



P Commands

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

passive-mode

To configure the required mode to initiate an IP connection, use the **passive-mode** command. To enable passive mode for the FCIP interface, use the **no** form of the command.

passive-mode

no passive-mode

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

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

Command Modes	Interface configuration submode.
----------------------	----------------------------------

Command History	Release	Modification
	1.1(1)	This command was introduced.

Usage Guidelines	Access this command from the switch(config-if)# submode.
	By default, the active mode is enabled to actively attempt an IP connection.
	If you enable the passive mode, the switch does not initiate a TCP connection and only waits for the peer to connect to it.

Examples	The following example enables passive mode on an FCIP interface:
	switch# config terminal
	switch(config)# interface fcip 1
	switch(config-if)# passive-mode

Related Commands	Command	Description
	show interface fcip	Displays an interface configuration for a specified FCIP interface.

password strength-check

To enable password strength checking, use the **password strength-check** command. To disable this feature, use the **no** form of the command.

password strength-check

no password strength-check

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

Defaults	Enabled.
-----------------	----------

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

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

Usage Guidelines	When you enable password strength checking, the NX-OS software only allows you to create strong passwords.
-------------------------	--

The characteristics for strong passwords included the following:

- At least 8 characters long
- Does not contain many consecutive characters (such as abcd)
- Does not contain many repeating characters (such as aaabb)
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

The following are examples of strong passwords:

- If2COM18
- 2004AsdfLkj30

Examples	The following example shows how to enable secure standard password:
-----------------	---

```
switch(config)# password strength-check
switch(config)#
```

Related Commands

Command	Description
show password strength-check	Displays if the password strength check is enabled.

pathtrace

To trace the route statistics, use the **pathtrace** command.

pathtrace domain *domain-id* **vsan** *vsan-id* [**reverse**] [**detail**]

pathtrace fcid *fc-id* **vsan** *vsan-id* [**reverse**] [**detail**]

Syntax Description

domain	Specifies the destination domain.
<i>domain-id</i>	Specifies the destination domain ID. The range is from 1 to 239.
vsan	Specifies the VSAN ID.
<i>vsan-id</i>	Specifies the VSAN number. The range is from 1 to 4094.
fcid	Specifies the FC-id of the destination N-Port.
<i>fc-id</i>	The range is from 0x0 to 0xffffffff.
detail	(Optional) Specifies the detailed statistics. This CLI when used with the detail option displays the statistics of the egress port at every hop.
reverse	(Optional) Specifies the trace reverse path. The reverse option of the CLI can be used to display the reverse path (from destination back to the source) information.

Defaults

None.

Command Modes

Any mode.

Command History

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

Usage Guidelines

Pathtrace command can be executed only for 6.2(5) and above releases.

Pathtrace is a utility tool which traces the path from the switch on which the cli is executed to a destination domain / destination device referenced by a fcid.

If pathtrace is executed in a topology where any device is running on a non pathtrace supported image, the pathtrace request packets will be dropped and the command will not be processed.

In the display embedded indicates that the respective port is an internal port.

The statistics displayed for various types of egress interfaces is as follows:

- FC interface.
- VFC interface: statistics are displayed for the associated Ethernet interface.
- FC port channel: The statistics are displayed at port channel level.
- VFC port channel: The statistics are displayed at the VFC port channel level.
- FCIP/ FCIP port channel: The statistics will not be displayed in 6.2.5 release.

- Pathtrace will not be supported for ioa, isapi and tie devices (DDTS: CSCuj41316).

Additional information supported for **Pathtrace** command is as follows:

- Interop mode is not supported. Pathtrace utility is supported on MDS platforms alone and will not work in combination with the other vendor switches. It will also not work on the N5k devices.
- Virtual domain support (IVR for Pathtrace) is not be supported for pathtrace.
- SNMP support is not there for Pathtrace.
- Maximum number of hops supported is 16 without reverse and 8 with the reverse option.
- – is displayed for unavailable/unsupported counters.
- The statistics are displayed only for the egress interface only.



Note

FCtrace and Pathtrace will not be supported in IVR scenario. FCtrace is supported on TE ports only.

Examples

The following example shows how to specify the Pathtrace for the domain and the fcid with all the options

```
switch# pathtrace fcid 0xca016c vsan 2000
```

The final destination port type is F_Port

Hop	Domain	In-Port	Out-Port	Speed	Cost	Switchname
0	111	embedded	fc1/6	4G	250	huashan22
1	202	fc1/6	fc1/1	2G	-	huashan21

NOTE: The stats are displayed for the egress interface only

```
switch# pathtrace fcid 0xca016c vsan 2000 reverse
```

The final destination port type is F_Port

Hop	Domain	In-Port	Out-Port	Speed	Cost	Switchname
0	111	embedded	fc1/6	4G	250	huashan22
1	202	fc1/6	fc1/1	2G	-	huashan21
2	202	embedded	fc1/6	4G	250	huashan21
3	111	fc1/6	embedded	-	-	huashan22

NOTE: The stats are displayed for the egress interface only

```
switch# pathtrace fcid 0xca016c vsan 2000 reverse domain
```

The final destination port type is F_Port

Hop	0	Domain	In-Port	Out-Port	Speed	Cost	Switchname
		111	embedded	fc1/6	4G	250	huashan22

Stats for egress port: fc1/6
TxRt(B/s): 2944

```

RxRt (B/s): 3632
  TxB_B: 32
  RxB_B: 32
  TxFrame: 137467
  RxFrame: 137475
  Errors: 0
  Discard: 0
  CRC: 0
-----
Hop 1      Domain In-Port      Out-Port      Speed Cost  Switchname
          202    fc1/6        fc1/1        2G    -    huashan21
-----
Stats for egress port: fc1/1
  TxRt (B/s): 1424
  RxRt (B/s): 1528
  TxB_B: 0
  RxB_B: 32
  TxFrame: 711
  RxFrame: 649
  Errors: 0
  Discard: 15
  CRC: 0
-----
Hop 2      Domain In-Port      Out-Port      Speed Cost  Switchname
          202    embedded    fc1/6        4G    250    huashan21
-----
Stats for egress port: fc1/6
  TxRt (B/s): 3632
  RxRt (B/s): 2952
  TxB_B: 32
  RxB_B: 32
  TxFrame: 137476
  RxFrame: 137467
  Errors: 0
  Discard: 0
  CRC: 0
-----
Hop 3      Domain In-Port      Out-Port      Speed Cost  Switchname
          111    fc1/6        embedded      -     -     huashan22
-----
Stats for egress port: embedded
  TxRt (B/s): -
  RxRt (B/s): -
  TxB_B: -
  RxB_B: -
  TxFrame: -
  RxFrame: -
  Errors: -
  Discard: -
  CRC: -

```

NOTE: The stats are displayed for the egress interface only

huashan22# **pathtrace fcid 0xca016c vsan 2000 domain**

The final destination port type is F_Port

```

-----
Hop 0      Domain In-Port      Out-Port      Speed Cost  Switchname
          111    embedded    fc1/6        4G    250    huashan22
-----
Stats for egress port: fc1/6
  TxRt (B/s): 2952
  RxRt (B/s): 3648
  TxB_B: 32

```

```

    RxB_B: 32
    TxFrame: 137472
    RxFrame: 137480
    Errors: 0
    Discard: 0
    CRC: 0

```

```

-----
Hop 1      Domain In-Port      Out-Port      Speed Cost  Switchname
          202    fc1/6          fc1/1          2G   -    huashan21
-----

```

Stats for egress port: fc1/1

```

    TxRt(B/s): 1424
    RxRt(B/s): 1528
    TxB_B: 0
    RxB_B: 32
    TxFrame: 711
    RxFrame: 649
    Errors: 0
    Discard: 15
    CRC: 0

```

NOTE: The stats are displayed for the egress interface only

switch# **pathtrace d 202 v 2000**

The final destination port type is Embedded

```

-----
Hop Domain In-Port      Out-Port      Speed Cost  Switchname
-----
0   111    embedded          fc1/6          4G   250    huashan22
1   202    fc1/6              embedded        -     -     huashan21
-----

```

NOTE: The stats are displayed for the egress interface only

switch# **pathtrace domain 202 vsan 2000 detail**

The final destination port type is Embedded

```

-----
Hop 0      Domain In-Port      Out-Port      Speed Cost  Switchname
          111    embedded          fc1/6          4G   250    huashan22
-----

```

Stats for egress port: fc1/6

```

    TxRt(B/s): 2960
    RxRt(B/s): 3672
    TxB_B: 32
    RxB_B: 32
    TxFrame: 137508
    RxFrame: 137516
    Errors: 0
    Discard: 0
    CRC: 0

```

```

-----
Hop 1      Domain In-Port      Out-Port      Speed Cost  Switchname
          202    fc1/6              embedded        -     -     huashan21
-----

```

Stats for egress port: embedded

```

    TxRt(B/s): -
    RxRt(B/s): -
    TxB_B: -
    RxB_B: -
    TxFrame: -
    RxFrame: -

```

```

Errors: -
Discard: -
CRC: -

```

NOTE: The stats are displayed for the egress interface only

```
switch# pathtrace domain 202 vsan 2000 reverse
```

The final destination port type is Embedded

Hop	Domain	In-Port	Out-Port	Speed	Cost	Switchname
0	111	embedded	fc1/6	4G	250	huashan22
1	202	fc1/6	embedded	-	-	huashan21
2	202	embedded	fc1/6	4G	250	huashan21
3	111	fc1/6	embedded	-	-	huashan22

NOTE: The stats are displayed for the egress interface only

```
switch# pathtrace domain 202 vsan 2000 reverse detail
```

The final destination port type is Embedded

Hop	Domain	In-Port	Out-Port	Speed	Cost	Switchname
0	111	embedded	fc1/6	4G	250	huashan22

Stats for egress port: fc1/6

```

TxRt (B/s): 2976
RxRt (B/s): 3696
Tx_B_B: 32
Rx_B_B: 32
TxFrame: 137510
RxFrame: 137518
Errors: 0
Discard: 0
CRC: 0

```

Hop	Domain	In-Port	Out-Port	Speed	Cost	Switchname
1	202	fc1/6	embedded	-	-	huashan21

Stats for egress port: embedded

```

TxRt (B/s): -
RxRt (B/s): -
Tx_B_B: -
Rx_B_B: -
TxFrame: -
RxFrame: -
Errors: -
Discard: -
CRC: -

```

Hop	Domain	In-Port	Out-Port	Speed	Cost	Switchname
2	202	embedded	fc1/6	4G	250	huashan21

Stats for egress port: fc1/6

```

TxRt (B/s): 3696
RxRt (B/s): 2976
Tx_B_B: 32
Rx_B_B: 32
TxFrame: 137519

```

```

RxFrame: 137510
Errors: 0
Discard: 0
CRC: 0

```

```

-----
Hop 3      Domain In-Port      Out-Port      Speed Cost  Switchname
          111      fc1/6      embedded      -    -    huashan22
-----

```

Stats for egress port: embedded

```

TxRt(B/s): -
RxRt(B/s): -
TxB_B: -
RxB_B: -
TxFrame: -
RxFrame: -
Errors: -
Discard: -
CRC: -

```

NOTE: The stats are displayed for the egress interface only

Related Commands

Command	Description
FCtrace	FCtrace is a utility which traces the path to a destination device. By displaying the switch's pwnn at every hop.

peer (DMM job configuration submode)

To add peer SSM information to a job, use the **peer** command in DMM job configuration submode. To remove the peer SSM information from a job, use the **no** form of the command.

peer *ip-address*

no peer *ip-address*

Syntax Description	<i>ip-address</i>	Specifies the peer SSM IP address. The format for the IP address is <i>A.B.C.D</i> .
--------------------	-------------------	--

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

Command Modes	DMM job configuration submode.
---------------	--------------------------------

Command History	Release	Modification
	3.2(1)	This command was introduced.

Usage Guidelines	In a dual-fabric topology, the migration job runs on an SSM in each fabric. The two SSMs exchange messages over the management IP network, so each SSM needs the IP address of the peer.
------------------	--

Examples	The following example shows how to add peer SSM information to a job:
----------	---

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# dmm module 3 job 1 create
Started New DMM Job Configuration.
Do not exit sub-mode until configuration is complete and committed
switch(config-dmm-job)# peer 224.2.1.2
switch(config-dmm-job)#
```

Related Commands	Command	Description
	show dmm ip-peer	Displays the IP peer of a DMM port.
	show dmm job	Displays job information.

peer-info ipaddr

To configure the peer information for the FCIP interface, use the **peer-info ipaddr** command. To remove the peer information for the FCIP interface, use the **no** form of the command.

peer-info ipaddr *address* [*port number*]

no peer-info ipaddr *address* [*port number*]

Syntax Description	ipaddr <i>address</i>	Configures the peer IP address.
	port <i>number</i>	Configures a peer port. The range is 1 to 65535.

Defaults None.

Command Modes Interface configuration submode.

Command History	Release	Modification
	1.1(1)	This command was introduced.

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

The basic FCIP configuration uses the peer's IP address to configure the peer information. You can also use the peer's port number, port profile ID, or port WWN to configure the peer information. If you do not specify a port, the default 3225 port number is used to establish connection.

Examples The following command assigns an IP address to configure the peer information. Since no port is specified, the default port number, 3225, is used:

```
switch# config terminal
switch(config)# interface fcip 10
switch(config-if)# peer-info ipaddr 209.165.200.226
```

The following command deletes the assigned peer port information:

```
switch(config-if)# no peer-info ipaddr 209.165.200.226
```

The following command assigns the IP address and sets the peer TCP port to 3000. The valid port number range is from 0 to 65535:

```
switch(config-if)# peer-info ipaddr 209.165.200.226 port 3000
```

The following command deletes the assigned peer port information:

```
switch(config-if)# no peer-info ipaddr 209.165.200.226 port 2000
```

Related Commands

Command	Description
show interface fcip	Displays an interface configuration for a specified FCIP interface.

periodic-inventory notification

To enable the periodic inventory notification message dispatches, use the **periodic-inventory notification** command in Call Home configuration submode. To revert to the default state, use the **no** form of the command.

periodic-inventory notification [*interval days*]

no periodic-inventory notification

Syntax Description	interval days (Optional) Specifies the notification interval. The range is 1 to 30.	
Defaults	Disabled. The initial default interval is 7 days.	
Command Modes	Call Home configuration submode.	
Command History	Release	Modification
	2.0(x)	This command was introduced.
Usage Guidelines	None.	
Examples	The following example shows how to enable periodic inventory notification and use the default interval: switch# config terminal switch(config)# callhome switch(config-callhome)# periodic-inventory notification	
	The following example shows how to enable periodic inventory notification and set the interval to 10 days: switch# config terminal switch(config)# callhome switch(config-callhome)# periodic-inventory notification interval 10	
Related Commands	Command	Description
	callhome	Enters Call Home configuration submode.
	show callhome	Displays Call Home configuration information.

permit (IPv6-ACL configuration)

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

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

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

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

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

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

Syntax Description

<i>ipv6-protocol-number</i>	Specifies an IPv6 protocol number. The range is 0 to 255.
ipv6	Applies the ACL to any IPv6 packet.
<i>source-ipv6-prefix/prefix-length</i>	Specifies a source IPv6 network or class of networks. The format is <i>X:X:X::X/n</i> .
any	Applies the ACL to any source or destination prefix.
host <i>source-ipv6-address</i>	Applies the ACL to the specified source IPv6 host address. The format is <i>X:X:X::X</i> .
<i>dest-ipv6-prefix/prefix-length</i>	Specifies a destination IPv6 network or class of networks. The format is <i>X:X:X::X/n</i> .
host <i>dest-ipv6-address</i>	Applies the ACL to the specified destination IPv6 host address. The format is <i>X:X:X::X</i> .
log-deny	(Optional) For packets that are dropped, creates an informational log message about the packet that matches the entry. The message includes the input interface.
icmp	Applies the ACL to any Internet Control Message Protocol (ICMP) packet.
<i>icmp-type</i>	Specifies an ICMP message type. The range is 0 to 255.
<i>icmp-code</i>	Specifies an ICMP message code. The range is 0 255.
tcp	Applies the ACL to any TCP packet.
<i>source-port-operator</i>	Specifies an operand that compares the source ports of the specified protocol. The operands are lt (less than), gt (greater than), and eq (equals).
<i>source-port-number</i>	Specifies the port number of a TCP or UDP port. The number can be from 0 to 65535. A range requires two port numbers.
udp	Applies the ACL to any UDP packet.

<i>dest-port-operator</i>	Specifies an operand that compares the destination ports of the specified protocol. The operands are lt (less than), gt (greater than), and eq (equals).
<i>dest-port-operator</i>	Specifies the port number of a TCP or UDP port. The number can be from 0 to 65535. A range requires two port numbers.
range	Specifies a range of ports to compare for the specified protocol.
established	(Optional) Indicates an established connection, which is defined as a packet whose SYN flag is not set.

Defaults

None.

Command Modes

IPv6-ACL configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

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

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



Caution

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

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

Examples

The following example configures an IPv6-ACL called List, enters IPv6-ACL submode, and adds an entry that permits IPv6 traffic from any source address to any destination address:

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

The following example removes a permit condition set for any destination prefix on a specified UDP host:

```
switch# config terminal
switch(config)# ipv6 access-list List1
```

```
switch(config-ipv6-acl)# no permit udp host 2001:db8:200d::4000 any
```

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

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

Related Commands

Command	Description
ipv6 access-list	Configures an IPv6 ACL and enters IPv6-ACL configuration submode.
deny	Configures deny conditions for an IPv6 ACL.

phone-contact

To configure the telephone contact number with the Call Home function, use the **phone-contact** command in Call Home configuration submode. To disable this feature, use the **no** form of the command.

phone-contact [*number*]

no phone-contact [*number*]

Syntax Description

number (Optional) Configures the customer's phone number. Allows up to 17 alphanumeric characters in international phone format.

Note Do not use spaces. Use the + prefix before the number.

Defaults

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the telephone contact number with the Call Home function:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# phone-contact +1-800-123-4567
```

Related Commands

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

ping

To diagnose basic network connectivity, use the **ping** command in EXEC mode.

ping [**ipv6**] [{*host-name* | *ip-address*} [**count** *repeat-count*] [**interface** {**gigabitethernet** *slot/port* | **mgmt** *number* | **port-channel** *number* | **vsan** *vsan-id*}] [**size** *size* [**timeout** *timeout*]]

Syntax Description

ipv6	Sends IPv6 echo messages.
host-name	Specifies the host name of system to ping. Maximum length is 64 characters.
ip-address	Specifies the address of the system to ping.
count <i>repeat-count</i>	Specifies the repeat count. The range is 0 to 64.
interface	Specifies the interface on which the ping packets are to be sent.
gigabitethernet <i>slot/port</i>	Specifies a Gigabit Ethernet slot and port number.
mgmt <i>number</i>	Specifies the management interface.
port-channel <i>number</i>	Specifies a PortChannel number. The range is 1 to 256.
vsan <i>vsan-id</i>	Specifies a VSAN ID. The range is 1 to 4093.
size <i>size</i>	Specifies the size. The range is 10 to 2000.
timeout <i>timeout</i>	Specifies the timeout. The range is 1 to 10.

Defaults

Prompts for input fields.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Added the ipv6 argument.

Usage Guidelines

The ping (Packet Internet Groper) program sends an echo request packet to an address, and then awaits a reply. The ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

Verify connectivity to the TFTP server using the **ping** command.

To abnormally terminate a ping session, type the **Ctrl-C** escape sequence.

Examples

The following example pings the system 192.168.7.27:

```
switch# ping 192.168.7.27
PING 192.168.7.27 (192.168.7.27): 56 data bytes
64 bytes from 192.168.7.27: icmp_seq=0 ttl=255 time=0.4 ms
64 bytes from 192.168.7.27: icmp_seq=1 ttl=255 time=0.2 ms
```

```
64 bytes from 192.168.7.27: icmp_seq=2 ttl=255 time=0.2 ms
64 bytes from 192.168.7.27: icmp_seq=3 ttl=255 time=0.2 ms
```

```
--- 209.165.200.226 ping statistics ---
13 packets transmitted, 13 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.4 ms
```

The following command shows the prompts that appear when you enter the **ping** command without an IP address:

```
switch# ping
Target IP address: 209.165.200.226
Repeat count [5]: 4
Datagram size [100]: 5
Timeout in seconds [2]: 1
Extended commands [n]: 3
PING 209.165.200.226 (209.165.200.226) 5(33) bytes of data.

--- 209.165.200.226 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3017ms
```

policy

To enter IKE policy configuration and configure a policy for the IKE protocol, use the **policy** command in IKE configuration submode. To delete the policy, use the **no** form of the command.

policy *priority*

no policy *priority*

Syntax Description	<i>priority</i>	Specifies the priority for the IKE policy. The range is 1 to 255, where 1 is the high priority and 255 is the lowest.
--------------------	-----------------	---

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

Command Modes	IKE configuration submode.
---------------	----------------------------

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

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

Examples	The following example shows how to configure a policy priority number for the IKE protocol:
----------	---

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

Related Commands	Command	Description
	crypto ike domain ipsec	Enters IKE configuration mode.
	crypto ike enable	Enables the IKE protocol.
	show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

port

To assign the TCP port number of a Gigabit Ethernet interface to the FCIP profile or a listener peer port for a iSCSI interface, use the **port** command. Use the **no** form of the command to negate the command or revert to factory defaults.

port *number*

no port *number*

Syntax Description	port <i>number</i> Configures a peer port. The range is 1 to 65535.									
Defaults	Disabled									
Command Modes	Fcip profile configuration submode. Interface configuration submode.									
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>1.1(1)</td><td>This command was introduced.</td></tr></table>		Release	Modification	1.1(1)	This command was introduced.				
Release	Modification									
1.1(1)	This command was introduced.									
Usage Guidelines	Associates the profile with the assigned local port number. If a port number is not assigned for a FCIP profile, the default TCP port 3225 is used.									
Examples	The following example configures port 5000 on FCIP interface 5: <pre>switch# config terminal switch(config)# fcip profile 5 switch(config-profile)# port 5000</pre> The following example configures port 4000 on iSCSI interface 2/1: <pre>switch# config terminal switch(config)# interface iscsi 2/1 switch(config-profile)# port 4000</pre>									
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td>show fcip profile</td><td>Displays information about the FCIP profile.</td></tr><tr><td>interface fcip <i>interface_number</i> use-profile profile-id</td><td>Configures the interface using an existing profile ID from 1 to 255.</td></tr><tr><td>show interface fcip</td><td>Displays an interface configuration for a specified FCIP interface.</td></tr></table>		Command	Description	show fcip profile	Displays information about the FCIP profile.	interface fcip <i>interface_number</i> use-profile profile-id	Configures the interface using an existing profile ID from 1 to 255.	show interface fcip	Displays an interface configuration for a specified FCIP interface.
Command	Description									
show fcip profile	Displays information about the FCIP profile.									
interface fcip <i>interface_number</i> use-profile profile-id	Configures the interface using an existing profile ID from 1 to 255.									
show interface fcip	Displays an interface configuration for a specified FCIP interface.									

port-channel persistent

To convert an automatically created PortChannel to a persistent PortChannel, use the **port-channel persistent** command in EXEC mode.

port-channel *port-channel number* **persistent**

Syntax Description	<i>port-channel number</i> Specifies the PortChannel number. The range is 1 to 256.
---------------------------	---

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

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

Command History	Release	Modification
	NX-OS 4.1(3)	Added usage guideline.
	2.0(x)	This command was introduced.

Usage Guidelines	The auto mode support is not available after 4.x. Any previously automatically created PortChannel needs to be made persistent by using the port-channel persistent command. This command needs to be run on both sides of the auto Port Channel.
-------------------------	--

Examples	The following example shows how to change the properties of an automatically created channel group to a persistent channel group: switch# port-channel 10 persistent
-----------------	--

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

port-group-monitor enable

To enable the Port Group Monitor feature, use the **port-group-monitor enable** command. To disable this feature, use the **no** form of the command.

port-group-monitor enable

no port-group-monitor enable

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

Defaults	Enable.
-----------------	---------

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

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

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

Examples	The following example shows how to enable Port Group Monitor:
-----------------	---

```
switch(config)# port-group-monitor enable
switch(config)#
```

The following example shows how to disable Port Group Monitor:

```
switch(config)# no port-group-monitor enable
switch(config)#
```

Related Commands	Command	Description
	show port-group-monitor	Displays Port Group Monitor information.

port-group-monitor activate

To activate the specified Port Group Monitor policy, use the **port-group-monitor activate** command. To deactivate the Port Group Monitor policy, use the **no** form of the command.

port-group-monitor activate {*name*}

no port-group-monitor activate {*name*}

Syntax Description	<i>name</i>
	(Optional) Specifies the name of the port group policy. The maximum size is 32 characters.

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

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

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

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

Examples The following example shows how to activate the Port Group Monitor policy:

```
switch(config)# port-group-monitor activate pgmon
switch(config)#
```

The following example shows how to deactivate the Port Group Monitor policy:

```
switch(config)# no port-group-monitor activate pgmon
switch(config)#
```

Related Commands	Command	Description
	show port-group-monitor	Displays Port Group Monitor information.

port-group-monitor name

To create the Port Group Monitor policy, use the **port-group-monitor name** command. To delete Port Group Monitor policy, use the **no** form of the command.

port-group-monitor name {*policy-name*}

no port-group-monitor name {*policy-name*}

Syntax Description	<i>policy-name</i> (Optional) Displays the policy name. Maximum size is 32 characters.
---------------------------	--

Defaults	Rising threshold is 80, falling threshold is 20, and interval is 60.
-----------------	--

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

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

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

Examples	The following example shows how to create Port Group Monitor policy name:
-----------------	---

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-group-monitor name pgmon
switch(config-port-group-monitor)#
```

The following example shows how to delete Port Group Monitor policy:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# no port-group-monitor name pgmon
switch(config-port-group-monitor)#
```

Related Commands	Command	Description
	port-group-monitor activate	Configures the specified Port Group Monitor policy
	monitor counter	Configure monitoring of a specific counter within a Port Group Monitor policy.
	counter	Configure individual counter in a port-monitor policy to use non-default values.
	show port-group-monitor	Displays Port Group Monitor information.

port-license

To make a port eligible or ineligible to acquire a port activation license on a Cisco MDS 9124 switch, use the **port-license** command.

port-license acquire

no port-license acquire

Syntax Description	acquire	Grants a license to a port.
--------------------	---------	-----------------------------

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

Command Modes	Interface configuration submode.
---------------	----------------------------------

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

Usage Guidelines	If a port already has a license, then no action is taken and the port-license command returns successfully. If a license is unavailable, then the port will remain unlicensed.
------------------	---



Note

This command is supported on the Cisco MDS 9124 switch only.

Examples	The following example shows how to make a port eligible to acquire a license:
----------	---

```
switch# config t
switch (config)# interface fc1/1
switch (config-if)# port-license
```

The following example shows how to acquire a license for a port, and then copies the configuration to the startup configuration so that the new licensing configuration is maintained:

```
switch# config t
switch(config)# interface fc1/1
switch(config-if)#
switch(config-if)# port-license acquire
switch(config-if)# end
switch# copy running-config startup-config
```

Related Commands	Command	Description
	show port-licenses	Displays port licensing information for a Cisco MDS 9124 switch.

port-monitor activate

To activate the specified port monitor policy, use **port-monitor activate** command. To deactivate the policy, use the **no** form of the command.

port-monitor activate [*name*]

no port-monitor activate [*name*]

Syntax Description	<i>name</i> (Optional) Name of RMON port policy.	
Defaults	None.	
Command Modes	Configuration mode.	
Command History	Release	Modification
	4.1(1b)	This command was introduced.
Usage Guidelines	If no name is given, the port monitor activates the default policy. Presently one policy is activated on one port type. Two policies can be active but on different port types. If the specified policy is not active, it is a redundant operation.	
Examples	The following example shows how to activate the port monitor default policy: <pre>switch(config)# port-monitor activate switch(config)#</pre>	
	The following example shows how to activate the port monitor Cisco policy: <pre>switch(config)# port-monitor activate Cisco switch(config)#</pre>	
Related Commands	Command	Description
	show port-monitor	Displays all port monitor policies.

port-monitor enable

To enable the user to activate or deactivate policies, use the **port-monitor enable** command. To disable port monitor policies, use the **no** form of the command.

port-monitor enable

no port-monitor enable

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

Defaults	Enabled.
-----------------	----------

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

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

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

Examples	The following example shows how to enable port monitor:
-----------------	---

```
switch(config)# port-monitor enable
switch(config)# no port-monitor enable
```

Related Commands	Command	Description
	show port-monitor	Displays all port monitor policies.

port-monitor name

To configure a new port monitor policy and enters port monitor configuration mode, use the **port-monitor name** command. To delete port monitor policy, use the **no** form of the command.

port-monitor name [*string*]

no port-monitor name [*string*]

Syntax Description

string (Optional) Displays the policy name.

Defaults

By default 13 individual counters are added and it defaults to port-type all.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

To enable the monitoring of various counters the following basic steps need to be done:

- Configure the port-monitor policy name
- Configure the types of ports included in the policy
- Configure any counters with non-default values that are needed
- Turn off the monitoring of any counters that are not needed (and are on by default) and turn on the monitoring of any counters that are needed if they are by default turned off
- Activate port-monitor policy

Examples

The following example shows how to create a cisco policy name and to assign the default value:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-monitor name cisco
switch(config-port-monitor)# do show port-monitor cisco

Policy Name   : cisco
Admin status  : Not Active
Oper status   : Not Active
Port type     : All Ports
Admin status  : Not Active
Oper status   : Not Active
Port type     : All Ports
-----
Counter      Threshold Interval Rising Threshold event Falling Threshold
event PMON Portguard
```

port-monitor name

Link Loss		Delta	60	5	4	1
4	Not enabled					
Sync Loss		Delta	60	5	4	1
4	Not enabled					
Signal Loss		Delta	60	5	4	1
4	Not enabled					
Invalid Words		Delta	60	1	4	0
4	Not enabled					
Invalid CRC's		Delta	60	5	4	1
4	Not enabled					
TX Discards		Delta	60	200	4	10
4	Not enabled					
LR RX		Delta	60	5	4	1
4	Not enabled					
LR TX		Delta	60	5	4	1
4	Not enabled					
Timeout Discards		Delta	60	200	4	10
4	Not enabled					
Credit Loss Reco		Delta	1	1	4	0
4	Not enabled					
TX Credit Not Available		Delta	1	10	4	0
4	Not enabled					
RX Datarate		Delta	60	80%	4	20%
4	Not enabled					
TX Datarate		Delta	60	80%	4	20%
4	Not enabled					

Related Commands

Command	Description
counter	Displays the individual counter.
monitor-counter	Configure the monitoring of a specific counter within a port-monitor policy.
port-monitor activate	Configures the specified port monitor policy.
port-type	Configures port type policies.
show port-monitor	Displays all port monitor policies.

port-security

To configure port security features and reject intrusion attempts, use the **port-security** command in configuration mode. Use the **no** form of the command to negate the command or revert to factory defaults.

port-security

```
{activate vsan vsan-id [force | no-auto-learn] | auto-learn vsan vsan-id | database vsan
vsan-id {any-wwn | pwwn wwn | nwwn wwn | swwn wwn} [fwwn wwn | interface {fc slot/port
| port-channel number} | swwn wwn [interface {fc slot/port | port-channel number}][]}
```

```
no port-security {activate vsan vsan-id [force | no-auto-learn] | auto-learn vsan vsan-id |
database vsan vsan-id {any-wwn | pwwn wwn | nwwn wwn | swwn wwn} [fwwn wwn |
interface {fc slot/port | port-channel number} | swwn wwn [interface {fc slot/port |
port-channel number}][]}
```

Syntax Description

activate	Activates a port security database for the specified VSAN and automatically enables auto-learn.
vsan <i>vsan-id</i>	Specifies the VSAN ID. The range is 1 to 4093.
force	(Optional) Forces the database activation.
no-auto-learn	(Optional) Disables the autolearn feature for the port security database.
auto-learn	Enables auto-learning for the specified VSAN.
database	Enters the port security database configuration mode for the specified VSAN.
any-wwn	Specifies any WWN to login to the switch.
nwwn <i>wwn</i>	Specifies the node WWN as the Nx port connection.
pwwn <i>wwn</i>	Specifies the port WWN as the Nx port connection.
swwn <i>wwn</i>	Specifies the switch WWN as the xE port connection.
fwwn <i>wwn</i>	Specifies a fabric WWN login.
interface	Specifies the device or switch port interface through which each device is connected to the switch.
fc <i>slot/port</i>	Specifies a Fibre Channel interface by the slot and port.
port-channel <i>number</i>	Specifies a PortChannel interface. The range is 1 to 128.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(1)	This command was introduced.
2.0(x)	Add the optional swwn keyword to the subcommands under the port-security database vsan command.

Usage Guidelines

When you activate the port security feature, the **auto-learn** option is also automatically enabled. You can choose to activate the port-security feature and disable autolearn using the **port-security activate vsan number no-auto-learn** command. In this case, you need to manually populate the port security database by individually securing each port.

If the **auto-learn** option is enabled on a VSAN, you cannot activate the database for that VSAN without the **force** option.

Examples

The following example activates the port security database for the specified VSAN, and automatically enables autolearning:

```
switch# config terminal
switch(config)# port-security activate vsan 1
```

The following example deactivates the port security database for the specified VSAN, and automatically disables auto-learn:

```
switch# config terminal
switch(config)# no port-security activate vsan 1
```

The following example disables the auto-learn feature for the port security database in VSAN 1:

```
switch# config terminal
switch(config)# port-security activate vsan 1 no-auto-learn
```

The following example enables auto-learning so the switch can learn about any device that is allowed to access VSAN 1. These devices are logged in the port security active database:

```
switch# config terminal
switch(config)# port-security auto-learn vsan 1
```

The following example disables auto-learning and stops the switch from learning about new devices accessing the switch. Enforces the database contents based on the devices learnt up to this point.

```
switch# config terminal
switch(config)# no port-security auto-learn vsan 1
```

The following example enters the port security database mode for the specified VSAN:

```
switch# config terminal
switch(config)# port-security database vsan 1
switch(config-port-security)#
```

The following example configures any WWN to login through the specified interfaces:

```
switch(config-port-security)# any-wwn interface fc1/1 - fc1/8
```

The following example configures the specified pWWN to only log in through the specified fWWN.

```
switch(config-port-security)# pwwn 20:11:00:33:11:00:2a:4a fwwn 20:81:00:44:22:00:4a:9e
```

The following example deletes the specified pWWN configured in the previous step:

```
switch(config-port-security)# no pwwn 20:11:00:33:11:00:2a:4a fwwn
20:81:00:44:22:00:4a:9e
```

The following example configures the specified pWWN to only log in through the specified sWWN:

```
switch(config-port-security)# pwwn 20:11:00:33:11:00:2a:4a swwn 20:00:00:0c:85:90:3e:80
```

The following example deletes the specified pWWN configured in the previous step:

```
switch(config-port-security)# no pwn 20:11:00:33:11:00:2a:4a swn
20:00:00:0c:85:90:3e:80
```

The following example configures the specified nWWN to log in through the specified fWWN:

```
switch(config-port-security)# nwn 26:33:22:00:55:05:3d:4c fwn 20:81:00:44:22:00:4a:9e
```

The following example configures the specified pWWN to login through any port on the local switch:

```
switch(config-port-security)# pwn 20:11:33:11:00:2a:4a:66
```

The following example configures the specified sWWN to only login through PortChannel 5:

```
switch(config-port-security)# swn 20:01:33:11:00:2a:4a:66 interface port-channel 5
```

The following example configures any WWN to log in through the specified interface:

```
switch(config-port-security)# any-wn interface fc3/1
```

The following example deletes the wildcard configured in the previous step:

```
switch(config-port-security)# no any-wn interface fc2/1
```

The following example deletes the port security configuration database from the specified VSAN:

```
switch# config terminal
switch(config)# no port-security database vsan 1
switch(config)#
```

The following example forces the VSAN 1 port security database to activate despite conflicts:

```
switch(config)# port-security activate vsan 1 force
```

Related Commands

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

port-security abort

To discard the port security Cisco Fabric Services (CFS) distribution session in progress, use the **port-security abort** command in configuration mode.

port-security abort vsan *vsan-id*

Syntax Description

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

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to discard a port security CFS distribution session in progress:

```
switch# config terminal
switch(config)# port-security abort vsan 33
```

Related Commands

Command	Description
port-security distribute	Enables CFS distribution for port security.
show port-security	Displays port security information.

port-security commit

To apply the pending configuration pertaining to the port security Cisco Fabric Services (CFS) distribution session in progress in the fabric, use the **port-security commit** command in configuration mode.

port-security commit vsan *vsan-id*

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

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

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

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

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

Examples	The following example shows how to commit changes to the active port security configuration:
----------	--

```
switch# config terminal  
switch(config)# port-security commit vsan 13
```

Related Commands	Command	Description
	port-security distribute	Enables CFS distribution for port security.
	show port-security	Displays port security information.

port-security database

To copy the port security database or to view the difference within the port security database, use the **port-security database** command in EXEC mode.

port-security database {copy | diff {active | config}} vsan *vsan-id*

Syntax Description

copy	Copies the active database to the configuration database.
diff	Provides the difference between the active and configuration port security database.
active	Writes the active database to the configuration database.
config	Writes the configuration database to the active database.
vsan <i>vsan-id</i>	Specifies the VSAN ID. The ranges is 1 to 4093.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

If the active database is empty, the port-security database is empty.

Use the **port-security database diff active** command to resolve conflicts.

Examples

The following example copies the active to the configured database:

```
switch# port-security database copy vsan 1
```

The following example provides the differences between the active database and the configuration database:

```
switch# port-security database diff active vsan 1
```

The following example provides information on the differences between the configuration database and the active database:

```
switch# port-security database diff config vsan 1
```

Related Commands	Command	Description
	port-security database	Copies and provides information on the differences within the port security database.
	show port-security database	Displays configured port security information.

port-security distribute

To enable Cisco Fabric Services (CFS) distribution for port security, use the **port-security distribute** command. To disable this feature, use the **no** form of the command.

port-security distribute

no port-security distribute

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

Defaults	Disabled.
-----------------	-----------

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

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

Usage Guidelines	Before distributing the Fibre Channel timer changes to the fabric, the temporary changes to the configuration must be committed to the active configuration using the port-security commit command.
-------------------------	--

Examples	The following example shows how to distribute the port security configuration to the fabric:
-----------------	--

```
switch# config terminal
switch(config)# port-security distribute
```

Related Commands	Command	Description
	port-security commit	Commits the port security configuration changes to the active configuration.
	show port-security	Displays port security information.

port-security enable

To enable port security, use the **port-security enable** command in **configuration mode**. To disable port security, use the **no** form of the command.

port-security enable

no port-security enable

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

Defaults	Disabled.
-----------------	-----------

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

Command History	Release	Modification
	2.0(x)	This command was introduced.
	NX-OS 4.1(1b)	This command was deprecated.

Usage Guidelines	Issuing the port-security enable command enables the other commands used to configure port security.
-------------------------	---

Examples	The following example shows how to enable port security:
-----------------	--

```
switch# config terminal
switch(config)# port-security enable
```

The following example shows how to disable port security:

```
switch# config terminal
switch(config)# no port-security enable
```

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

port-track enable

To enable port tracking for indirect errors, use the **port-track enable** command in configuration mode. To disable this feature, use the **no** form of the command.

port-track enable

no port-track enable

Syntax Description This command has no other arguments or keywords.

Defaults Disabled.

Command Modes Configuration mode.

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

Usage Guidelines The software brings the linked port down when the tracked port goes down. When the tracked port recovers from the failure and comes back up again, the tracked port is also brought up automatically (unless otherwise configured).

Examples The following example shows how to enable port tracking:

```
switch# config terminal
switch(config)# port-track enable
```

The following example shows how to disable port tracking:

```
switch# config terminal
switch(config)# no port-track enable
```

Related Commands	Command	Description
	show interface fc	Displays configuration and status information for a specified Fibre Channel interface.
	show interface port-channel	Displays configuration and status information for a specified PortChannel interface.

port-track force-shut

To force a shutdown of a tracked port, use the **port-track force-shut** command in interface configuration submode. To reenable the port tracking, use the **no** form of the command.

port-track force-shut

no port-track force-shut

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

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

Command Modes	Interface configuration submode.
----------------------	----------------------------------

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

Usage Guidelines	Use the port-track force-shut to keep the linked port down, even though the tracked port comes back up. You must explicitly bring the port up when required using the no port-track force-shut command.
-------------------------	---

Examples	The following example shows how to force the shutdown of an interface and the interfaces that it is tracking:
-----------------	---

```
switch# config terminal
switch(config)# interface fc 1/2
switch(config-if)# no port-track force-shut
```

Related Commands	Command	Description
	port-track enable	Enables port tracking.
	show interface fc	Displays configuration and status information for a specified Fibre Channel interface.
	show interface port-channel	Displays configuration and status information for a specified PortChannel interface.

port-track interface

To enable port tracking for specific interfaces, use the **port-track interface** command in **interface configuration submode**. To disable this feature, use the **no** form of the command.

port-track interface { **fc** *slot/port* | **fcip** *port* | **gigabitethernet** *slot/port* | **port-channel** *port* }
[**vsan** *vsan-id*]

no port-track interface { **fc** *slot/port* | **fcip** *port* | **gigabitethernet** *slot/port* | **port-channel** *port* }
[**vsan** *vsan-id*]

Syntax Description	fc <i>slot/port</i>	Specifies a Fibre Channel interface.
	fcip <i>port</i>	Specifies a FCIP interface.
	gigabitethernet <i>slot/port</i>	Specifies a Gigabit Ethernet interface.
	port-channel <i>port</i>	Specifies a PortChannel interface. The range is 1 to 128.
	vsan <i>vsan-id</i>	(Optional) Specifies a VSAN ID. The range is 1 to 4093.

Defaults None.

Command Modes Interface configuration submode.

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

Usage Guidelines When the ports that an interface is tracking goes down, the interface also goes down. When the tracked port comes backup, the linked interface also comes back up. Use the **port-track force-shut** command to keep the linked interface down.

Examples The following example shows how to enable port tracking for specific interfaces:

```
switch# config terminal
switch(config)# interface fc 1/2
switch(config-if)# port-track interface port-channel 2
switch(config-if)# port-track interface fcip 5
```

Related Commands	Command	Description
	port-track enable	Enables port tracking.
	port-track force-shut	Forcefully shuts an interface for port tracking.
	show interface fc	Displays configuration and status information for a specified Fibre Channel interface.
	show interface port-channel	Displays configuration and status information for a specified PortChannel interface.

port-type

To configure port type policies, use **port-type** command. To disable port type policies, use the **no** form of the command.

port-type {all | trunks | access-Ports}

no port-type {all | trunks | access-Ports}

Syntax Description

all	Configures both trunk ports and access ports.
trunks	Configures only trunk ports.
access ports	Configures only access ports.

Defaults

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

The default policy uses its own internal port type, which is the same as all ports.

Examples

The following example shows how to configure port monitoring for access ports:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-monitor name cisco
switch(config-port-monitor)# port-type access-port
trying to get name
name is cisco
sending port type access
switch(config-port-monitor)#
```

The following example shows how to configure port monitoring for all ports:

```
switch(config-port-monitor)# port-type all
trying to get name
name is cisco
sending port type all
switch(config-port-monitor)#
```

The following example shows how to configure port monitoring for trunk ports:

```
switch(config-port-monitor)# port-type trunks
trying to get name
name is cisco
sending port type trunks
switch(config-port-monitor)#
```

Related Commands

Command	Description
show port-monitor	Displays all port monitor policies.

portaddress

To enable the FICON feature in a specified VSAN, use the **ficon vsan** command in configuration mode. To disable the feature or to revert to factory defaults, use the **no** form of the command.

portaddress *portaddress* **block** *name string* **prohibit** **portaddress** *portaddress*

no **portaddress** *portaddress* **block** *name string* **prohibit** **portaddress** *portaddress*

Syntax Description

<i>portaddress</i>	Specifies the FICON port number for this interface. The range is 0 to 254.
block	Blocks a port address.
name <i>string</i>	Configures a name for the port address. Maximum length is 24 characters.
prohibit portaddress	Prohibits communication with a port address.

Defaults

None.

Command Modes

FICON configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The **shutdown/no shutdown** port state is independent of the **block/no block** port state. If a port is shutdown, unblocking that port will not initialize the port.

You cannot block or prohibit CUP port (0XFE).

If you prohibit ports, the specified ports are prevented from communicating with each other. Unimplemented ports are always prohibited.

Examples

The following example disables a port address and retains it in the operationally down state:

```
switch# config terminal
switch(config)# ficon vsan 2
switch(config-ficon)# portaddress 1
switch(config-ficon-portaddr)# block
```

The following example enables the selected port address and reverts to the factory default of the port address not being blocked:

```
switch(config-ficon-portaddr)# no block
```

The following example prohibits port address 1 in VSAN 2 from talking to ports 3:

```
switch(config-ficon-portaddr)# prohibit portaddress 3
```

The following example removes port address 5 from a previously-prohibited state:

```
switch(config-ficon-portaddr)# no prohibit portaddress 5
```

The following example assigns a name to the port address:

```
switch(config-ficon-portaddr)# name SampleName
```

The following example deletes a previously configured port address name:

```
switch(config-ficon-portaddr)# no name SampleName
```

Related Commands

Command	Description
show ficon	Displays configured FICON details.

power redundancy-mode

To configure the capacity of the power supplies on the Cisco MDS 9500 Family of switches, use the **power redundancy-mode** command in configuration mode. Use the **no** form of the command to negate the command or revert to factory defaults.

power redundancy-mode {combined [force] | redundant}

no power redundancy-mode {combined [force] | redundant}

Syntax Description

combined	Configures power supply redundancy mode as combined.
force	Forces combined mode without prompting.
redundant	Configures power supply redundancy mode as redundant.

Defaults

Redundant mode.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If power supplies with different capacities are installed in the switch, the total power available differs based on the configured mode:

- In **redundant** mode, the total power is the lesser of the two power supply capacities. This reserves enough power to keep the system powered on in case of a power supply failure. This is the recommended or default mode.
- In **combined** mode, the total power is twice the lesser of the two power supply capacities. In case of a power supply failure, the entire system could be shut down, depending on the power usage at that time.
- When a new power supply is installed, the switch automatically detects the power supply capacity. If the new power supply has a capacity that is lower than the current power usage in the switch and the power supplies are configured in **redundant** mode, the new power supply will be shut down.
- When you change the configuration from **combined** to **redundant** mode and the system detects a power supply that has a capacity lower than the current usage, the power supply is shut down. If both power supplies have a lower capacity than the current system usage, the configuration is not allowed.

Examples

The following examples demonstrate how the power supply redundancy mode could be set:

```
switch(config)# power redundancy-mode combined
WARNING: This mode can cause service disruptions in case of a power supply failure.
Proceed ? [y/n] y
switch(config)# power redundancy-mode redundant
```

Related Commands	Command	Description
	copy running-config startup-config	Copies all running configuration to the startup configuration.
	show environment power	Displays status of power supply modules, power supply redundancy mode, and power usage summary.

poweroff module

To power off individual modules in the system, use the **poweroff module** command in configuration mode. Use the **no** form of this command to power up the specified module.

poweroff module *slot*

no poweroff module *slot*

Syntax Description	<i>slot</i> Specifies the slot number for the module.	
Defaults	None.	
Command Modes	Configuration mode.	
Command History	Release	Modification
	1.0(2)	This command was introduced.
Usage Guidelines	Use the poweroff module command to power off individual modules. The poweroff module command cannot be used to power off supervisor modules.	
Examples	The following example powers off and powers up module 1: switch# config terminal switch(config)# poweroff module 1 switch(config)# switch(config)# no poweroff module 1 switch(config)#	
Related Commands	Command	Description
	copy running-config startup-config	Copies all running configuration to the startup configuration.
	show module	Displays information for a specified module.

priority

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

priority { **high** | **low** | **medium** }

no priority { **high** | **low** | **medium** }

Syntax Description

high	Configures the frames matching the class-map as high priority.
low	Configures the frames matching the class-map as low priority.
medium	Configures the frames matching the class-map as medium priority.

Defaults

The default priority is low.

Command Modes

QoS policy map class configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Before you can configure the priority in a QoS policy map class you must first:

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

Examples

The following example shows how to select the QoS policy class-map1 and configure the frame priority as high:

```
switch(config-pmap) # class class-map1
switch(config-pmap-c) # priority high
Operation in progress. Please check class-map parameters
switch(config-pmap-c) #
```

Related Commands

Command	Description
class	Configure a QoS policy map class.
qos class-map	Configures a QoS class map.
qos enable	Enables the QoS data traffic feature on the switch.

Command	Description
qos policy-map	Configures a QoS policy map.
show qos	Displays the current QoS settings.

purge fcdomain fcid

To purge persistent FCIDs, use the **purge fcdomain fcid** command in EXEC mode.

purge fcdomain fcid vsan *vsan-id*

Syntax Description	vsan <i>vsan-id</i>	Indicates that FCIDs are to be purged for a VSAN ID. The range is 1 to 4093.
--------------------	----------------------------	--

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

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

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

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

Examples	The following example shows how to purge all dynamic unused FCIDs in VSAN 4: <pre>switch# purge fcdomain fcid vsan 4 switch#</pre> The following example shows how to purge all dynamic unused FCIDs in VSANs 4, 5, and 6: <pre>switch# purge fcdomain fcid vsan 3-5 switch#</pre>
----------	--

purge module

To delete configurations in the running configuration for nonexistent modules, use the **purge module** command in EXEC mode.

purge module *slot* **running-config**

Syntax Description

<i>slot</i>	Specifies the module slot number.
running-config	Purges the running configuration from the specified module.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command cannot be issued on a supervisor module.

Examples

The following example displays the output of the **purge module** command issued on the module in slot 8:

```
switch# purge module 8 running-config
switch#
```

pwc

To view your present working context (PWC), use the **pwc** command in any mode.

pwc

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

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

Command Modes	All.
----------------------	------

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

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

Examples	The following example shows the present working context:
-----------------	--

```
switch# config t
switch(config)# islb initiator ip-address 120.10.10.2
switch(config-islb-init)# pwc
(config t) -> (islb initiator ip-address 120.10.10.2)
```

Related Commands	Command	Description
	pwd	Displays the current directory location.

pwd

To display the current directory location, use the **pwd** command in EXEC mode.

pwd

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

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

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

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

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

Examples	The following example changes the directory and displays the current directory:
-----------------	---

```
switch# cd bootflash:logs
switch# pwd
bootflash:/logs
```

Related Commands	Command	Description
	cd	Changes the current directory to the specified directory.
	dir	Displays the contents of a directory.

pwwn (DPVM database configuration submode)

To add a device to a dynamic port VSAN membership (DPVM) database using the pWWN, use the **pwwn** command in DPVM database configuration submode. To remove a device from a DPVM database using the pWWN, use the **no** form of the command.

pwwn *pwwn-id* **vsan** *vsan-id*

no pwwn *pwwn-id* **vsan** *vsan-id*

Syntax Description	<i>pwwn-id</i>	Specifies the port WWN ID. The format is <i>hh:hh:hh:hh:hh:hh:hh</i> , where <i>h</i> is a hexadecimal number.
	vsan <i>vsan-id</i>	Specifies the VSAN ID. The range is 1 to 4093.

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

Command Modes	DPVM database configuration submode.
----------------------	--------------------------------------

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

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

Examples	The following example shows how to add an entry to the DPVM database:
-----------------	---

```
switch# config terminal
switch(config)# dpvm database
switch(config-dpvm-db)# pwwn 11:22:33:44:55:66:77:88 vsan 1
```

The following example shows how to delete an entry from the DPVM database:

```
switch(config-dpvm-db)# no pwwn 11:22:33:44:55:66:77:88 vsan 1
```

Related Commands	Command	Description
	dpvm database	Configures the DPVM database.
	show dpvm	Displays DPVM database information.

pwwn (fcdomain database configuration submode)

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

```
pwwn pwwn-id fc-id
```

```
no pwwn pwwn-id
```

Syntax Description	<i>pwwn-id</i>	Specifies the pWWN ID. The format is <i>hh:hh:hh:hh:hh:hh:hh:hh</i> , where <i>h</i> is a hexadecimal number.
	<i>fc-id</i>	Specifies the FC ID of the device.

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

Command Modes	fcdomain database configuration submode.
---------------	--

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

Usage Guidelines	Only one FC ID can be mapped to a pWWN.
------------------	---

Examples	The following example shows how to map the pWWN to the persistent FC ID:
----------	--

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# native-autonomous-fabric-num 20 native-vsan 30 domain 15
switch(config-fcdomain-fcid)# pwwn 11:22:33:44:55:66:77:88 0x123456
```

The following example shows how to remove the mapping between the pWWN and the FC ID:

```
switch# config t
switch(config)# ivr fcdomain database autonomous-fabric-num 10 vsan 20
switch(config-fcdomain)# native-autonomous-fabric-num 20 native-vsan 30 domain 15
switch(config-fcdomain-fcid)# no pwwn 11:22:33:44:55:66:77:88
```

Related Commands	Command	Description
	ivr fcdomain database autonomous-fabric-num	Creates IVR persistent FC IDs.
	native-autonomous-fabric-num	Creates an IVR persistent FC ID database entry.
	show ivr fcdomain database	Displays IVR fcdomain database entry information.

pwwn (SDV virtual device configuration submode)

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

pwwn *pwwn-name* [**primary**]

no pwwn *pwwn-name* [**primary**]

Syntax Description	<i>pwwn-name</i>	Specifies the pWWN of a real device. The format is <i>hh:hh:hh:hh:hh:hh:hh:hh</i> , where <i>h</i> is a hexadecimal number.
	primary	Configures the virtual device as a real device.

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

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

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

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

Examples	The following example shows how to add a pWWN to a virtual device:
	switch# config terminal
	Enter configuration commands, one per line. End with CNTL/Z.
	switch(config)# sdv virtual-device name sqa2 vsan 1 switch(config-sdv-virt-dev)# pwwn 21:00:00:04:cf:cf:45:40

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

