P Commands

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.

Command Default

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.

Command Default

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.

path

To add a sensor to a sensor group, use the **path** command. To remove the sensor, use the **no** form of this command.

path analytics: *query*
path transceiver: *range*
path transceiver_peer: *range*
path show_stats_ *range*

no path analytics: *query*
no path transceiver: *range*
no path transceiver_peer: *range*
no path show_stats_ *range*

Syntax Description

Table 1: Syntax Description

Sensor Name	Sensor Description	Parameter	Parameter Description
analytics	Data traffic analytics information.	*query*	A user defined analytics query name.
transceiver	Local transceiver diagnostic information.	*range*	A single FC interface or continuous range of FC interfaces separated by '-'.
transceiver_peer	Local and remote transceiver diagnostic information.	*range*	A single FC interface or continuous range of FC interfaces separated by '-'.
show_stats_*range*	Interface counter information. *range* is a single FC interface or a continuous range of FC interfaces separated by '-'.	Not applicable	No parameters.

Command Default

No sensor paths are configured.

Command Modes

Telemetry sensor configuration mode (conf-tm-sensor)

Command History

Release	Modification
9.2(2)	Added **transceiver** and **transceiver_peer** options.
8.3(1)	This command was introduced.

Usage Guidelines

The distinguished name of a sensor is followed by the parameters for the sensor. Not all sensors have parameters.

Multiple sensors may be added to a sensor group. This allows discontiguous interface ranges to be defined in a single sensor group.

When using the **transceiver_peer** sensor, ensure that the peer devices in the specified interface range support FC Read Diagnostic Parameters (RDP) ELS requests. RDP allows the switch to collect peer port diagnostic information over the link to the peer. To determine if a peer device supports RDP, execute the **show rdp fcid** *fcid* **vsan** *vsan* command. If an interface rejects the RDP ELS command, the interface will be marked as not supporting it and will not be sent the RDP ELS again until the next time the interface comes up. In this case the streamed data will not include the remote transceiver data.

Examples

This example shows how to add interface counters for fc3/1 to a sensor group:

```
switch# configure
switch(config)# telemetry
switch(config-telemetry)# sensor-group 1
switch(conf-tm-sensor)# path show_stats_fc3/1
```

This example shows how to remove an analytics query from a sensor group:

```
switch# configure
switch(config)# telemetry
switch(config-telemetry)# sensor-group 2
switch(conf-tm-sensor)# no path analytics:init
```

This example shows how to create a subscription that streams local transceiver data from Fibre Channel interface 1/1 through 1/5 every 10 minutes to IP 192.0.2.1 port 50003:

```
switch# configure
switch(config)# telemetry
switch(config-telemetry)# sensor-group 3
switch(conf-tm-sensor)# path transceiver:fc1/1-5
switch(conf-tm-sensor)# destination group 1
switch(conf-tm-dest)# ip address 192.0.2.1 port 50003 protocol gRPC encoding GPB-compact
subscription 1
switch(conf-tm-sub)# snr-grp 1 sample-interval 600000
switch(conf-tm-sub)# dst-grp 1
```

Related Commands

Command	Description
analytics query	Configure a user-defined analytics query.
feature analytics	Enable the SAN Analytics feature.
feature telemetry	Enables the SAN Telemetry Streaming feature.
sensor-group	Creates a sensor group and enters sensor group configuration.
show running-config telemetry	Displays the existing telemetry configuration.
show rdp	Displays RDP details of a device.
show telemetry	Displays telemetry runtime information.

Command	Description
telemetry	Enters SAN Telemetry Streaming configuration mode.

pathtrace

To display per-hop interface information along the paths between 2 devices, use the **pathtrace** command.

pathtrace {**domain** *id* | **fcid** *id*} **vsan** *id* [[**reverse**] [**detail**]]

pathtrace {**domain** *id* | **fcid** *id*} **vsan** *id* [[**reverse**] [**detail**] | [**multipath**]]

Syntax Description

domain *id*	Traces the paths to all the edge devices in the domain ID. The range is from 1 to 239.
fcid *id*	Specifies the Fibre Channel ID of the destination N-port. The range is from 0x0 to 0xffffff.
vsan *id*	Specified the VSAN ID. The range is from 1 to 4094.
reverse	(Optional) Displays information about the reverse (or return) path.
detail	(Optional) Displays detailed information about each egress interface at every hop.
multipath	(Optional) Displays information about all Equal-Cost Multipath (ECMP) links.

Command Default

None.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.3(1)	This command was modified. The **multipath** keyword was added.
6.2(5)	This command was introduced.

Usage Guidelines

- If the **pathtrace** command is executed in a path where devices do not support the Pathtrace feature, the pathtrace request packets are dropped and the command is not processed.
- The Pathtrace feature is supported only on Cisco MDS NX-OS Release 6.2(5) and later releases.
- The Pathtrace feature is not supported in Inter-VSAN Routing (IVR).

Depending on the keywords used, Pathtace displays the following information for every egress interface in a path:

Name	Description	Limitations
Speed/Spd	The operational speed of an active interface. It represents the capable bandwidth of an inactive interface.	Not displayed for internal interfaces.
TxRt/Tx	The bits transmitted per second.	Not displayed for internal interfaces.

Name	Description	Limitations
RxRt/Rx	The bits received per second.	Not displayed for internal interfaces.
TxFrame	The number of frames transmitted.	Not displayed for internal interfaces.
RxFrame	The number of frames received.	Not displayed for internal interfaces.
TxB_B/TxB2B	The transmit buffer-to-buffer credit that is remaining.	Not displayed for internal interfaces.
RxB_B/RxB2B	The receive buffer-to-buffer credit that is remaining.	Not displayed for internal interfaces.
Errors	The aggregate of ingress and egress errors.	Not displayed for internal interfaces.
Discard/Discards	The aggregate of ingress and egress frame discards.	Not displayed for internal interfaces.
CRC	The Cyclic Redundancy Check (CRC) errors on the incoming frames.	Not displayed for internal interfaces.
TxWait	An interface's total transmission waiting time due to nonavailability of transmit buffer-to-buffer credits.	Displays a percentage of transmit wait time for last 1 second, 1 minute, 1 hour, and last 72 hours.
ZoneDrops	The number of frames dropped due to access control list (ACL) rules.	Displays only for Cisco MDS 9700 48-Port 32-Gbps Fibre Channel Switching Module (DS-X9648-1536K9).
FibDrops	The number of frames dropped due to forwarding information base (FIB) rules.	Displays only for Cisco MDS 9700 48-Port 32-Gbps Fibre Channel Switching Module (DS-X9648-1536K9).

Examples

The following example shows how to trace the path between a switch in which the command is executed and an edge device, using the edge device's FCID:

```
switch# pathtrace fcid 0xca016c vsan 2000
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   switch1
1   202    fc1/6            fc1/1            2G    -     switch2
NOTE: The stats are displayed for the egress interface only
```

The following example shows how to trace both the forward path and the return path between a switch in which the command is executed and all the edge devices in domain 83 on the 'sw-fcip69' switch:

```
switch# pathtrace domain 83 vsan 70 reverse
The final destination port type is Embedded
-------------------------------------------------------------------------------
Hop Domain In-Port          Out-Port         Speed       Cost  Switchname
-------------------------------------------------------------------------------
0   144    embedded         vfc69(Eth1/8)    10.0G       100   sw-ioa-70
1   83     vfc69(Eth1/1)    embedded         -           -     sw-fcip69
2   83     embedded         vfc69(Eth1/1)    10.0G       100   sw-fcip69
3   144    vfc69(Eth1/8)    embedded         -           -     sw-ioa-70

NOTE: The stats are displayed for the egress interface only
```

The following example shows how to display detailed information about the interfaces (both the forward path and the return path) between a switch in which the command is executed and an edge device, using the edge device's FCID:

```
switch# pathtrace fcid 0xca016c vsan 2000 reverse detail
The final destination port type is F_Port
-------------------------------------------------------------------------------
Hop 0       Domain In-Port          Out-Port         Speed Cost  Switchname
            111    embedded         fc1/6            4G    250   switch1
-------------------------------------------------------------------------------
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    -     switch2
-------------------------------------------------------------------------------
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   switch2
-------------------------------------------------------------------------------
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         -     -     switch1
-------------------------------------------------------------------------------
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
```

The following example shows how to trace the path between a switch in which the **pathtrace** command is executed and all the edge devices in the specified domain and VSAN:

```
switch# pathtrace domain 83 vsan 70
The final destination port type is Embedded
-------------------------------------------------------------------------------
Hop Domain In-Port          Out-Port         Speed       Cost  Switchname
-------------------------------------------------------------------------
0   144    embedded         vfc69(Eth1/8)    10.0G       100   sw-ioa-70
1   83     vfc69(Eth1/1)    embedded         -           -     sw-fcip69

NOTE: The stats are displayed for the egress interface only
```

The following example shows how to trace all the links (including equal-cost parallel links) in the paths between all the edge devices in a domain and a switch in which the command is executed for Fibre Channel, FCIP, and vFC respectively:

```
switch# pathtrace domain 238 vsan 1 multipath
***NOTE ***
 I - Ingress
 E -  Egress
 M - Member Port-channel
 * - Fport
.................................................
PATH 1   switch1 switch2
Domain   236       235
.................................................
-------------------------------------------------------------------------------------------------------------------
HOP 1   switch1(fc1/11)(E)-------(I)(fc1/12)switch2
-------------------------------------------------------------------------------------------------------------------
Interface  Spd(G)  Tx(B/s)  Rx(B/s)  TxB2B  RxB2B  Errors  Discards   CRC
TxWait(1s/1m/1h/72h) FibDrops   ZoneDrops
-------------------------------------------------------------------------------------------------------------------
(E)fc1/11  8.0     84       44       64     64     0       2          0     0%/0%/0%/0%
        -          -
(I)fc1/12  8.0     44       84       64     64     0       0          0     0%/0%/0%/0%
        -          -
-------------------------------------------------------------------------------------------------------------------
HOP 2   switch2(fc1/3)(E)*End Device
-------------------------------------------------------------------------------------------------------------------
Interface   Spd(G)  Tx(B/s)  Rx(B/s)  TxB2B  RxB2B  Errors  Discards   CRC
```

```
TxWait(1s/1m/1h/72h) FibDrops    ZoneDrops
-------------------------------------------------------------------------------------------------------------
(E)fc1/3    4.0     0        0        16     64     0       0          0     0%/0%/0%/0%
        -           -
.............................................................................................................
PATH 2   switch1 switch2
Domain   236       235
.............................................................................................................
-------------------------------------------------------------------------------------------------------------
HOP 1   switch1(fc1/12)(E)-------(I)(fc1/11)switch2
-------------------------------------------------------------------------------------------------------------
Interface  Spd(G)  Tx(B/s)  Rx(B/s)   TxB2B   RxB2B  Errors  Discards  CRC
TxWait(1s/1m/1h/72h) FibDrops    ZoneDrops
-------------------------------------------------------------------------------------------------------------
(E)fc1/12  8.0     64       180       64      64     0       0         0     0%/0%/0%/0%
        -           -
(I)fc1/11  8.0     180      64        64      64     0       0         0     0%/0%/0%/0%
        -           -
-------------------------------------------------------------------------------------------------------------
HOP 2   switch2(fc1/3)(E)*End Device
-------------------------------------------------------------------------------------------------------------
Interface  Spd(G)  Tx(B/s)  Rx(B/s) TxB2B  RxB2B   Errors  Discards   CRC
TxWait(1s/1m/1h/72h) FibDrops     ZoneDrops
-------------------------------------------------------------------------------------------------------------
(E)fc1/3   4.0     0        0        16     64      0       0          0     0%/0%/0%/0%
        -             -

switch# pathtrace domain 132 vsan 447   multipath
***NOTE ***
I - Ingress
E -  Egress
M - Member Port-channel
* - Fport
................................................
PATH 1   switch1 switch2
Domain   187       132
................................................
-----------------------------------------------------------------------------------------------
HOP 1              switch1(port-channel216)(E)-------(I)(port-channel216)switch2
-----------------------------------------------------------------------------------------------
Interface          InputRate(B/s)     OutputRate(B/s)    InputFrames(/sec)
OutputFrames(/sec)
-----------------------------------------------------------------------------------------------
(E)port-channel216 3393959           640827945         161838662680576     1375239938244608

   (M)fcip50       292049             55048436           3239                27507

   (M)fcip51       291539             55052889           3237                27508

   (M)fcip52       291702             55080573           3239                27522

   (M)fcip53       278265             52552382           3090                26258

   (M)fcip54       278291             52561525           3090                26263

   (M)fcip55       278346             52559754           3090                26262

   (M)fcip65       291647             55073072           3238                27518

   (M)fcip66       278491             52584017           3092                26274

   (M)fcip67       278362             52571056           3091                26268

   (M)fcip86       278290             52554341           3090                26259
```

```
   (M)fcip87       278426             52587737          3092               26276

   (M)fcip88       278551             52602163          3093               26283

(I)port-channel216 640830213          3394016           1375252823146496   161842957647872

   (M)fcip50       55058685           292105            27512              3240

   (M)fcip51       55080107           291690            27522              3239

   (M)fcip52       55097520           291794            27530              3240

   (M)fcip53       52559881           278311            26262              3090

   (M)fcip54       52570959           278345            26268              3091

   (M)fcip55       52571081           278410            26268              3091

   (M)fcip65       55051714           291539            27507              3237

   (M)fcip66       52564219           278387            26264              3091

   (M)fcip67       52562847           278324            26264              3090

   (M)fcip86       52564931           278345            26265              3091

   (M)fcip87       52571632           278350            26268              3091

   (M)fcip88       52576637           278416            26271              3091
```

```
switch# pathtrace domain 83 vsan 70 multipath
***NOTE ***
I - Ingress
E -  Egress
M - Member Port-channel
* - Fport
................................................
PATH 1   switch1 switch2
Domain   144       83
................................................
-------------------------------------------------------------------------
HOP 1              switch1(vfc69)(E)-------(I)(vfc69)switch2
-------------------------------------------------------------------------------------------
Interface     Spd(G)  FcoeOut(Oct)       FcoeIn(Oct)        FcoeOutPkt         FcoeInPkt

-------------------------------------------------------------------------------------------
(E)vfc69      10.0    165604             153648             697                700


(I)vfc69      10.0    153716             166276             701                698
```

Note

- In the output, *embedded* indicates that the respective port is an HBA interface in an edge device.
- Some of the terminologies used in the multipath outputs are defined in the following table:

Term	Description
FCIP	
InputRate(B/s)	The number of bytes received per second on the in port of an FCIP link.
OutputRate(B/s)	The number of bytes received per second on the out port of an FCIP link.
InputFrames(/sec)	The number of frames received per second on the in port of an FCIP link.
OutputFrames(/sec)	The number of frames received per second on the out port of an FCIP link.
vFC	
FcoeOut(Oct)	The number of egress FCoE octets on a vFC interface.
FcoeIn(Oct)	The number of ingress FCoE octets on a vFC interface.
FcoeOutPkt	The number of egress FCoE packets on a vFC interface.
FcoeInPkt	The number of ingress FCoE packets on a vFC interface.

Related Commands

Command	Description
FCtrace	Traces the path to a destination device by displaying the corresponding switch's pWWN 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

ip-address	Specifies the peer SSM IP address. The format for the IP address is *A.B.C.D.*

Command Default

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 *address*	Configures the peer IP address.
port *number*	Configures a peer port. The range is 1 to 65535.

Command Default

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 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.

Command Default

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

ipv6-protocol-number	Specifies an IPv6 protocol number. The range is 0 to 255.
ipv6	Applies the ACL to any IPv6 packet.
source-ipv6-prefix/prefix-length	Specifies a source IPv6 network or class of networks. The format is *X:X:X::X/n* .
any	Applies the ACL to any source or destination prefix.
host *source-ipv6-address*	Applies the ACL to the specified source IPv6 host address. The format is *X:X:X::X* .
dest-ipv6-prefix /*prefix-length*	Specifies a destination IPv6 network or class of networks. The format is *X:X:X::X/n* .
host *dest-ipv6-address*	Applies the ACL to the specified destination IPv6 host address. The format is *X:X:X::X* .
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.
icmp-type	Specifies an ICMP message type. The range is 0 to 255.
icmp-code	Specifies an ICMP message code. The range is 0 255.
tcp	Applies the ACL to any TCP packet.
source-port-operator	Specifies an operand that compares the source ports of the specified protocol. The operands are **lt** (less than), **gt** (greater than), and **eq** (equals).

source-port-number	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.
dest-port-operator	Specifies an operand that compares the destination ports of the specified protocol. The operands are **lt** (less than), **gt** (greater than), and **eq** (equals).
dest-port-operator	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 whole SYN flag is not set.

Command Default

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
sswitch(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.

Command Default

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the 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 *repeat-count*	Specifies the repeat count. The range is 0 to 64.
interface	Specifies the interface on which the ping packets are to be sent.
gigabitethernet *slot*/*port*	Specifies a Gigabit Ethernet slot and port number.
mgmt *number*	Specifies the management interface.
port-channel *number*	Specifies a PortChannel number. The range is 1 to 256.
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.
size *size*	Specifies the size. The range is 10 to 2000.
timeout *timeout*	Specifies the timeout. The range is 1 to 10.

Command Default

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

priority	Specifies the priority for the IKE policy. The range is 1 to 255, where 1 is the high priority and 255 is the lowest.

Command Default

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 *number*	Configures a peer port. The range is 1 to 65535.

Command Default

Disabled

Command Modes

Fcip profile configuration submode.

Interface configuration submode.

Command History

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:

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)# port 5000
```

The following example configures port 4000 on ISCSI interface 2/1:

```
switch# config terminal
switch(config)# interface iscsi 2/1
switch(config-profile)# port 4000
```

Related Commands

Command	Description
show fcip profile	Displays information about the FCIP profile.
interface fcip *interface_number* 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.

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

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

Command Default

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.

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

port-channel number	Specifies the PortChannel number. The range is 1 to 256.

Command Default

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 activate

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

port-group-monitor activate name
no port-group-monitor activate name

Syntax Description

name	(Optional) Specifies the name of the port group policy. The maximum size is 32 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 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 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.

Command Default

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 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

policy-name	Displays the policy name. Maximum size is 32 characters.

Command Default

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)#
```

Related Commands

Command	Description
port-group-monitor activate	Activates the default 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-group-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.

Command Default

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

name	(Optional) Name of PMON port policy.

Command Default

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:

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

The following example shows how to activate the port monitor Cisco policy:

```
switch(config)# port-monitor activate pmon_policy
switch(config)#
```

Related Commands

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

port-monitor check-interval

To check errors at a lesser time interval compared to a poll interval, use the **port-monitor check-interval** command. To disable check-interval, use the no form of the command.

port-monitor check-interval *seconds*
no port-monitor check-interval *seconds*

Syntax Description

seconds	Specifies the check-interval time in seconds.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
7.3(1)D1(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure the check interval time to 30 seconds:

```
switch# configure terminal
switch(config)# port-monitor check-interval 30
```

Related Commands

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

port-monitor cong-isolation-recover

To configure congestion isolation recover, use the **port-monitor cong-isolation-recover** command. To revert to the default configuration, use the **no** form of the command.

port-monitor cong-isolation-recover { **recovery-interval** *seconds* | **isolate-duration** *hours* **num-occurrence** *number* }
no port-monitor cong-isolation-recover { **recovery-interval** *seconds* | **isolate-duration** *hours* **num-occurrence** *number* }

Syntax Description

recovery-interval *seconds*	Specifies the FPIN recovery interval.
isolate-duration *hours*	Specifies the FPIN isolate interval.
num-occurrence *number*	Specifies the number of occurrence.

Command Default

The congestion isolation recover is set to 900 seconds (15 minutes).

Command Modes

Configuration mode (config)

Command History

Release	Modification
8.5(1)	This command was introduced.

Examples

This example shows how to configure the isolate-duration to 24-hours and the number of rising threshold occurrences to be detected in this interval to 3:

```
switch# configure
switch(config)# port-monitor cong-isolation-recover isolate-duration 24 num-occurrence 3
```

This example shows how to configure the recovery-interval to 15 minutes:

```
switch# configure
switch(config)# port-monitor cong-isolation-recover recovery-interval 15
```

Related Commands

Command	Description
feature fpm	Enables Fabric Performance Monitor (FPM).
show port-monitor	Displays counter information for a port monitor policy.

port-monitor dirl

To specify the recovery interval for DIRL, use the **port-monitor dirl** command. To revert to the default interval, use the **no** form of the command.

port-monitor dirl recovery-interval *seconds*
no port-monitor dirl recovery-interval *seconds*

Syntax Description

recovery-interval *seconds*	Specifies the DIRL recovery interval.

Command Default

The DIRL recovery interval is set to 60 seconds.

Command Modes

Configuration mode (config)

Command History

Release	Modification
8.5(1)	This command was introduced.

Examples

This example shows how to configure the DIRL recovery interval of 60 seconds:

```
switch# configure
switch(config)# port-monitor fpin recovery-interval 60
```

Related Commands

Command	Description
feature fpm	Enables Fabric Performance Monitor (FPM).
show port-monitor	Displays counter information for a port monitor policy.

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.

Command Default

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 fpin

To specify the recovery interval for FPIN, use the **port-monitor fpin** command. To revert to the default interval, use the **no** form of the command.

port-monitor fpin { **recovery-interval** *seconds* | **isolate-duration** *hours* **num-occurrence** *number* }
no port-monitor fpin { **recovery-interval** *seconds* | **isolate-duration** *hours* **num-occurrence** *number* }

Syntax Description

recovery-interval *seconds*	Specifies the FPIN recovery interval.
isolate-duration *hours*	Specifies the FPIN isolate interval.
num-occurrence *number*	Specifies the number of occurrence.

Command Default

The FPIN recovery interval is set to 900 seconds (15 minutes).

Command Modes

Configuration mode (config)

Command History

Release	Modification
8.5(1)	This command was introduced.

Examples

This example shows how to configure the FPIN recovery interval of 1200 seconds (20 minutes):

```
switch# configure
switch(config)# port-monitor fpin recovery-interval 1200
```

This example shows how to configure the isolate-duration to 24-hours and the number of rising threshold occurrences to be detected in this interval to 3:

```
switch# configure
switch(config)# port-monitor fpin isolate-duration 24 num-occurrence 3
```

Related Commands

Command	Description
feature fpm	Enables Fabric Performance Monitor (FPM).
show port-monitor	Displays counter information for a port monitor policy.

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 *policy-name*
no port-monitor name *policy-name*

Syntax Description

policy-name	Displays the policy name.

Command Default

By default 16 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 user defined policy by name *cisco* and to assign the default values to the name:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# port-monitor name pmon_policy
switch(config-port-monitor)# show port-monitor pmon_policy
Policy Name  : pmon_policy
Admin status : Not Active
Oper status  : Not Active
Port type    : All Ports

Counter                  Threshold  Interval Rising Threshold      event Falling Threshold
     event  Warning Threshold    PMON Portguard
-------                  ---------  -------- -----------------      ----- ------------------
    -----  ------------------    --------------
Link Loss                Delta      60       5                     4     1
     4      Not enabled           Not enabled
Sync Loss                Delta      60       5                     4     1
     4      Not enabled           Not enabled
Signal Loss              Delta      60       5                     4     1
     4      Not enabled           Not enabled
Invalid Words            Delta      60       1                     4     0
```

```
     4      Not enabled           Not enabled
Invalid CRC's             Delta      60       5                    4     1
     4      Not enabled           Not enabled
State Change              Delta      60       100                  2     0
     4      Not enabled           Not enabled
TX Discards               Delta      60       200                  4     10
     4      Not enabled           Not enabled
LR RX                     Delta      60       5                    4     1
     4      Not enabled           Not enabled
LR TX                     Delta      60       5                    4     1
     4      Not enabled           Not enabled
Timeout Discards          Delta      60       200                  4     10
     4      Not enabled           Not enabled
Credit Loss Reco          Delta      1        1                    4     0
     4      Not enabled           Not enabled
TX Credit Not Available   Delta      1        10%                  4     0%
     4      Not enabled           Not enabled
RX Datarate               Delta      60       80%                  4     20%
     4      Not enabled           Not enabled
TX Datarate               Delta      60       80%                  4     20%
     4      Not enabled           Not enabled
TX-Slowport-Oper-Delay    Absolute   1        50ms                 4     0ms
     4      Not enabled           Not enabled
TXWait                    Delta      1        40%                  4     0%
     4      Not enabled           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 *vsan-id*	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 *wwn*	Specifies the node WWN as the Nx port connection.
pwwn *wwn*	Specifies the port WWN as the Nx port connection.
swwn *wwn*	Specifies the switch WWN as the xE port connection.
fwwn *wwn*	Specifies a fabric WWN login.
interface	Specifies the device or switch port interface through which each device is connected to the switch.
fc *slot/port*	Specifies a Fibre Channel interface by the slot and port.
port-channel *number*	Specifies a PortChannel interface. The range is 1 to 128.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Release	Modification
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 pwwn 20:11:00:33:11:00:2a:4a swwn 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)# nwwn 26:33:22:00:55:05:3d:4c fwwn 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)# pwwn 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)# swwn 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-wwn interface fc3/1
```

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

```
switch(config-port-security)# no any-wwn 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 *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

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 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 *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

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 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 *vsan-id*	Specifies the VSAN ID. The ranges is 1 to 4093.

Command Default

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.

Command	Description
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.

Command Default

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.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

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.

Command Default

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.

Command Default

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

Command Default

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.

Command	Description
show interface port-channel	Displays configuration and status information for a specified PortChannel interface.

port-type

To configure the port types that a port-monitor policy monitors, use **port-type** command. To revert to the default port type, use the **no** form of the command.

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

Syntax Description

all	Configures both trunk ports and access ports, except NP and TNP ports.
trunks	Configures only trunk ports (E and TE ports).
access-port	Configures only access ports (F and TF ports). NP and TNP ports are not supported in port monitor.

Command Default

The default port type is **all**.

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# configure
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
```

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
```

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
```

Note Currently, port monitor cannot monitor NP and TNP ports.

Related Commands

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

power redundancy-mode (MDS 9500 switches)

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.

Command Default

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.

power redundancy-mode (MDS 9700 switch)

To configure the capacity of the power supplies on the Cisco MDS 9700 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**] | **insrc-redundant** | **ps-redundant** | **redundant**}
no power redundancy-mode {**combined** [**force**] | **insrc-redundant** | **ps-redundant** | **redundant**}

Syntax Description

combined	Configures power supply redundancy mode as combined.
force	Forces combined mode without prompting.
insrc-redundant	Configure power supply redundancy mode as grid/AC input source redundant.
ps-redundant	Configure power supply redundancy mode as PS redundant.
redundant	Configures power supply redundancy mode as redundant.

Command Default

Redundant mode.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(1)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to configure the power supply redundancy mode as grid/AC input source redundant:

```
switch(config)# power redundancy-mode insrc-redundant
switch(config)# 2014 May 29 12:40:22 mds9706 %PLATFORM-4-PFM_PS_RED_MODE_CHG: Power redundancy
 mode changed to insrc-redundant
switch(config)# show environment power
Power Supply:
Voltage: 50 Volts
Power                              Actual        Total
Supply    Model                    Output     Capacity    Status
                                  (Watts )     (Watts )
-------  -------------------  -----------  -----------  --------------
1        DS-CAC97-3KW              333 W       3000 W     Ok
2        DS-CAC97-3KW              345 W       3000 W     Ok
3        DS-CAC97-3KW              345 W       3000 W     Ok
4        DS-CAC97-3KW              337 W       3000 W     Ok
                                  Actual        Power
Module    Model                    Draw    Allocated    Status
                                  (Watts )     (Watts )
-------  -------------------  -----------  -----------  --------------
1        DS-X9848-480K9            354 W        500 W    Powered-Up
```

```
3        DS-X97-SF1-K9              107 W        190 W    Powered-Up
4        DS-X97-SF1-K9              105 W        190 W    Powered-Up
6        DS-X9448-768K9             403 W        650 W    Powered-Up
Xb1      DS-X9706-FAB1               48 W         85 W    Powered-Up
Xb2      DS-X9706-FAB1               47 W         85 W    Powered-Up
Xb3      DS-X9706-FAB1               48 W         85 W    Powered-Up
Xb4      DS-X9706-FAB1               48 W         85 W    Powered-Up
Xb5      DS-X9706-FAB1               48 W         85 W    Powered-Up
Xb6      DS-X9706-FAB1               48 W         85 W    Powered-Up
fan1     DS-C9706-FAN                29 W        300 W    Powered-Up
fan2     DS-C9706-FAN                29 W        300 W    Powered-Up
fan3     DS-C9706-FAN                33 W        300 W    Powered-Up
N/A - Per module power not available
Power Usage Summary:
--------------------
Power Supply redundancy mode (configured)                InSrc-Redundant
Power Supply redundancy mode (operational)               InSrc-Redundant
Total Power Capacity (based on configured mode)               6000 W
Total Power of all Inputs (cumulative)                       12000 W
Total Power Output (actual draw)                              1360 W
Total Power Allocated (budget)                                3090 W
Total Power Available for additional modules                  2910 W
switch(config)#
```

The following example shows how to configure the power supply redundancy mode as PS redundant:

```
switch(config)# power redundancy-mode ps-redundant
switch(config)# 2014 May 29 12:40:22 mds9706 %PLATFORM-4-PFM_PS_RED_MODE_CHG: Power redundancy
 mode changed to ps-redundant
switch(config)# show environment power
Power Supply:
Voltage: 50 Volts
Power                              Actual        Total
Supply    Model                    Output     Capacity    Status
                                  (Watts )     (Watts )
-------  -------------------  -----------  -----------  --------------
1        DS-CAC97-3KW               333 W       3000 W     Ok
2        DS-CAC97-3KW               345 W       3000 W     Ok
3        DS-CAC97-3KW               345 W       3000 W     Ok
4        DS-CAC97-3KW               341 W       3000 W     Ok
                                  Actual        Power
Module    Model                     Draw    Allocated    Status
                                  (Watts )     (Watts )
-------  -------------------  -----------  -----------  --------------
1        DS-X9848-480K9             364 W        500 W    Powered-Up
3        DS-X97-SF1-K9              107 W        190 W    Powered-Up
4        DS-X97-SF1-K9              105 W        190 W    Powered-Up
6        DS-X9448-768K9             403 W        650 W    Powered-Up
Xb1      DS-X9706-FAB1               48 W         85 W    Powered-Up
Xb2      DS-X9706-FAB1               47 W         85 W    Powered-Up
Xb3      DS-X9706-FAB1               48 W         85 W    Powered-Up
Xb4      DS-X9706-FAB1               48 W         85 W    Powered-Up
Xb5      DS-X9706-FAB1               48 W         85 W    Powered-Up
Xb6      DS-X9706-FAB1               48 W         85 W    Powered-Up
fan1     DS-C9706-FAN                26 W        300 W    Powered-Up
fan2     DS-C9706-FAN                29 W        300 W    Powered-Up
fan3     DS-C9706-FAN                33 W        300 W    Powered-Up
N/A - Per module power not available
Power Usage Summary:
--------------------
Power Supply redundancy mode (configured)                PS-Redundant
Power Supply redundancy mode (operational)               PS-Redundant
Total Power Capacity (based on configured mode)               9000 W
Total Power of all Inputs (cumulative)                       12000 W
```

```
Total Power Output (actual draw)                            1364 W
Total Power Allocated (budget)                              3090 W
Total Power Available for additional modules                5910 W
switch(config)#
```

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

slot	Specifies the slot number for the module.

Command Default

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.

poweroff power-supply

To power off individual power supply units (PSU) in the system, use the **poweroff power-supply** command in configuration mode. Use the **no** form of this command to power up the specified PSU.

poweroff power-supply *psu*

no poweroff power-supply *psu*

Syntax Description

psu	Specifies the power supply number in the chassis.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
9.4(1)	This command was introduced.

Usage Guidelines

Note This command allows you to shut down PSUs, so that they are ignored by the system. You can power off PSUs that are connected to input power or disconnected from input power. System power warnings are generated when the installed PSUs have disconnected power inputs or are switched off. Powering off such PSUs allow them to remain installed the chassis for future increase of power capacity, but not supply power or generate alarms.

For power calculations, PSUs that are shut down are not included. They are included only after they are enabled and providing output. If powering down a PSU causes the available power capacity to fall below the allocated capacity, then the command is rejected and the PSU state is not changed. ISSD to versions of Cisco MDS NX-OS that do not support this feature is blocked if any power supply unit is powered off. To proceed, power on all the PSUs and then do the ISSD.

This command is supported on Cisco MDS 9700 Series Switches only.

Examples

The following example shows how a PSU power off command is rejected if the action would result in insufficient system power capacity:

```
mds-9710# show hardware capacity power

Power Resources Summary:
------------------------
Power Supply redundancy mode(administratively):  PS-Redundant
Power Supply redundancy mode(operationally):     PS-Redundant
Total Power Capacity                             9000.00 W
Power reserved for SUP,Fabric,and Fan Module(s)  2640.00 W ( 29.33 % )
```

```
Power currently used by Modules                  3060.00 W ( 34.00 % )
Total Power Available                            3300.00 W ( 36.67 % )
Total Power Output (actual draw)                 2249.00 W

mds-9710#
```

The following example shows how to power off a PSU:

```
mds-9710(config)# poweroff power-supply 3
mds-9710(config)#
```

The following example shows the error message that is displayed when powering off one of the PSUs results in less power for the entire system:

```
mds-9710(config)# poweroff power-supply 4
Error: no change to power supply 4 - powering it off would cause insufficient power for the
 system.
```

The following example shows how to verify the status of PSUs:

```
mds-9710(config)# show environment power


Power Supply:
Voltage: 50 Volts
Power                              Actual       Actual        Total
Supply    Model                    Output        Input     Capacity          Status
-------  -------------------  -----------  -----------  -----------  --------------
1        DS-CAC97-3KW              557 W        610 W       3000 W        Ok
2        DS-CAC97-3KW              568 W        619 W       3000 W        Ok
3        DS-CAC97-3KW              562 W        612 W       3000 W        Powered-dn
4        DS-CAC97-3KW              562 W        609 W       3000 W        Ok
5        ------------                0 W          0 W          0 W        Absent
6        ------------                0 W          0 W          0 W        Absent
7        ------------                0 W          0 W          0 W        Absent
8        ------------                0 W          0 W          0 W        Absent

Mod  Power-Status  Reason
---  ------------  --------------------------
3    Powered-dn     Configured Power down

                                  Actual        Power
                                  Actual        Power
Module    Model                     Draw    Allocated     Status
-------  -------------------  -----------  -----------  --------------
1        DS-X9448-768K9            377 W        650 W    Powered-Up
2        DS-X9748-3072K9           158 W        350 W    Powered-Up
3        DS-X9648-1536K9           232 W        750 W    Powered-Up
4        DS-X9334-K9               407 W        480 W    Powered-Up
5        DS-X97-SF4-K9              93 W        120 W    Powered-Up
6        DS-X97-SF4-K9              92 W        120 W    Powered-Up
7        DS-X9848-480K9            N/A            0 W    Powered-Dn
8        DS-X9334-K9               421 W        480 W    Powered-Up
9        DS-X9748-3072K9           142 W        350 W    Powered-Up
10       DS-X9448-768K9            N/A            0 W    Powered-Dn
Xb1      DS-X9710-FAB3              88 W        150 W    Powered-Up
Xb2      DS-X9710-FAB3              98 W        150 W    Powered-Up
Xb3      xbar                      N/A          150 W    Absent
Xb4      xbar                      N/A          150 W    Absent
Xb5      xbar                      N/A          150 W    Absent
Xb6      xbar                      N/A          150 W    Absent
fan1     DS-C9710-FAN-S             40 W        500 W    Powered-Up
fan2     DS-C9710-FAN-S             40 W        500 W    Powered-Up
fan3     DS-C9710-FAN-S             45 W        500 W    Powered-Up
```

```
N/A - Per module power not available


Power Usage Summary:
--------------------
Power Supply redundancy mode (configured)               PS-Redundant
Power Supply redundancy mode (operational)              PS-Redundant

Total Power Capacity (based on configured mode)              9000 W
Total Power of all Inputs (cumulative)                      12000 W
Total Power Output (actual draw)                             2249 W
Total Power Input  (actual draw)                             2450 W
Total Power Allocated (budget)                               5700 W
Total Power Available for additional modules                 3300 W
```

Related Commands

Command	Description
show environment power	Displays information about system power and PSUs.
show hardware capacity power	Displays the system power allocation and usage

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.

Command Default

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 dwrr-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
```

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

priority-flow-control long-distance

To enable the long distance Priority Flow Control (PFC), use the **long-distance** command. To disable this feature, use the **no** form of the command.

priority-flow-control long-distance
no priority-flow-control long-distance

Syntax Description

This command has no arguments or keywords.

Command Default

Default value for **long-distance** is set to False.

Command Modes

Interface Configuration mode.

Command History

Release	Modification
6.2(9)	Added the long-distance keyword to the syntax description.

Usage Guidelines

This command does not require a license.

Examples

The following example shows how to enable the long distance priority flow control:

```
switch(config)#interface ethernet-port-channel 1023
switch(config-if)# priority-flow-control long-distance
switch(config-if)#
```

The following example shows how to disable the long distance priority flow control:

```
switch(config)#interface ethernet-port-channel 1023
switch(config-if)# no priority-flow-control long-distance
switch(config-if)#
```

Related Commands

Command	Description
show sys int eth-qos port-node ethernet *intf*	Displays all the attributes of the interface including long distance.

priority-flow-control mode

To enable the mode Priority Flow Control (PFC), use the **priority-flow-control mode** command. To disable this feature, use the **no** form of the command.

priority-flow-control mode {**auto** | **off** | **on**}
no priority-flow-control mode {**auto** | **off** | **on**}

Syntax Description

auto	Sets the PFC mode to automatic.
off	Sets the PFC mode to off.
on	Sets the PFC mode to on.

Command Default

Default value for **mode** is set to auto.

Command Modes

Interface Configuration mode.

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

The following example shows how to set the PFC mode to on:

```
switch# configure terminal
switch(config)# interface ethernet 2/5
switch(config-if)# priority-flow-control mode on
switch(config-if)#
```

The following example shows how to set the PFC mode to off:

```
switch# configure terminal
switch(config)# interface ethernet 2/5
switch(config-if)# priority-flow-control mode off
```

switch(config-if)#

Related Commands

Command	Description
show interface priority-flow-control	Displays the status of priority flow control (PFC) on all interfaces.

purge analytics

To delete specific view instance and its associated flow metrics, use the **purge analytics** command.

purge analytics query *"query_string"*

Syntax Description

query *"query_string"*	Query syntax.

Command Default

None.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Note

- The *"query_string"* must have the format *"select all from <view-name>"*.
- You can clear the flow metrics without installing a push query.
- The where clause in the purge query can accept only the *port* key field.

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

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

Examples

This example shows an output after purging a view instance and its flow metrics:

```
switch# purge analytics query "select all from fc-scsi.scsi_target where port=fc3/17"
switch# show analytics query "select all from fc-scsi.scsi_target where port=fc3/17"
Table is empty for query "select all from fc-scsi.scsi_target where port=fc3/17"
```

Related Commands

Command	Description
analytics query	Installs a push analytics query.
clear analytics	Resets all flow metrics for a view instance.
feature analytics	Enables the SAN Analytics feature on a switch.
show analytics query	Displays the SAN analytics query information.
show analytics type	Displays the SAN analytics type.
ShowAnalytics	Displays the SAN analytics information in a tabular format.

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 *vsan-id*	Indicates that FCIDs are to be purged for a VSAN ID. The range is 1 to 4093.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to purge all dynamic unused FCIDs in VSAN 4:

```
switch# purge fcdomain fcid vsan 4
switch#
```

The following example shows how to purge all dynamic unused FCIDs in VSANs 4, 5, and 6:

```
switch# purge fcdomain fcid vsan 3-5
switch#
```

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

slot	Specifies the module slot number.
running-config	Purges the running configuration from the specified module.

Command Default

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.

Command Default

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.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example 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

pwwn-id	Specifies the port WWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Command Default

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

pwwn-id	Specifies the pWWN ID. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
fc-id	Specifies the FC ID of the device.

Command Default

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 (fc-management database configuration submode)

To configure the device port WWN, use the **pwwn** command. To disable this feature, use the **no** form of the command.

pwwn *dev_pwwn* **feature** {**all** | **fcs** | **fdmi** | **unzoned-ns** | **zone**} **operation** {**both** | **read** | **write**}
no pwwn *dev_pwwn* **feature** {**all** | **fcs** | **fdmi** | **unzoned-ns** | **zone**} [**operation** {**both** | **read** | **write**}]

Syntax Description

dev-pwwn	The WWN of the device. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
feature	Specifies the name of the feature.
all	Enables or disables all FC-CT queries.
fcs	Enables or disables the FC-CT query for the fabric configuration server.
fdmi	Enables or disables the FC-CT query for Fabric Device Common Interface (FDMI).
unzoned-ns	Enables or disables the FC-CT query for unzoned name server.
zone	Enables or disables the FC-CT query for zone server.
operation	(Optional) Specifies the read and write management FC-CT query.
both	Specifies both read and write query.
read	Specifies the get query.
write	Specifies the write query.

Command Default

None.

Command Modes

FC-management mode.

Command History

Release	Modification
6.2(9)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure an entry in the FC management security database:

```
switch(config)# fc-management database vsan 1
switch(config-fc-mgmt)#
switch(config-fc-mgmt)# pwwn 1:1:1:1:1:1:1:1 feature all operation both
Successful.
switch(config-fc-mgmt)#
switch(config-fc-mgmt)# pwwn 2:2:2:2:2:2:2:2 feature all operation read
Successful.
```

```
switch(config-fc-mgmt)#
switch(config-fc-mgmt)# pwwn 3:3:3:3:3:3:3:3 feature all operation write
Successful.
switch(config-fc-mgmt)#
switch(config-fc-mgmt)# show fc-management database
Fc-Management Security Database
---------------------------------------------------------------
VSAN PWWN FC-CT Permissions per FC services
---------------------------------------------------------------
1 01:01:01:01:01:01:01:01 Zone(RW), Unzoned-NS(RW), FCS(RW), FDMI(RW)
1 02:02:02:02:02:02:02:02 Zone(R), Unzoned-NS(R), FCS(R), FDMI(R)
1 03:03:03:03:03:03:03:03 Zone(W), Unzoned-NS(W), FCS(W), FDMI(W)
---------------------------------------------------------------
Total 3 entriesswitch(config-fc-mgmt)#
```

Related Commands

Command	Description
fc-management database	Configures the Fibre Channel Common Transport (FC-CT) management security database.

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, usethe **no** form of the command.

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

Syntax Description

pwwn-name	Specifies the pWWN of a real device. The format is *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*, where *h* is a hexadecimal number.
primary	Configures the virtual device as a real device.

Command Default

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.