CHAPTER 17

P Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See the "Command Modes" section to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family Configuration Guide*.

passive-mode

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

passive-mode

no passive-mode

Syntax Description

This command has no keywords or arguments.

Defaults

Disabled

Command Modes

Interface configuration submode

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.1(1).

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 merely 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.

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.

Defaults

None.

Command Modes

Interface configuration submode

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.1(1).

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 10.1.1.1
```

The following command deletes the assigned peer port information.

```
switch(config-if)# no peer-info ipaddr 10.10.1.1
```

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 10.1.1.1 port 3000
```

The following command deletes the assigned peer port information.

```
switch(config-if)# no peer-info ipaddr 10.1.1.1 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*	Specifies the notification interval. The range is 1 to 30.

Defaults

Disabled.

The initial default interval is 7 days.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
2.0(1b)	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.

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 20 alphanumeric characters in international phone format. **Note** Do not use spaces. Use the **+** prefix before the number.

Defaults

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

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

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

Related Commands

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

ping

To diagnose basic network connectivity, use the **ping** (packet internet groper) command in EXEC mode.

ping {*host-name* | *system-address*}

Syntax Description

host-name	Host name of system to ping. Maximum length is 64 characters.
system-address	Address of system to ping.

Defaults

None.

Command Modes

EXEC mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.0(2).

Usage Guidelines

The ping 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 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

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

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.

Defaults

None.

Command Modes

IKE configuration submode.

Command History

Release	Modification
2.0(1b)	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.

Defaults

Disabled

Command Modes

Fcip profile configuration submode

Interface configuration submode

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.1(1).

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.

port-channel persistent

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

port-channel *port-channel-id* **persistent**

Syntax Description

port-channel-id	Specifies the port channel ID. The range is 1 to 128.

Defaults

None.

Command Modes

EXEC mode.

Command History

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

Usage Guidelines

This command is not reversible. A user-created channel group cannot be converted to an autocreated channel group.When the **port-channel persistent** command is applied to an autocreated channel group, the channel group number does not change and the member ports properties change to those of a user-created channel group. The channel mode remains active.

Examples

The following example shows how to change the properties of an autocreated channel group to a persistent channel group.

```
switch# port-channel 10 persistent
```

Related Commands

Command	Description
port-channel protocol	Enables the PortChannel protocol.
show interface port-channel	Displays PortChannel interface information.
show port-channel	Displays PortChannel information.

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.
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.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.
force	Forces the database activation.
no-auto-learn	Disables the autolearn feature for the port security database.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.2(1)	This command was introduced.
2.0(1b)	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.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	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.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(1b)	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

port-security	Activates a port security database for the specified VSAN and automatically enables auto-learn.
database	Enters the port security database configuration mode for the specified VSAN.
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.

Defaults

None.

Command Modes

EXEC mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.2(1).

Usage Guidelines

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

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

Examples

The following example copies the active to the configured database.

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

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

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

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

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

Related Commands

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

port-security distribute

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

port-security distribute

no port-security distribute

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.0(2).

Command History

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

Usage Guidelines

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

Examples

The following example shows how to distribute the port security configuration to the fabric.

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

Related Commands

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

port-security enable

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

port-security enable

no port-security enable

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

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

Examples

The following example shows how to enable port security.

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

The following example shows how to disable port security.

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

Related Commands

Command	Description
show port-security	Displays port security information.

port-track enable

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

port-track enable

no port-track enable

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

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

Examples

The following example shows how to enable port tracking.

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

The following example shows how to disable port tracking.

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

Related Commands

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

port-track force-shut

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

port-track force-shut

no port-track force-shut

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Interface configuration submode.

Command History

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

Usage Guidelines

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

Examples

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

```
switch# config terminal
switch(config)# interface fc 1/2
switch(config-if)# oport-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*	Specifies a VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
2.0(1b)	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.

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.

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*

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

Syntax Description

portnumber	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	Prohibit communication with a portaddress.

Defaults

None.

Command Modes

FICON configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(1).

Usage Guidelines

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

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

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

Examples

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

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

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

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

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

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

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

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

The following example assigns a name to the port address.

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

The following example deletes a previously configured port address name.

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

Related Commands

Command	Description
show ficon	Displays configured FICON details.

power redundancy-mode

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

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

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

Syntax Description

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

Defaults

Redundant mode.

Command Modes

Configuration mode

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.0(2).

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

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.

Defaults

None.

Command Modes

Configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.0(2).

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
show module	Displays information for a specified module.
copy running-config startup-config	Copies all running configuration to the startup configuration.

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. The default.
medium	Configures the frames matching the class-map as medium priority.

Defaults

The default priority is low.

Command Modes

QoS policy map class configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

Command	Description
class	Configure a QoS policy map class.
show qos	Displays the current QoS settings.

purge fcdomain fcid

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

purge fcdomain fcid vsan *vsan-id*

Syntax Description

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

Defaults

None.

Command Modes

EXEC mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.0(2).

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.

Defaults

None.

Command Modes

EXEC mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.1(1).

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#
```

pwd

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

pwd

Syntax Description

This command has no keywords or arguments.

Defaults

None.

Command Modes

EXEC mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.0(2).

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*, where *h* is a hexadecimal number.
vsan *vsan-id*	Specifies the VSAN ID. The range is 1 to 4093.

Defaults

None.

Command Modes

DPVM database configuration submode.

Command History

Release	Modification
2.0(1b)	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.

Defaults

None.

Command Modes

fcdomain database configuration submode.

Command History

Release	Modification
2.1(2)	This command was introduced.

Usage Guidelines

Only one FC ID can be mapped to a pWWN.

Examples

The following example shows how to map the pWWN to the persistent FC ID.

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

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

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

Related Commands

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