.

**Command Modes** Configuration mode.

Release	Modification
2.1(2)	This command was introduced.

**Usage Guidelines** Prior to Cisco MDS SAN-OS Release 2.1(2), WWNs assigned to static iSCSI initiators by the system can be inadvertently returned to the system when an upgrade fails or the system software is manually downgraded (that is, when you manually boot up an older Cisco MDS SAN-OS release without using the **install all** command). In these instances, the system can later assign those WWNs to other iSCSI initiators (dynamic or static) and cause conflicts.

As of Cisco MDS SAN-OS Release 2.1(2), you can use the **iscsi duplicate-wwn-check** command to check for and remove any configured WWNs that belong to the system.



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

## Examples

The following example shows how to check the current running configuration for conflicts between iSCSI initiators' static WWN allocation and what the system thinks is available in its WWN pool:

```
switch# config terminal
Enter configuration command, one per line. End with CNTL/Z.
switch(config)# iscsi duplicate-wwn-check
```

List of Potential WWN Conflicts:

```
-----
Node : iqn.test-local-nwn:1-local-pwn:1
nWWN : 22:03:00:0d:ec:02:cb:02
pWWN : 22:04:00:0d:ec:02:cb:02
```

The following example shows how to remove the conflicting nWWN and pWWN:

```
switch(config)# iscsi initiator name iqn.test-local-nwn:1-local-pwn:1
switch(config-iscsi-init)# no static nWWN 22:03:00:0d:ec:02:cb:02
switch(config-iscsi-init)# no static pWWN 22:04:00:0d:ec:02:cb:02
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>iscsi initiator name</b>	Assigns an iSCSI name and changes to iSCSI initiator configuration submode.
<b>static</b>	Assigns persistent WWNs to an iSCSI initiator in iSCSI initiator configuration submode.
<b>show iscsi initiator</b>	Displays information about configured iSCSI initiators.

# iscsi dynamic initiator

To configure dynamic initiator modes, use the **iscsi dynamic initiator** command in configuration mode. To revert to the default mode, use the **no** form of the command.

**iscsi dynamic initiator** {deny | islb}

**no dynamic initiator** {deny | islb}

## Syntax Description

<b>deny</b>	Specifies that dynamic initiators are denied from logging on to the MDS switch.
<b>islb</b>	Specifies iSLB dynamic initiator mode.

## Command Default

iSCSI.

## Command Modes

Configuration mode.

## Command History

Release	Modification
3.0(1)	This command was introduced.

## Usage Guidelines

Three dynamic initiator modes are supported:

- iSCSI—Dynamic initiators are treated as iSCSI initiators and can access dynamic virtual targets and configured iSCSI virtual targets.
- iSLB—Dynamic initiators are treated as iSLB initiators and can access dynamic virtual targets.
- Deny—Dynamic initiators are not allowed to log in to the MDS switch.

iSCSI dynamic initiator is the default mode of operation. This configuration is distributed using CFS.



**Note** Configuring dynamic initiator modes is supported only through the CLI, not through Device Manager or Fabric Manager.

A dynamic iSCSI initiator can be converted to a static iSCSI initiator and its WWNs can be made persistent.

A dynamic iSLB initiator can be converted to a static iSLB initiator and its WWNs can be made persistent.



**Note** You cannot convert a dynamic iSCSI initiator to a static iSLB initiator, or a dynamic iSLB initiator to a static iSCSI initiator.



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

---

**Examples**

The following command configures the dynamic initiator mode as iSLB:

```
switch(config)# iscsi dynamic initiator islb
```

The following command configures the dynamic initiator mode as deny:

```
switch(config)# iscsi dynamic initiator deny
```

The following command reverts to the default dynamic initiator mode of iSCSI:

```
switch(config)# no iscsi dynamic initiator deny
```

---

**Related Commands**

Command	Description
<b>iscsi save-initiator</b>	Permanently saves the automatically assigned nWWN or pWWN mapping.
<b>show iscsi global</b>	Displays global iSCSI configured information.

# iscsi enable

To enable the iSCSI feature in any Cisco MDS switch, use the **iscsi enable** command. To disable this feature, use the **no** form of the command.

**iscsi enable**  
**no iscsi enable**

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

**Command Default** Disabled.

**Command Modes** Configuration mode.

Release	Modification
1.3(1)	This command was introduced.
3.2(2c)	Updated the example command.
NX-OS 4.1(1)	This command was deprecated.

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



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

## Examples

The following command enables the iSCSI feature:

```
switch(config)# iscsi enable
switch(config)# iscsi enable module 8
switch(config)# int iscsi 2/1
switch(config-if)#
switch(config)# no shutdown
```

The following command disables the iSCSI feature (default):

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

## iscsi enable module

To enable iSCSI features for each IPS linecard to create corresponding iSCSI interfaces, use the **iscsi enable module** command.

**iscsi enable module** *module-num*

### Syntax Description

<i>module-num</i>	Specifies the desired IPS linecard module number on which iSCSI interfaces need to be enabled.
-------------------	--

### Command Default

iSCSI interfaces are disabled on IPS linecards by default.

### Command Modes

Configuration mode.

### Command History

Release	Modification
3.2(1)	This command was introduced.

### Usage Guidelines

None.

### Examples

The following example shows how to enable the iSCSI interface on a desired module number on the switch:

```
switch# config terminal
switch(config)# iscsi enable module 1
```



**Note** The iSCSI feature must be enabled before executing this command.

### Related Commands

Command	Description
<b>iscsi enable</b>	Enables the iSCSI features but does not create the interfaces.

# iscsi import target fc

To allow dynamic mapping of Fibre Channel targets, use the **iscsi import target fc** command. To disable this feature, use the **no** form of the command.

**iscsi import target fc**  
**no iscsi import target fc**

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

**Command Default** Disabled.

**Command Modes** Configuration mode.

Release	Modification
1.1(1)	This command was introduced.

**Usage Guidelines** This command directs iSCSI to dynamically import all Fibre Channel targets into iSCSI.



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

## Examples

The following example allows dynamic mapping of Fibre Channel targets:

```
switch# config terminal
switch(config)# iscsi import target fc
```

The following example disables dynamic mapping of Fibre Channel targets:

```
switch(config)# no iscsi import target fc
```

Command	Description
<b>show iscsi global</b>	Displays all iSCSI initiators configured by the user.



# iscsi initiator idle-timeout

To configure the iSCSI initiator idle timeout, use the **iscsi initiator idle-timeout** command. To revert to the default, use the **no** form of the command.

**iscsi initiator idle-timeout** *seconds*  
**no iscsi initiator idle-timeout** *seconds*

## Syntax Description

<i>seconds</i>	Specifies the timeout in seconds. The range is 0 to 3600.
----------------	---

## Command Default

300 seconds.

## Command Modes

Configuration mode.

## Command History

Release	Modification
1.3	This command was introduced.

## Usage Guidelines

When the idle timeout value is set to 0, the initiator information is cleared immediately after the last session from the initiator terminates.



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

## Examples

The following example configures the iSCSI initiator idle timeout to 180 seconds:

```
switch# config terminal
switch(config)# iscsi initiator idle-timeout 180
```

The following example reverts the default value of 300 seconds:

```
switch# config terminal
switch(config)# no iscsi initiator idle-timeout 240
```

## Related Commands

Command	Description
<b>show iscsi global</b>	Displays global iSCSI configuration information.

## iscsi initiator ip-address

To assign persistent WWNs to an iSCSI initiator or assign an iSCSI initiator into VSANs other than the default VSAN, use the **iscsi initiator ip-address** command. To revert to the default, use the **no** form of the command.

**iscsi initiator ip-address** *ipaddress* **static** {**nwwn** | **pwwn**} {*wwn-id* | **system-assign** *number*} **vsan** *vsan-id*

**no iscsi initiator ip-address** *ipaddress* **static** {**nwwn** | **pwwn**} {*wwn-id* | **system-assign** *number*} **vsan** *vsan-id*

### Syntax Description

<i>ipaddress</i>	Specifies the initiator IP address.
<b>nwwn</b>	Configures the initiator node WWN hex value.
<b>pwwn</b>	Configures the peer WWN for special frames.
<i>wwn-id</i>	Enters the pWWN or nWWN ID.
<b>system-assign</b> <i>number</i>	Generates the nWWN value automatically. The number ranges from 1 to 64.
<b>vsan</b> <i>vsan-id</i>	Specifies a VSAN ID. The range is 1 to 4093.

### Command Default

Disabled.

### Command Modes

Configuration mode.

### Command History

Release	Modification
1.1(1)	This command was introduced.

### Usage Guidelines

Under a circumstance where an iSCSI initiator needs to have a persistent binding to FC WWNs, this command should be used. Also, an iSCSI initiator can be put into multiple VSANs. An iSCSI host can become a member of one or more VSANs.



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

### Examples

The following command configures an iSCSI initiator. using the IP address of the initiator node:

```
switch(config)# iscsi initiator ip address 209.165.200.226
```

The following command deletes the configured iSCSI initiator.

```
switch(config)# no iscsi initiator ip address 209.165.200.226
```

The following command uses the switch's WWN pool to allocate the nWWN for this iSCSI initiator and keeps it persistent:

```
switch(config-(iscsi-init))# static nWWN system-assign
```

The following command assigns the user provided WWN as nWWN for the iSCSI initiator. You can only specify one nWWN for each iSCSI node:

```
switch(config-(iscsi-init))# nWWN 20:00:00:05:30:00:59:11
```

The following command uses the switch's WWN pool to allocate two pWWNs for this iSCSI initiator and keeps it persistent:

```
switch(config-(iscsi-init))# static pWWN system-assign 2
```

The following command assigns the user provided WWN as pWWN for the iSCSI initiator:

```
switch(config-(iscsi-init))# pWWN 21:00:00:20:37:73:3b:20
```

#### Related Commands

Command	Description
<b>show iscsi initiator</b>	Displays information about configured iSCSI initiators.

## iscsi initiator name

To configure an iSCSI initiator name and change to iSCSI configuration mode, use the **iscsi initiator name** command. To revert to factory defaults, use the **no** form of the command.

**iscsi initiator name** *name*

**no iscsi initiator name** *name*

### Syntax Description

<i>name</i>	Enters the initiator name to be used. The minimum length is 16 characters and maximum is 223 characters.
-------------	--

### Command Default

Disabled.

### Command Modes

Configuration mode.

### Command History

Release	Modification
1.3(2)	This command was introduced.

### Usage Guidelines

Under a circumstance where an iSCSI initiator needs to have a persistent binding to FC WWNs, this command should be used. Also, an iSCSI initiator can be put into multiple VSANs. An iSCSI host can become a member of one or more VSANs.



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

### Examples

The following example configures an iSCSI initiator using the iSCSI name of the initiator node:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# iscsi initiator name iqn.1987-02.com.cisco.initiator
```

### Related Commands

Command	Description
<b>show iscsi initiator</b>	Displays information about configured iSCSI initiators.

# iscsi interface vsan-membership

To configure VSAN membership for iSCSI interfaces, use the **iscsi interface vsan-membership** command. Use the **no** form of this command to disable this feature or to revert to factory defaults.

**iscsi interface vsan-membership**  
**no iscsi interface vsan-membership**

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

**Command Default** Disabled.

**Command Modes** Configuration mode.

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

**Usage Guidelines** If the **iscsi interface vsan-membership** command is disabled, you will not be able to configure iSCSI VSAN membership.



**Caution** Changing the VSAN membership, the forwarding mode, and the authentication of an iSCSI interface that is part of an iSLB VRRP group impacts load balancing on the interface.



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

## Examples

The following command enables the iSCSI interface VSAN membership:

```
switch# config terminal
switch(config)# iscsi interface vsan-membership
```

The following command disables the iSCSI interface VSAN membership (default):

```
switch(config)# no iscsi interface vsan-membership
```

Related Commands	Command	Description
	<b>show iscsi initiator</b>	Displays information about configured iSCSI initiators.

# iscsi save-initiator

To permanently save the automatically assigned nWWN and pWWN mapping, use the **iscsi save-initiator** command.

**iscsi save-initiator** [**ip-address** *ip-address* | **name** *name*]

## Syntax Description

<b>ip-address</b> <i>ip-address</i>	(Optional) Specifies the initiator IP address.
<b>name</b> <i>name</i>	(Optional) Specifies the initiator name to be used from 1 to 255 characters. The minimum length is 16 characters.

## Command Default

If initiator name or IP address is not specified, the nWWN and pWWN mapping for all initiators becomes permanent.

## Command Modes

Configuration mode.

## Command History

Release	Modification
1.3(1)	This command was introduced.

## Usage Guidelines

After executing the **iscsi save-initiator** command, issue the **copy running-config startup-config** to save the nWWN and pWWN mapping across switch reboots.

After a dynamic iSCSI initiator has logged in, you may decide to permanently save the automatically assigned nWWN and pWWN mapping so this initiator uses the same mapping the next time it logs in.

You can convert a dynamic iSCSI initiator to static iSCSI initiator and make its WWNs persistent.



**Note** You cannot convert a dynamic iSCSI initiator to a static iSLB initiator or a dynamic iSLB initiator to a static iSCSI initiator.



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

## Examples

The following example shows how to save the nWWN and pWWN mapping for all the initiators:

```
switch(config)# iscsi save-initiator
```

The following example shows how to save the nWWN and pWWN mapping for an initiator named iqn.1987-02.com.cisco.initiator:

```
switch(config)# iscsi save-initiator name iqn.1987-02.com.cisco.initiator
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>iscsi initiator</b>	Configures an iSCSI initiator.
<b>show iscsi initiator</b>	Displays information about configured iSCSI initiators.

## iscsi virtual-target name

To create a static iSCSI virtual target, use the **iscsi virtual-target** command. To revert to the default values, use the **no** form of the command.

```
iscsi virtual-target name name advertise interface {gigabitethernet slot/port [.subinterface] |
port-channel channel-id [.subinterface]} all-initiator-permit initiator {initiator-name | ip-address
ipaddress [netmask]} permit pwwn pwwn-id [fc-lun number iscsi-lun number [secondary-pwwn
pwwn-id [sec-lun number]] | secondary-pwwn pwwn-id] revert-primary-port trespass
no iscsi virtual-target name name advertise interface {gigabitethernet slot/port [.subinterface]
| port-channel channel-id [.subinterface]} all-initiator-permit initiator {initiator-name | ip-address
ipaddress [netmask]} permit pwwn pwwn-id [fc-lun number iscsi-lun number [secondary-pwwn
pwwn-id [sec-lun number]] | secondary-pwwn pwwn-id] revert-primary-port trespass
```

### Syntax Description

<i>name</i>	Enters the virtual target name to be used. The minimum length is 16 characters and maximum of 223 bytes.
<b>advertise interface</b>	Advertises the virtual target name on the specified interface.
<b>gigabitethernet</b> <i>slot/port subinterface</i>	Selects the Gigabit Ethernet interface or subinterface to configure.
<b>port-channel</b> <i>channel-id subinterface</i>	Selects the Port Channel interface or subinterface to configure.
<b>all-initiator-permit</b>	Enables all iSCSI initiator access to this target.
<b>initiator</b>	Configures specific iSCSI initiator access to this target.
<i>initiator-name</i>	Specifies the iSCSI initiator name to be used access a specified target. Maximum length is 255 characters.
<b>ip-address</b> <i>ip-address</i>	Specifies the iSCSI initiator IP address.
<b>permit</b>	Permits access to the specified target.
<b>pwwn</b> <i>pwwn-id</i>	Specifies the peer WWN ID for special frames.
<b>secondary-pwwn</b> <i>pwwn-id</i>	(Optional) Specifies the secondary pWWN ID.
<b>fc-lun</b> <i>number</i>	(Optional) Specifies the Fibre Channel Logical Unit Number (LUN).
<b>iscsi-lun</b> <i>number</i>	(Optional) Specifies the iSCSI virtual target number.
<b>sec-lun</b> <i>number</i>	(Optional) Specifies the secondary Fibre Channel LUN.
<b>revert-primary-port trespass</b>	Moves LUNs forcefully from one port to another.

### Command Default

Disabled.

### Command Modes

Configuration mode.



**Command History**

Release	Modification
1.1(1)	This command was introduced.
1.3(1)	Added <b>revert-to-primary</b> and <b>trespass</b> subcommands.

**Usage Guidelines**

This command is used to configure a static iSCSI target for access by iSCSI initiators. A virtual target may contain a subset of LUs of an FC target or one whole FC target.

Do not specify the LUN if you want to map the whole Fibre Channel target to an iSCSI target. All Fibre Channel LUN targets are exposed to iSCSI.



**Note** The CLI interprets the LUN identifier value as a hexadecimal value whether or not the 0x prefix is included.

One iSCSI target cannot contain more than one Fibre Channel target.



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

**Examples**

The following example creates a static virtual target and enters ISCSI target configuration submode:

```
switch# config terminal
switch(config)# iscsi virtual-target name 0123456789ABDEFGHI
switch(config-iscsi-tgt)#
```

The following command advertises the virtual target only on the specified interface. By default, it is advertised on all interfaces in all IPS modules.

```
switch(config-iscsi-tgt)# advertise interface gigabitethernet 4/1
```

The following command maps a virtual target node to a Fibre Channel target:

```
switch(config-iscsi-tgt)# pwwn 26:00:01:02:03:04:05:06
```

The following command enters the secondary pWWN for the virtual target node:

```
switch(config-iscsi-tgt)# pwwn 26:00:01:02:03:04:05:06 secondary-pwwn 66:00:01:02:03:04:05:02
```

Use the LUN option to map different Fibre Channel LUNs to different iSCSI virtual targets. If you have already mapped the whole Fibre Channel target, you will not be able to use this option.

```
switch(config-iscsi-tgt)# pwwn 26:00:01:02:03:04:05:06 fc-lun 0 iscsi-lun 0
```

The following command allows the specified iSCSI initiator node to access this virtual target. You can issue this command multiple times to allow multiple initiators.

```
switch(config-iscsi-tgt)# initiator iqn.1987-02.com.cisco.initiator1 permit
```

The following command prevents the specified initiator node from accessing virtual targets:

```
switch(config-iscsi-tgt)# no initiator iqn.1987-02.com.cisco.initiator1 permit
```

The following command allows the specified IP address to access this virtual target:

```
switch(config-iscsi-tgt)# initiator ip-address 209.165.200.226 permit
```

The following command prevents the specified IP address from accessing virtual targets:

```
switch(config-iscsi-tgt)# no initiator ip-address 209.165.200.226 permit
```

The following command allows all initiators in this subnetwork to access this virtual target:

```
switch(config-iscsi-tgt)# initiator ip-address 10.50.0.0 255.255.255.0 permit
```

The following command prevents all initiators in this subnetwork from accessing virtual targets:

```
switch(config-iscsi-tgt)# no initiator ip-address 10.50.0.0 255.255.255.0 permit
```

The following command allows all initiator nodes to access this virtual target:

```
switch(config-iscsi-tgt)# all-initiator-permit
```

The following command prevents any initiator node from accessing virtual targets:

```
switch(config-iscsi-tgt)# no all-initiator-permit
```

The following command configures a primary and secondary port and moves the LUNs from one port to the other using the **trespass** command:

```
switch# config terminal
switch(config)# iscsi virtual-target name iqn.1987-02.com.cisco.initiator
switch(config-iscsi-tgt)# pwn 50:00:00:a1:94:cc secondary-pwn 50:00:00:a1:97:ac
switch(config-iscsi-tgt)# trespass
```

## Related Commands

Command	Description
<b>show iscsi virtual target</b>	Displays information about iSCSI virtual targets.

# islb abort

To discard a pending iSCSI Server Load Balancing (iSLB) configuration, use the **islb abort** command.

**islb abort**

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

**Command Default** None.

**Command Modes** Configuration mode.

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

**Usage Guidelines** You can use the **islb abort** command to discard the pending changes to the iSLB configuration and release the fabric lock. This action has no effect on the active configuration on any switch in the fabric.

The **islb abort** command can be issued only by the user who started the Cisco Fabric Services (CFS) session and only on the switch that started the CFS session.

## Examples

The following example discards the pending iSLB configuration distribution:

```
switch# config t
switch(config)# islb abort
```

Related Commands	Command	Description
	<b>clear islb session</b>	Clears a pending iSLB configuration. This command can be issued on any switch by a user with admin privileges.
	<b>islb commit</b>	Commits the iSLB configuration distribution and releases the fabric lock.
	<b>show islb cfs-session status</b>	Displays iSLB information.
	<b>show islb pending</b>	Displays the pending configuration changes.
	<b>show islb pending-diff</b>	Displays the differences between the pending configuration and the current configuration.

# islb commit

To commit a pending iSCSI server load balancing (iSLB) configuration, use the **islb commit** command.

## islb commit

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

**Command Default** None.

**Command Modes** Configuration mode.

Release	Modification
3.0(1)	This command was introduced.

**Usage Guidelines** You can use the **islb commit** command to commit the pending changes to the iSLB configuration and release the fabric lock. This action changes the active configuration on all Cisco MDS switches in the fabric.

The **islb commit** command can be issued only by the user who started the Cisco Fabric Services (CFS) session and only on the switch that started the CFS session.

## Examples

The following example commits the pending iSLB configuration distribution:

```
switch# config t
switch(config)# islb commit
```

## Related Commands

Command	Description
<b>clear islb session</b>	Clears a pending iSLB configuration. This command can be issued on any switch by a user with admin privileges.
<b>islb abort</b>	Discards the pending iSLB configuration distribution and releases the fabric lock.
<b>islb distribute</b>	Enables iSLB configuration distribution.
<b>show islb cfs-session status</b>	Displays iSLB information.
<b>show islb pending</b>	Displays the pending configuration changes.
<b>show islb pending-diff</b>	Displays the differences between the pending configuration and the current configuration.

# islb distribute

To enable Cisco Fabric Services for iSCSI Server Load Balancing (iSLB) configuration, use the **islb distribute** command. To disable the iSLB configuration distribution, use the **no** form of the command

**islb distribute**  
**no islb distribute**

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

**Command Default** Disabled.

**Command Modes** Configuration mode.

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

**Usage Guidelines** You can use the **islb distribute** command to enable the distribution of iSLB configuration information to other Cisco MDS switches in the fabric using the Cisco Fabric Services (CFS) infrastructure. You can synchronize the iSLB configuration across the fabric from the console of a single MDS switch.



**Note** The only initiator configuration that is distributed throughout the fabric using CFS is a statically mapped, iSLB initiator configuration. Dynamically mapped and statically mapped iSCSI initiator configurations are not distributed. iSCSI initiator idle-timeout and global authentication parameters are also distributed.

If you are using both iSLB and inter-VSAN routing (IVR), ensure that the following conditions are satisfied; otherwise, traffic may be disrupted in the fabric.

- You must enable both features on at least one switch in the fabric.
- You must configure and activate zoning from the switch for normal zones, IVR zones, and and iSLB zones.

## Examples

The following example enables iSLB configuration distribution:

```
switch# config t
switch(config)# islb distribute
```

The following example disables iSLB configuration distribution:

```
switch(config)# no islb distribute
```

Related Commands	Command	Description
	<b>clear islb session</b>	Clears a pending iSLB configuration. This command can be issued on any switch by a user with admin privileges.

<b>Command</b>	<b>Description</b>
<b>islb abort</b>	Discards the pending iSLB configuration distribution and releases the fabric lock.
<b>islb commit</b>	Commits the iSLB configuration distribution and releases the fabric lock.

# islb initiator

To configure the iSCSI server load balancing (iSLB) initiator and enter iSLB initiator configuration submode, use the **islb initiator** command. To delete the configured iSLB initiator, use the **no** form of the command.

```
islb initiator {ip-address {ip-addressip6-address} | name name}
no islb initiator name name
```

Syntax Description	Parameter	Description
	<b>ip-address</b>	Specifies the iSLB initiator node IP address.
	<i>ip-address</i>	Specifies the initiator IPv4 address.
	<i>ip6-address</i>	Specifies the initiator IPv6 address.
	<b>name</b> <i>name</i>	Specifies the iSLB initiator node name. The maximum size is 223.

**Command Default** None.

**Command Modes** Configuration mode.

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

**Usage Guidelines** You can use the **islb initiator** command to enter iSLB initiator configuration submode to configure static mapping for an iSLB initiator.

## Examples

The following example enters iSLB initiator configuration submode to configure static mapping (using the IPv4 *ip-address* option) for an iSLB initiator:

```
switch# config t
switch(config)# islb initiator ipaddress 10.1.2.3
switch(config-islb-init)#
```

The following example deletes the configured iSLB initiator:

```
switch(config)# no islb initiator ipaddress 10.1.2.3
```

The following example enters iSLB initiator configuration submode to configure static mapping (using the IPv6 option) for an iSLB initiator:

```
switch# config t
switch(config)# islb initiator ipaddress 1111.2222.3333.4::5
switch(config-islb-init)#
```

The following example deletes the configured iSLB initiator:

```
switch(config)# no islb initiator ipaddress 1111.2222.3333.4::5
```

The following example enters iSLB initiator configuration submode to configure static mapping (using the name option) for an iSLB initiator:

```
switch# config t
switch(config)# islb initiator name iqn.1987-02.co..cisco.initiator
switch(config-islb-init)#
```

The following example deletes the configured iSLB initiator:

```
switch(config)# no islb initiator ipaddress name iqn.1987-02.co..cisco.initiator
```

#### Related Commands

Command	Description
<b>show islb initiator configured</b>	Displays iSLB initiator configuration information.
<b>show islb initiator detail</b>	Displays more detailed information about the iSLB configuration.
<b>show islb initiator iscsi-session</b>	Displays iSLB session details.
<b>show islb initiator summary</b>	Displays iSLB initiator summary information.



## islb save-initiator

To permanently save the automatically assigned nWWN and pWWN mapping for the iSLB initiator, use the **islb save-initiator** command.

**islb save-initiator** [**ip-address** *ip-address* | **name** *name*]

<b>Syntax Description</b>	<b>ip-address</b> <i>ip-address</i>	(Optional) Specifies the initiator IP address. The format is <i>A.B.C.D</i> or <i>X:X:X::X</i> .
	<b>name</b> <i>name</i>	(Optional) Specifies the initiator name to be used from 1 to 223 characters.

**Command Default** None.

**Command Modes** Configuration mode.

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

**Usage Guidelines** Saving the automatically assigned nWWN and pWWN mapping allows the initiator to use the same mapping the next time it logs in.

You can convert a dynamic iSLB initiator to a static iSLB initiator and make its WWNs persistent.



**Note** You cannot convert a dynamic iSCSI initiator to a static iSLB initiator or a dynamic iSLB initiator to a static iSCSI initiator.



**Note** Making the dynamic mapping for iSLB initiators static is the same as for iSCSI.



**Note** Only a statically mapped iSLB initiator configuration is distributed throughout the fabric using CFS. Dynamically and statically configured iSCSI initiator configurations are not distributed.

### Examples

The following example saves the nWWNs and pWWNs that have automatically been assigned to the iSLB initiator whose name is specified:

```
switch# config t
switch(config)# islb save-initiator name iqn.1987-02.com.cisco.initiator
```

The following example saves the nWWNs and pWWNs that have automatically been assigned to the iSLB initiator whose IPv4 address is specified:

```
switch(config)# islb save-initiator ip-address 10.10.100.11
```

The following example saves the nWWNs and pWWNs that have automatically been assigned to all the iSLB initiators:

```
switch(config)# islb save-initiator
```

Please execute "copy run start" to keep the WWNs persistent across switch reboots

---

**Related Commands**

Command	Description
<b>show islb session</b>	Displays detailed iSLB session information.

# islb virtual-target name

To configure an iSLB virtual target and enter iSLB target configuration submode, use the **islb virtual-target name** command. To revert to the default values, use the **no** form of the command.

**islb virtual-target name** *name* {**all-initiator-permit** | **initiator** {*initiator-name* **permit** | **ip address** {*A.B.C.D* **permit** | *X:X:X::X* **permit**}} | **pWWN permit** | **revert-primary-port permit** | **trespass permit**}

**no islb virtual-target name** *name* {**all-initiator-permit** | **initiator** {*initiator-name* **permit** | **ip address** {*A.B.C.D* **permit** | *X:X:X::X* **permit**}} | **pWWN permit** | **revert-primary-port permit** | **trespass permit**}

**Syntax Description**

<i>name</i>	Specifies the virtual target name to be used. The minimum length is 16 bytes and the maximum length is 223 bytes.
<b>all-initiator-permit</b>	Configures all iSLB initiators to access the target.
<b>initiator</b>	Configures the iSLB initiator to access the target.
<i>initiator-name</i>	Specifies the initiator name. The minimum length is 16 bytes and the maximum length is 223 bytes.
<i>X:X:X::X permit</i>	Permits access to the specified target.
<b>ip address</b>	Specifies the initiator IP address. The format is <i>A.B.C.D</i> or <i>X:X:X::X</i> .
<b>pWWN permit</b>	Specifies the pWWN of the Fibre Channel target. The format is <i>hh:hh:hh:hh:hh:hh:hh:hh</i> .
<b>revert-primary-port permit</b>	Reverts to the primary port when it becomes active again.
<b>trespass permit</b>	Enables trespass support.

**Command Default**

Disabled.

**Command Modes**

Configuration mode.

**Command History**

Release	Modification
3.0(1)	This command was introduced.

**Usage Guidelines**

This command is used to configure a static target for access by iSLB initiators.

**Examples**

The following example creates a static virtual target and enters iSLB target configuration submode:

```
switch# config terminal
switch(config)# islb virtual-target name ABCDEFGHIJ1234567890
ips-hacl(config-islb-tgt)#
```

The following example allows all iSLB initiators to access the target:

```
ips-ha1(config-islb-tgt)# all-initiator-permit
```

The following command allows the specified IP address to access this virtual target:

```
switch(config-islb-tgt)# initiator ip-address 209.165.200.226 permit
```

The following example prevents the specified IP address from accessing virtual targets:

```
switch(config-islb-tgt)# no initiator ip-address 209.165.200.226 permit
```

The following example allows all initiators in this subnetwork to access this virtual target:

```
switch(config-islb-tgt)# initiator ip-address 10.50.0.0 255.255.255.0 permit
```

The following example prevents all initiators in this subnetwork from accessing virtual targets:

```
switch(config-islb-tgt)# no initiator ip-address 10.50.0.0 255.255.255.0 permit
```

The following example maps a pWWN to a Fibre Channel target:

```
ips-ha1(config-islb-tgt)# pwwn 26:00:01:02:03:04:05:06
```

#### Related Commands

Command	Description
<b>show islb virtual-target</b>	Displays information about iSLB virtual targets.

# islb vrrp

To configure iSCSI server load balancing (iSLB) on a Virtual Router Redundancy Protocol (VRRP) group, use the **islb vrrp** command. To disable the iSLB configuration on the VRRP group, use the **no** form of the command.

```
islb vrrp {group-number load-balance | ipv6 group-number load-balance}
no islb vrrp {group-number load-balance | ipv6 group-number load-balance}
```

## Syntax Description

<i>group-number</i>	Specifies an IPv4 Virtual Router group number. The range is 1 to 255.
<b>load-balance</b>	Enables load balancing on the VRRP group.
<b>ipv6</b>	Specifies IPv6 on the VRRP group.
<i>group-number</i>	Specifies an IPv6 Virtual Router group number. The range is 1 to 255.
<b>load-balance</b>	Enables load balancing on the VRRP group.

## Command Default

None.

## Command Modes

Configuration mode.

## Command History

Release	Modification
3.0(1)	This command was introduced.

## Usage Guidelines

The host is configured with a VRRP address as the portal address. When the VRRP master port receives the first iSCSI session from an initiator, it assigns a slave port to serve that particular host. The information is synchronized to all switches via Cisco Fabric Services (CFS) if recovery is needed when a master port fails. The initiator gets a temporary redirect iSCSI login response. The host then logs in to the slave port at its physical IP address. If the slave port goes down, the host will revert to the master port. The master port knows through CFS that the slave port has gone down and redirects the host to another slave port.

There are separate VRRP groups for IPv4 and IPv6. Each address family is allowed 256 virtual routers.



**Note** An initiator can also be redirected to the physical IP address of the master interface.



**Tip** The load balancing distribution is based on the number of initiators on a port and not on the number of sessions.




---

**Caution** A Gigabit Ethernet interface configured for iSLB can only be in one VRRP group because redirected sessions do not carry information about the VRRP IP address or group. This restriction allows the slave port to uniquely identify the VRRP group to which it belongs.

---




---

**Caution** Changing the VSAN membership, the forwarding mode, and the authentication of an iSCSI interface that is part of an iSLB VRRP group impacts load balancing on the interface.

---

The following example enables VRRP load balancing for IPv4 Virtual Router group 20:

```
switch# config t
switch(config)# islb vrrp 20 load-balance
```

The following example disables VRRP load balancing for IPv4 Virtual Router group 20:

```
switch(config)# no islb vrrp 20 load-balance
```

The following example enables VRRP load balancing for IPv6 Virtual Router group 30:

```
switch(config)# islb vrrp ipv6 30 load-balance
```

The following example disables VRRP load balancing for IPv6 Virtual Router group 30:

```
switch(config)# no islb ipv6 30 load-balance
```

---

#### Related Commands

Command	Description
<b>show islb session</b>	Displays detailed iSLB session information.

# islb zoneset activate

To activate iSCSI server load balancing (iSLB) auto zones, use the **islb zoneset activate** command.

**islb zoneset activate**

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

**Command Default** None.

**Command Modes** Configuration mode.

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

**Usage Guidelines** Auto-zoning of the initiator with the initiator targets is enabled by default. A zone set must be active for a VSAN for auto-zones to be created in that VSAN. The **zoneset activate** command creates auto-zones only if at least one other change has been made to the zone set.

**Examples** The following example activates an iSLB auto zone:

```
switch# config t
switch(config)# islb zoneset activate
```

Related Commands	Command	Description
	<b>show zoneset active</b>	Displays active zone sets.

# isns

To tag a Gigabit Ethernet or PortChannel interface to an Internet Storage Name Service (iSNS) profile, use the **isns** command in interface configuration submode. To untag the interface, use the **no** form of the command.

**isns** *profile-name*

**no isns** *profile-name*

## Syntax Description

<i>profile-name</i>	Specifies the iSNS profile name.
---------------------	----------------------------------

## Command Default

Disabled.

## Command Modes

Interface configuration submode.

## Command History

Release	Modification
2.0(x)	This command was introduced.

## Usage Guidelines

To use this command, iSNS must be enabled using the **isns-server enable** command.

Use the **isns reregister** command in EXEC mode to reregister associated iSNS objects (tagged to an iSNS profile) with the iSNS server.

## Examples

The following example shows how to tag a Gigabit Ethernet interface to an iSNS profile:

```
switch# config terminal
switch(config)# interface gigabitethernet 1/2
switch(config-if)# isns Profile1
```

The following example shows how to tag a PortChannel interface to an iSNS profile:

```
switch# config terminal
switch(config)# interface port-channel 2
switch(config-if)# isns Profile2
```

## Related Commands

Command	Description
<b>isns reregister</b>	Reregisters the iSNS object.
<b>isns-server enable</b>	Enables the iSNS server.
<b>show interface gigabitethernet</b>	Displays configuration and status information for a specified Gigabit Ethernet interface.
<b>show interface port-channel</b>	Displays configuration and status information for a specified PortChannel interface.
<b>show isns</b>	Displays iSNS information.



# isns distribute

To enable Cisco Fabric Services (CFS) distribution for Internet Storage Name Service (iSNS), use the **isns distribute** command. To disable this feature, use the **no** form of the command.

**isns distribute**  
**no isns distribute**

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

**Command Default** Enabled.

**Command Modes** Configuration mode.

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

**Usage Guidelines** To use this command, iSNS must be enabled using the **isns-server enable** command.

You can configure the pWWN and nWWN of iSCSI initiators and permit a group of iSCSI initiators to share a given nWWN and pWWN pair by using a proxy initiator. The number of iSCSI initiators that register with the iSNS server is more than the number of iSCSI targets that register with the iSNS server. To synchronize the iSCSI initiator entries across switches, you can distribute the iSCSI initiator configuration to iSNS servers across switches.

## Examples

The following example shows how to initiate iSNS information distribution:

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

The following example shows how to cancel iSNS information distribution:

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

Related Commands	Command	Description
	<b>isns-server enable</b>	Enables the iSNS server.
	<b>show isns</b>	Displays iSNS information.

## isns esi retries

To configure the number of entity status inquiry (ESI) retry attempts, use the **isns esi retries** command in configuration mode. To revert to the default value, use the **no** form of the command.

**isns esi retries** *number*  
**no isns esi retries** *number*

### Syntax Description

<i>number</i>	Specifies the number of retries. The range is 0 to 10.
---------------	--

### Command Default

3 retries.

### Command Modes

Configuration mode.

### Command History

Release	Modification
2.0(x)	This command was introduced.

### Usage Guidelines

To use this command, Internet Storage Name Service (iSNS) must be enabled using the **isns-server enable** command.

The iSNS client queries the ESI port at user-configured intervals. Receipt of a response indicates that the client is still alive. Based on the configured value, the interval specifies the number of failed tries before which the client is deregistered from the server.

### Examples

The following example shows how change the ESI retries limit to eight:

```
switch# config terminal
switch(config)# isns esi retries 8
```

### Related Commands

Command	Description
<b>isns-server enable</b>	Enables the iSNS server.
<b>show isns</b>	Displays iSNS information.

## isns profile name

To create an Internet Storage Name Service (iSNS) profile and enter iSNS profile configuration submode, use the **isns profile name** command in configuration mode. To delete the iSNS profile, use the **no** form of the command.

```
isns profile name profile-name
no isns profile name profile-name
```

<b>Syntax Description</b>	<i>profile-name</i> Specifies the profile name. Maximum length is 64 characters.
---------------------------	--

<b>Command Default</b>	None.
------------------------	-------

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

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

<b>Usage Guidelines</b>	To use this command, iSNS must be enabled using the <b>isns-server enable</b> command.
-------------------------	--

**Examples** The following example shows how to specify an iSNS profile name and enter iSNS profile configuration submode:

```
switch# config terminal
switch(config)# isns profile name UserProfile
switch(config-isns-profile)#
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>server</b>	Configures a server IP address in an iSNS profile.
	<b>show isns</b>	Displays iSNS information.

# isns reregister

To register all Internet Storage Name Service (iSNS) objects for an interface that is already tagged to an iSNS profile, use the **isns register** command.

**isns reregister** {**gigabitethernet** *slot/number* | **port-channel** *channel-group*}

## Syntax Description

<b>gigabitethernet</b> <i>slot/port</i>	Specifies tagged Gigabit Ethernet interface slot and port.
<b>port-channel</b> <i>channel-group</i>	Specifies tagged PortChannel group. The range is 1 to 128.

## Command Default

None.

## Command Modes

EXEC mode.

## Command History

Release	Modification
1.3(1)	This command was introduced.

## Usage Guidelines

Use this command to reregister portals and targets with the iSNS server for a tagged interface.

## Examples

The following command reregisters portal and targets for a tagged interface:

```
switch# isns reregister gigabitethernet 1/4
```

## Related Commands

Command	Description
<b>show isns profile</b>	Displays details for configured iSNS profiles.

# isns-server enable

To enable the Internet Storage Name Service (iSNS) server, use the **isns-server enable** command in configuration mode. To disable iSNS, use the **no** form of the command.

**isns-server enable**  
**no isns-server enable**

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

**Command Default** Disabled.

**Command Modes** Configuration mode.

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

**Usage Guidelines** Performing the **isns-server enable** command enables the commands used to configure iSNS.

**Examples** The following example shows how to enable iSNS:

```
switch# config terminal
switch(config)# isns-server enable
```

The following example shows how to disable iSNS:

```
switch# config terminal
switch(config)# no isns-server enable
```

Related Commands	Command	Description
	<b>isns distribute</b>	Enables iSNS distributed support.
	<b>isns esi retries</b>	Configures ESI retry attempts.
	<b>isns profile name</b>	Creates and configures iSNS profiles.
	<b>server</b>	Configures iSNS server attributes.
	<b>show isns</b>	Displays iSNS information.

## ivr aam pre-deregister-check

To configure fabric precheck before deregistering IVR with AAM, use the **ivr aam pre-deregister-check** command in configuration mode.

**ivr aam pre-deregister-check**

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

**Command Default** None.

**Command Modes** configuration mode.

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

**Usage Guidelines** None.

**Examples** The following example shows how to configure precheck before deregistering IVR with AAM:

```
switch# config terminal
switch(config)# feature ivr
switch(config-if)# ivr distribute
switch(config-if)# ivr nat
switch(config-if)# ivr commit
switch(config-if)# ivr aam pre-deregister-check
switch(config-if)#
```

Related Commands	Command	Description
	<b>show ivr aam</b>	Displays ivr aam status.

# ivr aam register

To register IVR with AAM, use the **ivr aam register** command in configuration submenu. To deregister IVR with AAM, use the **no** form of the command.

**ivr aam register**  
**no ivr aam register**

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

**Command Default** None.

**Command Modes** configuration mode.

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

**Usage Guidelines** None.

**Examples** The following example shows how to register IVR with AAM:

```
switch# config terminal
switch(config)# feature ivr
switch(config-if)# ivr distribute
switch(config-if)# ivr nat
switch(config-if)# ivr commit
switch(config-if)# ivr aam register
switch(config-if)# 2009 Oct 20 22:12:32 isola-77 last message repeated 7 times
```

The following example shows how to deregister IVR with AAM:

```
switch# config terminal
switch(config)# feature ivr
switch(config-if)# ivr distribute
switch(config-if)# ivr nat
switch(config-if)# ivr commit
switch(config-if)# ivr aam pre-deregister-check
switch(config)# no ivr aam register
```

You could use "show ivr aam pre-deregister-check" to check pre-deregister status. If the status indicates a failure, but you still go ahead with the commitment, the deregister might fail.

```
switch(config)#
```

Related Commands	Command	Description
	<b>show ivr aam</b>	Displays IVR AAM status.

## ivr abort

To discard an Inter-VSAN Routing (IVR) CFS distribution session in progress, use the **ivr abort** command in configuration mode.

### ivr abort

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

**Command Default** None.

**Command Modes** Configuration mode.

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

**Usage Guidelines** None.

**Examples** The following example shows how to discard an IVR CFS distribution session in progress:

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

Related Commands	Command	Description
	<b>ivr distribute</b>	Enables CFS distribution for IVR.
	<b>show ivr</b>	Displays IVR CFS distribution status and other details.



# ivr commit

To apply the pending configuration pertaining to the Inter-VSAN Routing (IVR) Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **ivr commit** command in configuration mode.

## ivr commit

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

**Command Default** None.

**Command Modes** Configuration mode.

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

**Usage Guidelines** None.

**Examples** The following example shows how to apply an IVR configuration to the switches in the fabric:

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

Related Commands	Command	Description
	<b>ivr distribute</b>	Enables CFS distribution for IVR.
	<b>show ivr</b>	Displays IVR CFS distribution status and other details.

## ivr copy active-service-group user-configured-service-group

To copy the active service group to the user-configured service group, use the **ivr copy active-service-group user-configured-service-group** command in EXEC mode.

**ivr copy active-service-group user-configured-service-group**

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

**Command Default** None.

**Command Modes** EXEC mode.

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

**Usage Guidelines** None.

**Examples** The following example copies the active service group to the user-defined service group:

```
switch# ivr copy active-service-group user-configured-service-group
```

```
Successfully copied active service group to user-configured service group database
```

Related Commands	Command	Description
	<b>clear ivr service-group database</b>	Clears the IVR service group database.
	<b>show ivr service-group</b>	Displays IVR service groups.

# ivr copy active-topology user-configured-topology

To copy the active inter-VSAN routing (IVR) VSAN topology to the user configured topology, use the **ivr copy active-topology user-configured-topology** command in EXEC mode.

**ivr copy active-topology user-configured-topology**

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

**Command Default** None.

**Command Modes** EXEC mode.

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

**Usage Guidelines** The **ivr copy active-topology user-configured-topology** command is useful if you need to edit the active IVR topology, which is not allowed. Instead you copy the active IVR topology to the user configured topology, and then edit the user configured topology.

## Examples

The following example copies the active IVR topology to the user configured topology:

```
switch# ivr copy active-topology user-configured-topology
Successfully copied active VSAN-topology to user-configured topology database
```

Related Commands	Command	Description
	<b>ivr copy active-zoneset full-zoneset</b>	Copies the active zone set to the full zone set.
	<b>ivr copy auto-topology user-configured topology</b>	Copies the automatically discovered inter-VSAN routing (IVR) VSAN topology to the user configured topology.
	<b>show ivr vsan topology</b>	Displays the IVR VSAN topology configuration.

## ivr copy active-zoneset full-zoneset

To copy the active zone set to the full zone set, use the **ivr copy active-zoneset full-zoneset** command in EXEC mode.

**ivr copy active-zoneset full-zoneset**

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

**Command Default** None.

**Command Modes** EXEC mode.

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

**Usage Guidelines** Copying the active zone set to the full zone set may overwrite common zone and zone set configurations in the full zoning database.

**Examples** The following example copies the active zone set to the full zone set:

```
switch# ivr copy active-zoneset full-zoneset

WARNING: This command may overwrite common zones/zonesets
         in the IVR full zoneset database
Please enter yes to proceed.(y/n) [n]?
```

Related Commands	Command	Description
	<b>ivr copy active-topology user-configured topology</b>	Copies the active inter-VSAN routing (IVR) VSAN topology to the user configured topology.
	<b>ivr copy auto-topology user-configure topology</b>	Copies the automatically discovered inter-VSAN routing (IVR) VSAN topology to the user configured topology.
	<b>show ivr zoneset active</b>	Displays the active IVR zone set.

# ivr copy auto-topology user-configured-topology

To copy the automatically discovered inter-VSAN routing (IVR) VSAN topology to the user configured topology, use the **ivr copy auto-topology user-configured-topology** command in EXEC mode.

**ivr copy auto-topology user-configured-topology**

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

**Command Default** None.

**Command Modes** EXEC configuration mode.

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

**Usage Guidelines** After using the **ivr copy auto-topology user-configured-topology** command to copy the automatically discovered VSAN topology into the user- configured topology you must use the **ivr commit** command to apply the pending configuration changes to the IVR topology using Cisco Fabric Services (CFS) distribution.

## Examples

The following example copies the automatically discovered VSAN topology into the user configured topology:

```
switch# ivr copy auto-topology user-configured-topology
```

Related Commands	Command	Description
	<b>ivr commit</b>	Applies the changes to the IVR topology.
	<b>ivr copy active-topology user-configured topology</b>	Copies the active inter-VSAN routing (IVR) VSAN topology to the user configured topology.
	<b>ivr copy active-zoneset full-zoneset</b>	Copies the active zone set to the full zone set.
	<b>show ivr vsan topology</b>	Displays the IVR VSAN topology configuration .

# ivr distribute

To enable Cisco Fabric Services (CFS) distribution for Inter-VSAN Routing (IVR), use the **ivr distribute** command. To disable this feature, use the **no** form of the command.

**ivr distribute**  
**no ivr distribute**

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

**Command Default** Disabled.

**Command Modes** Configuration mode.

Release	Modification
2.0(x)	This command was introduced.

**Usage Guidelines** None.

**Examples** The following example shows how to enable IVR fabric distribution:

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

Command	Description
<b>ivr commit</b>	Commits temporary IVR configuration changes to the active configuration.
<b>show ivr</b>	Displays IVR CFS distribution status and other details.

# ivr enable

To enable the Inter-VSAN Routing (IVR) feature, use the **ivr enable** command in configuration mode. To disable this feature, use the **no** form of the command.

**ivr enable**  
**no ivr enable**

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

**Command Default** Disabled.

**Command Modes** Configuration mode.

Command History	Release	Modification
	1.3(1)	This command was introduced.
	NX-OS 4.1(1b)	This command was deprecated.

**Usage Guidelines** The IVR feature must be enabled in all edge switches in the fabric that participate in the IVR. The configuration and display commands for the IVR feature are only available when IVR is enabled on a switch. When you disable this configuration, all related configurations are automatically discarded.



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

## Examples

The following command enters the configuration mode and enables the IVR feature on this switch:

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

Related Commands	Command	Description
	<b>show ivr</b>	Displays IVR feature information.

## ivr fcdomain database autonomous-fabric-num

To create IVR persistent FC IDs, use the **ivr fcdomain database autonomous-fabric-num** command. To delete the IVR fcdomain entry for a given AFID and VSAN, use the **no** form of the command.

```
ivr fcdomain database autonomous-fabric-num afid-num vsan vsan-id
no ivr fcdomain database autonomous-fabric-num afid-num vsan vsan-id
```

### Syntax Description

<i>afid-num</i>	Specifies the current AFID. The range is 1 to 64.
<i>vsan vsan-id</i>	Specifies the current VSAN. The range is 1 to 4093.

### Command Default

None.

### Command Modes

Configuration mode.

### Command History

Release	Modification
2.1(2)	This command was introduced.

### Usage Guidelines

This configuration only takes effect when NAT mode is enabled.

### Examples

The following example shows how to enter IVR fcdomain database configuration submode for AFID 10 and VSAN 20:

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config) fcdomain#
```

The following example shows how to delete all persistent FC ID database entries for AFID 10 and VSAN 20:

```
switch# config t
switch(config)# no ivr fcdomain database autonomous-fabric-num 10 vsan 20
```

### Related Commands

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



# ivr nat

To explicitly enable Network Address Translation (NAT) functionality for Inter-VSAN Routing (IVR), use the **ivr nat** command in configuration mode. To disable this feature, use the **no** form of the command.

**ivr nat**  
**no ivr nat**

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

**Command Default** Disabled.

**Command Modes** Configuration mode.

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

**Usage Guidelines** The **ivr nat** command allows you to explicitly enable NAT functionality of IVR. Upgrading to SAN-OS Release 2.x from SAN-OS Release 1.3.x does not automatically enable the Fibre Channel NAT functionality. This command also allows you to continue to operate in non-NAT mode even in SAN-OS Release 2.x and later and NX-OS.



**Note** You might need to operate in non-NAT mode to support proprietary protocols that embed FCIDs in the frame payloads.

## Examples

The following example shows how to explicitly enable NAT functionality for IVR:

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

Related Commands	Command	Description
	<b>show ivr</b>	Displays IVR feature information.

# ivr refresh

To refresh devices being advertised by Inter-VSAN Routing (IVR), use the **ivr refresh** command in EXEC mode.

**ivr refresh**

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

**Command Default** None.

**Command Modes** EXEC mode.

Command History	Release	Modification
	2.0(2)	This command was introduced.

**Usage Guidelines** The **IVR refresh** command runs internally when IVR zone set or topology is activated. The limit for the maximum number of IVR zones per VSAN is 250 zones (two members per zone).

**Examples** The following example shows refresh devices being advertised by IVR:

```
switch# ivr refresh
```

Related Commands	Command	Description
	<b>ivr enable</b>	Enables the Inter-VSAN Routing (IVR) feature.
	<b>ivr withdraw domain</b>	Withdraws an overlapping virtual domain from a specified VSAN.

# ivr service-group activate

To activate an inter-VSAN routing (IVR) service group, use the **ivr service-group activate** command in configuration mode. To disable this feature, use the **no** form of the command.

```
ivr service-group activate [default-sg-deny]
no ivr service-group activate [default-sg-deny]
```

<b>Syntax Description</b>	<b>default-sg-deny</b> (Optional) Sets the policy to deny for the default service group.
---------------------------	--

**Command Default** Deactivated.

**Command Modes** Configuration mode.

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

**Usage Guidelines** You must activate a configured IVR service group for the IVR service group to take effect. Once a configured IVR service group is activated, it replaces the currently activated service group, if there is one.

Activating an IVR service group with the **default-sg-deny** option sets the default service group policy to deny. To change the default service group policy to allow, issue the **ivr service-group activate** command again, but without the **default-sg-deny** option.

## Examples

The following example activates the default IVR service group:

```
switch# config terminal
switch(config)# ivr service-group activate
```

The following example sets the default IVR service group policy to deny:

```
switch# config terminal
switch(config)# ivr service-group activate default-sg-deny
```

The following example disables the default service group:

```
switch# config terminal
switch(config)# no ivr service-group activate
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ivr enable</b>	Enables inter-VSAN routing (IVR).
	<b>ivr service-group name</b>	Configures an inter-VSAN routing (IVR) service group.
	<b>show ivr service-group database</b>	Displays an inter-VSAN routing service group database.

## ivr service-group name

To configure an Inter-VSAN Routing (IVR) service group, use the **ivr service-group name** command in configuration mode. To disable this feature, use the **no** form of the command.

**ivr service-group name** *service-group*  
**no ivr service-group name** *service-group*

### Syntax Description

<i>service-group</i>	Specifies the service group name.
----------------------	-----------------------------------

### Command Default

Disabled.

### Command Modes

Configuration mode.

### Command History

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

### Usage Guidelines

In a complex network topology, you might only have a few IVR-enabled VSANs. To reduce the amount of traffic to non-IVR-enabled VSANs, you can configure a service group that restricts the traffic to the IVR-enabled VSANs. A service group is a combination of AFIDs and VSANs. Up to 16 service groups can be configured. A VSAN or AFID can belong to just one service group. When a new IVR-enabled switch is added to the network, you must update the service group to include the new VSANs.

There can be a maximum of 128 AFID/VSAN combinations in all service group. However, all 128 combinations can be in one service group.

The default service group ID is 0. The default service group is for all VSANs that are not a part of a user-defined service group.

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

- IVR using the **ivr commit** command
- IVR distribution using the **ivr commit** command
- Automatic IVR topology discovery using the **ivr commit auto command**.

Using the **autonomous-fabric-id (IVR topology database configuration)** command, you can restrict the IVR traffic to the AFIDs and VSANs configured in the service group.

### Examples

The following example shows how to configure an IVR service group and change to IVR service group configuration mode:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ivr enable
switch(config)# ivr vsan-topology auto
switch(config)# ivr service-group name serviceGroup1
switch(config-ivr-sg)#
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>ivr enable</b>	Enables the Inter-VSAN Routing (IVR) feature
<b>ivr vsan-topology auto</b>	Enables automatic discovery of the IVR topology.
<b>show ivr</b>	Displays IVR feature information.

# ivr virtual-fcdomain-add

To add the Inter-VSAN Routing (IVR) virtual domains in a specific VSAN(s) to the assigned domains list in that VSAN, use the **ivr virtual-fcdomain-add** command. To delete the IVR virtual domains, use the **no** form of the command.

```
ivr virtual-fcdomain-add vsan-ranges vsan-range
no ivr virtual-fcdomain-add vsan-ranges vsan-range
```

<b>Syntax Description</b>	<table border="1"> <tr> <td><b>vsan-ranges</b> <i>vsan-range</i></td> <td>Specifies the IVR VSANs or range of VSANs. The range of values for a VSAN ID is 1 to 4093.</td> </tr> </table>	<b>vsan-ranges</b> <i>vsan-range</i>	Specifies the IVR VSANs or range of VSANs. The range of values for a VSAN ID is 1 to 4093.
<b>vsan-ranges</b> <i>vsan-range</i>	Specifies the IVR VSANs or range of VSANs. The range of values for a VSAN ID is 1 to 4093.		

**Command Default** Disabled.

**Command Modes** Configuration mode.

<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>1.3(4)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	1.3(4)	This command was introduced.
Release	Modification				
1.3(4)	This command was introduced.				

**Usage Guidelines** Use the **no ivr virtual-fcdomain-add** command to remove the currently active domains from the fcdomain manager list in a specified VSAN.

## Examples

The following command adds the IVR virtual domains in VSAN:

```
switch# config terminal
switch(config)# ivr virtual-fcdomain-add vsan-ranges 1
```

The following command reverts to the factory default of not adding IVR virtual domains:

```
switch# config terminal
switch(config)# no ivr virtual-fcdomain-add vsan-ranges 1
```

<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>ivr withdraw domain</b></td> <td>Removes overlapping domains.</td> </tr> <tr> <td><b>show ivr virtual-fcdomain-add-status</b></td> <td>Displays the configured VSAN topology for a fabric.</td> </tr> </tbody> </table>	Command	Description	<b>ivr withdraw domain</b>	Removes overlapping domains.	<b>show ivr virtual-fcdomain-add-status</b>	Displays the configured VSAN topology for a fabric.
Command	Description						
<b>ivr withdraw domain</b>	Removes overlapping domains.						
<b>show ivr virtual-fcdomain-add-status</b>	Displays the configured VSAN topology for a fabric.						

## ivr virtual-fcdomain-add2

To configure the request domain\_ID (RDI) mode in a specific autonomous fabric ID (AFID) and VSAN for all IVR-enabled switches, use the **ivr virtual-fcdomain-add2** command. To delete the RDI mode, use the **no** form of the command.

```
ivr virtual-fcdomain-add2 autonomous-fabric-id value vsan-ranges value
no ivr virtual-fcdomain-add2 autonomous-fabric-id value vsan-ranges value
```

Syntax Description	Parameter	Description
	<b>fabric-id</b> <i>value</i>	Specifies the fabric ID on which the RDI mode needs to be configured.
	<b>vsan-ranges</b> <i>value</i>	Specifies the VSAN range value on which the RDI mode needs to be configured.

**Command Default** None.

**Command Modes** Configuration mode.

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

**Usage Guidelines** This is a CFS distributable command.

**Examples** The following example configures the RDI mode on a specific AFID and VSAN:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch# ivr virtual-fcdomain-add2 autonomous-fabric-id 1 vsan-ranges 2
switch# fabric is now locked for configuration. Please 'commit' configuration when done.
switch(config)# ivr commit
```

Related Commands	Command	Description
	<b>show ivr virtual-fcdomain-add-status2</b>	Displays the RDI mode in a specific AFID and VSAN for all IVR-enabled switches.

# ivr vsan-topology

To configure manual or automatic discovery of the Inter-VSAN Routing (IVR) topology, use the **ivr vsan-topology** command in configuration mode.

**ivr vsan-topology** {**activate** | **auto**}

## Syntax Description

<b>activate</b>	Configures manual discovery of the IVR topology and disables automatic discovery mode.
<b>auto</b>	Configures automatic discovery of the IVR topology.

## Command Default

Disabled.

## Command Modes

Configuration mode.

## Command History

Release	Modification
1.3(1)	This command was introduced.
2.1(1a)	Added <b>auto</b> keyword.

## Usage Guidelines

To use this command you must first enable IVR using the **ivr enable** command and configure the IVR database using the **ivr vsan-topology database** command.



**Caution** Active IVR topologies cannot be deactivated. You can only switch to automatic topology discovery mode.

## Examples

The following **ivr vsan-topology activate** command activates the VSAN topology database:

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

The following command enables VSAN topology database auto mode, which allows the switch to automatically discover the IVR topology:

```
switch(config)# ivr vsan-topology auto
```

## Related Commands

Command	Description
<b>autonomous-fabric-id(IVR topology database configuration)</b>	Configure an autonomous phobic ID into the IVR topology database.



Command	Description
<b>ivr enable</b>	Enables the Inter-VSAN Routing (IVR) feature.
<b>show ivr</b>	Displays IVR feature information.

## ivr vsan-topology auto

To configure automatic discovery of the Inter-VSAN Routing (IVR) topology, use the **ivr vsan-topology auto** command in configuration mode.

**ivr vsan-topology auto**

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

**Command Default** Disabled.

**Command Modes** Configuration mode.

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

**Usage Guidelines** To use this command you must first enable IVR using the **ivr enable** command. IVR configuration distribution must be enabled using the **ivr distribute** command before configuring automatic topology discovery. Once automatic IVR topology discovery is enabled, you cannot disable IVR configuration distribution.

### Examples

The following command enables VSAN topology database auto mode, which allows the switch to automatically discover the IVR topology.

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

    activate  Activate VSAN topology database for inter-VSAN routing
    auto      Enable discovery of VSAN topology for inter-VSAN routing
    database  Configure VSAN topology database for inter-VSAN routing
switch(config)# ivr vsan-topology auto
switch(config)#
```

### Related Commands

Command	Description
<a href="#">ivr enable</a>	Enables the Inter-VSAN Routing (IVR) feature.
<a href="#">autonomous-fabric-id (IVR topology database configuration)</a>	Configure an autonomous phobic ID into the IVR topology database
<b>show ivr</b>	Displays IVR feature information.

## ivr vsan-topology database

To configure an Inter-VSAN Routing (IVR) topology database, use the **ivr vsan-topology database** command in configuration mode. To delete an IVR topology database, use the **no** form of the command.

**ivr vsan-topology database**  
**no ivr vsan-topology database**

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

**Command Default** None.

**Command Modes** Configuration mode.

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

**Usage Guidelines** To use this command you must first enable IVR using the **ivr enable** command. You can have up to 64 VSANs (or 128 VSANs as of Cisco MDS SAN-OS Release 2.1(1a)) in an IVR topology. Specify the IVR topology using the following information:

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



**Note** The use of a single AFID does not allow for VSANs that are logically and physically separate but have the same VSAN number in an IVR topology.



**Caution** You can only configure a maximum of 128 IVR-enabled switches and 64 distinct VSANs (or 128 distinct VSANs as of Cisco MDS SAN-OS Release 2.1(1a)) in an IVR topology.

The **no ivr vsan-topology database** command only clears the configured database, not the active database. You can only delete the user-defined entries in the configured database. Auto mode entries only exist in the active database.

### Examples

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

```
switch# config terminal
```

```

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

```

**Related Commands**

Command	Description
<b>autonomousfabric-id(IVR topology database configuration)</b>	Configures an autonomous phobic ID into the IVR topology database
<b>ivr enable</b>	Enables the Inter-VSAN Routing (IVR) feature.
<b>show ivr</b>	Displays IVR feature information.

# ivr withdraw domain

To withdraw overlapping virtual domain from a specified VSAN, use the **ivr withdraw domain** command in EXEC mode.

**ivr withdraw domain** *domain-id* **vsan** *vsan-id*

Syntax Description	Parameter	Description
	<i>domain-id</i>	Specifies the domain id. The range is 1 to 239.
	<b>vsan</b> <i>vsan-id</i>	Specifies the VSAN ID. The range is 1 to 4093.

**Command Default** None.

**Command Modes** EXEC mode.

Command History	Release	Modification
	1.3(4)	This command was introduced.

**Usage Guidelines** When you enable the **ivr virtual-fcdomain-add** command, links may fail to come up due to overlapping virtual domain identifiers. If so, temporarily withdraw the overlapping virtual domain from that VSAN using the **ivr withdraw domain** command in EXEC mode.

**Examples** The following command withdraws overlapping domains:

```
switch# ivr withdraw domain 10 vsan 20
```

Related Commands	Command	Description
	<b>show ivr virtual-fcdomain-add-status</b>	Displays the configured VSAN topology for a fabric.

## ivr zone name

To configure a zone for Inter-VSAN Routing (IVR), use the **ivr zone name** command. To disable a zone for IVR, use the **no** form of the command.

**ivr zone name** *ivzs-name*  
**no ivr zone name** *ivz-name*

### Syntax Description

<i>ivz-name</i>	Specifies the IVZ name. Maximum length is 59 characters.
-----------------	--

### Command Default

None.

### Command Modes

Configuration mode.

### Command History

Release	Modification
1.3(1)	This command was introduced.

### Usage Guidelines

This command enters IVR zone configuration submode.

### Examples

The following command enters the configuration mode, enables the IVR feature, creates an IVZ, and adds a pWWN-VSAN member:

```
switch# config terminal
switch(config)# ivr enable
switch(config)# ivr zone name Ivz_vsan2-3
switch(config-ivr-zone)# member pwn 21:00:00:e0:8b:02:ca:4a vsan 3
```

### Related Commands

Command	Description
<b>show ivr</b>	Displays IVR feature information.

## ivr zone rename

To rename an inter-VSAN routing (IVR) zone, use the **ivr zone rename** command.

**ivr zone rename** *current-name new-name*

Syntax Description	
<i>current-name</i>	Specifies the current zone name. The maximum size is 64 characters.
<i>new-name</i>	Specifies the new zone name. The maximum size is 64 characters.

**Command Default** None.

**Command Modes** EXEC mode.

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

**Usage Guidelines** None.

**Examples** The following example renames the IVR zone from *east* to *west*:

```
switch# ivr zone rename east west
```

Related Commands	Command	Description
	<b>ivr zone name</b>	Creates and configures an IVR zone.
	<b>show ivr</b>	Displays IVR information.

# ivz zoneset

To configure a zoneset for Inter-VSAN Routing (IVR), use the **ivz zoneset** command. To revert to the factory defaults, use the **no** form of the command.

```
ivz zoneset {activate name ivzs-name [force] | name ivzs-name}
no ivz zoneset {activate name ivzs-name [force] | name ivzs-name}
```

## Syntax Description

<b>activate</b>	Activates a previously configured IVZS.
<b>force</b>	(Optional) Forces a IVZS activation
<b>name ivzs-name</b>	Specifies the IVZS name. Maximum length is 59 characters.

## Command Default

None.

## Command Modes

Configuration mode.

## Command History

Release	Modification
1.3(1)	This command was introduced.

## Usage Guidelines

This command enters IVR zoneset configuration submode.



**Note** To replace the active IVR zone set with a new IVR zone set without disrupting traffic, activate the new IVR zone set without deactivating the current active IVR zone set.

## Examples

The following command enters the configuration mode, enables the IVR feature, creates an IVZS, adds a IVZ member, and activates the IVZS:

```
switch# config terminal
switch(config)# ivz enable
switch(config)# ivz zoneset name Ivz_zoneset1
switch(config-ivz-zoneset)# member Ivz_vsan2-3
switch(config-ivz-zoneset)# exit
switch(config)# ivz zoneset activate name IVR_ZoneSet1
```

## Related Commands

Command	Description
<b>show ivz</b>	Displays IVR feature information.



## ivr zoneset rename

To rename an inter-VSAN routing (IVR) zone set, use the **ivr zoneset rename** command.

**ivr zoneset rename** *current-name new-name*

Syntax Description	
<i>current-name</i>	Specifies the current zone set name. The maximum size is 64 characters.
<i>new-name</i>	Specifies the new zone set name. The maximum size is 64 characters.

**Command Default** None.

**Command Modes** EXEC mode.

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

**Usage Guidelines** None.

**Examples** The following example renames the IVR zone set from *north* to *south*:

```
switch# ivr zoneset rename north south
```

Related Commands	Command	Description
	<b>ivr zoneset name</b>	Creates and configures an IVR zone set.
	<b>show ivr</b>	Displays IVR information.

