CHAPTER 22

T 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*.

tacacs+ abort

To discard a TACACS+ Cisco Fabric Services (CFS) distribution session in progress, use the **tacacs+ abort** command in configuration mode.

tacacs+ abort

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

To use this command, TACACS+ must be enabled using the **tacacs+ enable** command.

Examples

The following example shows how to discard a TACACS+ CFS distribution session in progress.

```
switch# config terminal
switch(config)# tacacs+ abort
```

Related Commands

Command	Description
show tacacs+	Displays TACACS+ CFS distribution status and other details.
tacacs+ distribute	Enables CFS distribution for TACACS+.
tacacs+ enable	Enables TACACS+.

tacacs+ commit

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

tacacs+ commit

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

To use this command, TACACS+ must be enabled using the **tacacs+ enable** command.

Examples

The following example shows how to apply a TACACS+ configuration to the switches in the fabric.

```
switch# config terminal
switch(config)# tacacs+ commit
```

Related Commands

Command	Description
show tacacs+	Displays TACACS+ CFS distribution status and other details.
tacacs+ enable	Enables TACACS+.
tacacs+ distribute	Enables CFS distribution for TACACS+.

tacacs+ distribute

To enable Cisco Fabric Services (CFS) distribution for TACACS+, use the **tacacs+ distribute** command. To disable this feature, use the **no** form of the command.

tacacs+ distribute

no tacacs+ distribute

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

To use this command, TACACS+ must be enabled using the **tacacs+ enable** command.

Examples

The following example shows how to enable TACACS+ fabric distribution.

```
switch# config terminal
switch(config)# tacacs+ distribute
```

Related Commands

Command	Description
show tacacs+	Displays TACACS+ CFS distribution status and other details.
tacacs+ commit	Commits TACACS+ database changes to the fabric.
tacacs+ enable	Enables TACACS+.

tacacs+ enable

To enable TACACS+ in a switch, use the **tacacs+ enable** command in configuration mode. The disable this feature, use the **no** form of the command.

tacacs+ enable

no tacacs+ enable

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

Further TACACS+ commands are only available when the TACACS+ feature is enabled.

Using SHA-1 as the hash algorithm may prevent RADIUS or TACACS+ usage.

Examples

```
switch# config terminal
switch(config)# tacacs+ enable
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.

tacacs-server host

To configure TACACS+ server options on a switch, use the **tacacs-server host** command in configuration mode. Use the **no** form of the command to revert to factory defaults.

tacacs-server host {*server-name* | *ip-address*}
[**key** [**0**|**7**] *shared-secret*] [**port** *port-number*] [**timeout** *seconds*]

no tacacs-server host {*server-name* | *ip-address*}
[**key** [**0**|**7**] *shared-secret*] [**port** *port-number*] [**timeout** *seconds*]

Syntax Description

server-name	Enters TACACS+ server DNS name. The maximum character size is 256.
ip-address	Enters TACACS+ server IP address.
key	TACACS+ server's shared secret.
0	Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ client and server. This is the default.
7	Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.
shared secret	Configures a preshared key to authenticate communication between the TACACS+ client and server.
port *port-number*	TACACS+ server port for authentication. The range is 1 to 65535.
timeout	TACACS+ server timeout period in seconds.
seconds	Specifies the time (in seconds) between retransmissions to the TACACS+ server. The range is 1 to 60 seconds.

Defaults

Timeout: 1 second.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

This command is only available when the TACACS+ feature is enabled using the **tacacs+ enable** command.

Examples

The following example configures TACACS+ authentication.

```
switch# config terminal
switch(config)# tacacs-server host 10.10.2.3 key HostKey
switch(config)# tacacs-server host tacacs2 key 0 abcd
switch(config)# tacacs-server host tacacs3 key 7 1234
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
tacacs+ enable	Enable TACACS+.

tacacs-server key

To configure a global TACACS+ shared secret, use the **tacacs-server key** command. Use the **no** form of this command to removed a configured shared secret.

tacacs-server key [**0** | **7**] *shared-secret*

no tacacs-server key [**0** | **7**] *shared-secret*

Syntax Description

key	Global TACACS+ shared secret.
0	Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ client and server. This is the default.
7	Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.
shared-secret	Configures a preshared key to authenticate communication between the TACACS+ client and server.

Defaults

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

You need to configure the TACACS+ preshared key to authenticate the switch to the TACACS+ server. The length of the key is restricted to 65 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all TACACS+ server configurations on the switch. You can override this global key assignment by explicitly using the **key** option in the **tacacs-server host** command.

This command is only available when the TACACS+ feature is enabled using the **tacacs+ enable** command.

Examples

The following example configures TACACS+ server shared keys.

```
switch# config terminal
switch(config)# tacacs-server key AnyWord
switch(config)# tacacs-server key 0 AnyWord
switch(config)# tacacs-server key 7 public
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
tacacs+ enable	Enable TACACS+.

tacacs-server timeout

To specify the time between retransmissions to the TACACS+ servers, use the **tacacs-server timeout** command. You can revert the retransmission time to its default by issuing the **no** form of the command.

tacacs-server timeout *seconds*

notacacs-server timeout *seconds*

Syntax Description

seconds	Specifies the time (in seconds) between retransmissions to the RADIUS server. The default is one (1) second and the valid range is 1 to 60 seconds.

Defaults

None.

Command Modes

Configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(2).

Usage Guidelines

This command is only available when the TACACS+ feature is enabled using the **tacacs+ enable** command.

Examples

The following example configures the TACACS+ server timeout value.

```
switch# config terminal
switch(config)# tacacs-server timeout 30
```

Related Commands

Command	Description
show tacacs-server	Displays TACACS+ server information.
tacacs+ enable	Enable TACACS+.

tail

To display the last lines (tail end) of a specified file, use the **tail** command in EXEC mode.

tail *filename* [*number-of-lines*]

Syntax Description

filename	The name of the file for which you want to view the last lines.
number-of-lines	(Optional) The number of lines you want to view. The range is 0 to 80 lines.

Defaults

Displays the last 10 lines.

Command Modes

EXEC mode.

Command History

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

Usage Guidelines

You need two separate CLI terminals to use this command. In one terminal, execute the run-script or any other desired command. In the other, issue the **tail** command for the mylog file. On the second terminal session, you will see the last lines of the mylog file (as it grows) that is being saved in response to the command issued in the first terminal.

If you specify a long file and would like to exit in the middle, enter **Ctrl-c** to exit this command.

Examples

The following example displays the last lines (tail end) of a specified file.

```
switch# run-script slot0:test mylog
```

In another terminal, issue the **tail** command for the mylog file.

```
switch# tail mylog
config terminal
```

In the second CLI terminal, you see the last lines of the mylog file (as it grows) that is being saved in response to the command issued in the first terminal.

tcp cwm

To configure congestion window monitoring (CWM) TCP parameters, use the **tcp cwm** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp cwm [**burstsize** *size*]

no tcp cwm [**burstsize** *size*]

Syntax Description

burstsize *size*	Specifies the burstsize ranging from 10 to 100 KB.

Defaults

Enabled.

The default FCIP burst size is 10 KB.

The default iSCSI burst size is 50 KB

Command Modes

FCIP profile configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(4).

Usage Guidelines

Use these TCP parameters to control TCP retransmission behavior in a switch.

Examples

The following example configures a FCIP profile and enables congestion monitoring.

```
switch# config terminal
switch(config)# fcip profile 5
switch(config-profile)# tcp cwm
```

The following example assigns the burstsize value at 20 KB:

```
switch(config-profile)# tcp cwm burstsize 20
```

The following example disables congestion monitoring.

```
switch(config-profile)# no tcp cwm
```

The following example leaves the CWM feature in an enabled state but changes the burstsize to the default of 10 KB.

```
switch(config-profile)# no tcp cwm burstsize 25
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp keepalive-timeout

To configure the interval between which the TCP connection verifies if the FCIP link is functioning, use the **tcp keepalive-timeout** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp keepalive-timeout *seconds*

no tcp keepalive-timeout *seconds*

Syntax Description

seconds	Specifies the time in seconds. The range is 1 to 7200.

Defaults

60 seconds.

Command Modes

FCIP profile configuration submode.

Command History

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

Usage Guidelines

This command can be used to detect FCIP link failures.

Examples

The following example configures a FCIP profile:

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

The following example specifies the keepalive timeout interval for the TCP connection:

```
switch(config-profile)# tcp keepalive-timeout 120
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp maximum-bandwidth-kbps

To manage the TCP window size in Kbps, use the **tcp maximum-bandwidth-kbps** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp max-bandwidth-kbps *bandwidth* **min-available-bandwidth-kbps** *threshold* {**round-trip-time-ms** *milliseconds* | **round-trip-time-us** *microseconds*}

no tcp max-bandwidth-kbps *bandwidth* **min-available-bandwidth-kbps** *threshold* {**round-trip-time-ms** *milliseconds* | **round-trip-time-us** *microseconds*}

Syntax Description

bandwidth	Specifies the Kbps bandwidth. The range is 1000 to 1000000.
min-available-bandwidth-kbps	Configures the minimum slow start threshold.
threshold	Specifies the Kbps threshold. The range is 1000 to 1000000.
round-trip-time-ms *milliseconds*	Configures the estimated round trip time across the IP network to reach the FCIP peer end point in milliseconds. The range is 0 to 300.
round-trip-time-us *microeconds*	Configures the estimated round trip time across the IP network to reach the FCIP peer end point in microseconds. The range is 0 to 300000.

Defaults

Enabled.

The FCIP defaults are **max-bandwidth** = 1G, **min-available-bandwidth** = 500 Kbps, and **round-trip-time** =1 ms.

The iSCSI defaults are **max-bandwidth** = 1G, **min-available-bandwidth** = 70 Kbps, and **round-trip-time** =1 ms.

Command Modes

FCIP profile configuration submode.

Command History

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

Usage Guidelines

The **maximum-bandwidth** option and the **round-trip-time** option together determine the window size.

The **minimum-available-bandwidth** option and the **round-trip-time** option together determine the threshold below which TCP aggressively increases its size. After it reaches the threshold the software uses standard TCP rules to reach the maximum available bandwidth.

Examples

The following example configures a FCIP profile:

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

The following example configures the maximum available bandwidth at 900 Kbps, the minimum slow start threshold as 300 Kbps, and the round trip time as 10 milliseconds:

```
switch(config-profile)# tcp max-bandwidth-kbps 900 min-available-bandwidth-kbps 300
round-trip-time-ms 10
```

The following example reverts to the factory defaults:

```
switch(config-profile)# no tcp max-bandwidth-kbps 900 min-available-bandwidth-kbps 300
round-trip-time-ms 10
```

The following example configures the maximum available bandwidth at 2000 Kbps, the minimum slow start threshold as 2000 Kbps, and the round trip time as 200 microseconds:

```
switch(config-profile)# tcp max-bandwidth-kbps 2000 min-available-bandwidth-kbps 2000
round-trip-time-us 200
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp maximum-bandwidth-mbps

To manage the TCP window size in Mbps, use the **tcp maximum-bandwidth-mbps** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp max-bandwidth-mbps *bandwidth* **min-available-bandwidth-mbps** *threshold* {**round-trip-time-ms** *milliseconds* | **round-trip-time-us** *microseconds*}

no tcp max-bandwidth-mbps *bandwidth* **min-available-bandwidth-mbps** *threshold* {**round-trip-time-ms** *milliseconds* | **round-trip-time-us** *microseconds*}

Syntax Description

bandwidth	Specifies the Mbps bandwidth. The range is 1 to 1000.
min-available-bandwidth-mbps	Configures the minimum slow start threshold.
threshold	Specifies the Mbps threshold. The range is 1 to 1000.
round-trip-time-ms *milliseconds*	Configures the estimated round trip time across the IP network to reach the FCIP peer end point in milliseconds. The range is 0 to 300.
round-trip-time-us *microeconds*	Configures the estimated round trip time across the IP network to reach the FCIP peer end point in microseconds. The range is 0 to 300000.

Defaults

Enabled.

The FCIP defaults are **max-bandwidth** = 1G, **min-available-bandwidth** = 500 Kbps, and **round-trip-time** =1 ms.

The iSCSI defaults are **max-bandwidth** = 1G, **min-available-bandwidth** = 70 Kbps, and **round-trip-time** =1 ms.

Command Modes

FCIP profile configuration submode.

Command History

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

Usage Guidelines

The **maximum-bandwidth** option and the **round-trip-time** option together determine the window size.

The **minimum-available-bandwidth** option and the **round-trip-time** option together determine the threshold below which TCP aggressively increases its size. After it reaches the threshold the software uses standard TCP rules to reach the maximum available bandwidth.

Examples

The following example configures a FCIP profile:

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

The following example configures the maximum available bandwidth at 900 Mbps, the minimum slow start threshold as 300 Mbps, and the round trip time as 10 milliseconds:

```
switch(config-profile)# tcp max-bandwidth-mbps 900 min-available-bandwidth-mbps 300
round-trip-time-ms 10
```

The following example reverts to the factory defaults:

```
switch(config-profile)# no tcp max-bandwidth-mbps 900 min-available-bandwidth-mbps 300
round-trip-time-ms 10
```

The following example configures the maximum available bandwidth at 2000 Mbps, the minimum slow start threshold as 2000 Mbps, and the round trip time as 200 microseconds:

```
switch(config-profile)# tcp max-bandwidth-mbps 2000 min-available-bandwidth-mbps 2000
round-trip-time-us 200
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp max-jitter

To estimate the maximum delay jitter experienced by the sender in microseconds, use the **tcp max-jitter** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp max-jitter *microseconds*

no tcp max-jitter *microseconds*

Syntax Description

microseconds	Specifies the delay time in microseconds ranging from 0 to 10000.

Defaults

Enabled.

The default value is 100 microseconds for FCIP and 500 microseconds for iSCSI interfaces.

Command Modes

FCIP profile configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(4).

Usage Guidelines

None.

Examples

The following example configures delay jitter time:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# fcip profile 3
switch(config-profile)# tcp max-jitter 600
switch(config-profile)# do show fcip profile 3
FCIP Profile 3
    Internet Address is 10.3.3.3  (interface GigabitEthernet2/3)
    Tunnels Using this Profile: fcip3
    Listen Port is 3225
    TCP parameters
        SACK is enabled
        PMTU discovery is enabled, reset timeout is 3600 sec
        Keep alive is 60 sec
        Minimum retransmission timeout is 200 ms
        Maximum number of re-transmissions is 4
        Send buffer size is 0 KB
        Maximum allowed bandwidth is 1000000 kbps
        Minimum available bandwidth is 500000 kbps
        Estimated round trip time is 1000 usec
        Congestion window monitoring is enabled, burst size is 10 KB
        Configured maximum jitter is 600 us
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp max-retransmissions

To specify the maximum number of times a packet is retransmitted before TCP decides to close the connection, use the **tcp max-retransmissions** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp max-retransmissions *number*

no tcp max-retransmissions *number*

Syntax Description

number	Specifies the maximum number. The range is 1 to 8.

Defaults

Enabled

Command Modes

FCIP profile configuration submode.

Command History

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

Usage Guidelines

The default is 4 and the range is from 1 to 8 retransmissions.

Examples

The following example configures a FCIP profile:

```
switch# config terminal
switch(config)# fcip profile 5
```

The following example specifies the maximum number of retransmissions :

```
switch(config-profile)# tcp max-retransmissions 6
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp min-retransmit-time

To control the minimum amount of time TCP waits before retransmitting, use the **tcp min-retransmit-time** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp min-retransmit-time *milliseconds*

no tcp min-retransmit-time *milliseconds*

Syntax Description

milliseconds	Specifies the time in milliseconds. The range is 200 to 5000.

Defaults

300 milliseconds.

Command Modes

FCIP profile configuration submode.

Command History

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

Usage Guidelines

None.

Examples

The following example configures a FCIP profile:

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

The following example specifies the minimum TCP retransmit time for the TCP connection:

```
switch(config-profile)# tcp min-retransmit-time 500
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp pmtu-enable

To configure path MTU (PMTU) discovery, use the **tcp pmtu-enable** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp pmtu-enable [**reset-timeout** *seconds*]

no tcp pmtu-enable [**reset-timeout** *seconds*]

Syntax Description

reset-timeout *seconds*	Specifies the PMTU reset timeout. The range is 60 to 3600 seconds.

Defaults

Enabled.

3600 seconds.

Command Modes

FCIP profile configuration submode.

Command History

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

Usage Guidelines

None.

Examples

The following example configures a FCIP profile:

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

The following example disables PMTU discovery:

```
switch(config-profile)# no tcp pmtu-enable
```

The following example enables PMTU discovery with a default of 3600 seconds:

```
switch(config-profile)# tcp pmtu-enable
```

The following example specifies the PMTU reset timeout to 90 seconds:

```
switch(config-profile)# tcp pmtu-enable reset-timeout 90
```

The following example leaves the PMTU in an enabled state but changes the timeout to the default of 3600 seconds:

```
switch(config-profile)# no tcp pmtu-enable reset-timeout 600
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp qos

To specify the differentiated services code point (DSCP) value to mark all IP packets (type of service—TOS field in the IP header) on an ISCSI interface, use the **tcp qos** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp qos *value*

no tcp qos *value*

Syntax Description

value	Applies the control DSCP value to all outgoing frames in the control TCP connection.

Defaults

0

Command Modes

FCIP profile configuration submode.

Command History

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

Usage Guidelines

Use these TCP parameters to control TCP retransmission behavior in a switch.

Examples

The following example configures the TCP QoS value on an iSCSI interface.

```
switch# config terminal
switch(config)# interface iscsi 1/2
switch(config-if)# tcp qos 5
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp qos control

To specify the differentiated services code point (DSCP) value to mark all IP packets (type of service—TOS field in the IP header), use the **tcp qos control** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp qos control *value* **data** *value*

no tcp qos control *value* **data** *value*

Syntax Description

value	Applies the control DSCP value to all FCIP frames in the control TCP connection.
data *value*	Applies the data DSCP value applies to all FCIP frames in the data connection.

Defaults

Enabled.

Command Modes

FCIP profile configuration submode.

Command History

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

Usage Guidelines

Use these TCP parameters to control TCP retransmission behavior in a switch.

Examples

The following example configures a FCIP profile:

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

The following example configures the control TCP connection and data connection to mark all packets on that DSCP value:

```
switch(config-profile)# tcp qos control 3 data 5
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp sack-enable

To enable selective acknowledgment (SACK) to overcome the limitations of multiple lost packets during a TCP transmission, use the **tcp sack-enable** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp sack-enable

no tcp sack-enable

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

FCIP profile configuration submode.

Command History

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

Usage Guidelines

The receiving TCP sends back SACK advertisements to the sender. The sender can then retransmit only the missing data segments.

Examples

The following example configures a FCIP profile:

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

The following example enables the SACK mechanism on the switch:

```
switch(config-profile)# tcp sack-enable
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp send-buffer-size

To define the required additional buffering—beyond the normal send window size —that TCP allows before flow controlling the switch's egress path for the FCIP interface, use the **tcp send-buffer-size** command. Use the **no** form of this command to disable this feature or revert to its factory defaults.

tcp send-buffer-size *size*

no tcp send-buffer-size *size*

Syntax Description

size	Specifies the buffer size in KB. The range is 0 to 8192.

Defaults

Enabled.

The default FCIP buffer size is 0 KB.

The default iSCSI buffer size is 4096 KB

Command Modes

FCIP profile configuration submode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(4).

Usage Guidelines

None.

Examples

The following example configures a FCIP profile:

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

The following example configure the advertised buffer size to 5000 KB :

```
switch(config-profile)# tcp send-buffer-size 5000
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.

tcp-connection

To configure the number of TCP connections for the FCIP interface, use the **tcp-connection** command. To revert to the default, use the **no** form of the command.

tcp-connection *number*

no tcp-connection *number*

Syntax Description

number	Enters the number of attempts (1 or 2).

Defaults

Two attempts.

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.

Use the **tcp-connection** option to specify the number of TCP connections from a FCIP link. By default, the switch tries two (2) TCP connections for each FCIP link.

Examples

The following example configures the TCP connections.

```
switch# config terminal
switch(config)# interface fcip 50
switch(config-if)# tcp-connection 1
switch(config-if)# no tcp-connection 1
```

Related Commands

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

telnet

To log in to a host that supports Telnet, use the **telnet** command in EXEC mode.

telnet {*hostname* | *ip-address*} [*port*]

Syntax Description

hostname	Specifies a host name. Maximum length is 64 characters.
ip-address	Specifies an IP address.
port	(Optional) Specifies a port number. The range is 0 to 2147483647.

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 establishes a Telnet session to the specified IP address.

```
switch# telnet 172.22.91.153
Trying 172.22.91.153...
Connected to 172.22.91.153.
Login:xxxxxxxx
Password:xxxxxxxxx
switch#
```

Related Commands

Command	Description
telnet server enable	Enables the Telnet server.

telnet server enable

To enable the Telnet server if you wish to return to a Telnet connection from a secure SSH connection, use the **telnet server enable** command. To disable the Telnet server, use the **no** form of this command

telnet server enable

no telnet server enable

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example enables the Telnet server.

```
switch(config)# telnet server enable
updated
```

The following example disables the Telnet server.

```
switch(config)# no telnet server enable
updated
```

Related Commands

Command	Description
telnet	Logs in to a host that supports Telnet.

terminal

To configure terminal attributes, use the **terminal** command in EXEC mode. To revert to the defaults, use the **no** form of the command.

terminal {**length** *lines* | **monitor** | **session-timeout** | **terminal-type** *type* | **tree-update** | **width** *integer*}

terminal no {**length** | **monitor** | **session-timeout** | **terminal-type** | **width**}

Syntax Description

length *lines*	Specifies the number of lines on the screen. The range is 0 to 512. Enter 0 to scroll continuously.
monitor	Copies Syslog output to the current terminal line.
session-timeout	Specifies the session timeout value in minutes. The range is 0 to 525600. Enter 0 to disable.
terminal-type *type*	Sets the terminal type. Maximum length is 80 characters.
tree-update	Updates the main parse tree.
width *integer*	Sets the width of the display terminal, from 0 to 80.

Defaults

The default number of lines for the length is 24. The default width is 80 lines.

Command Modes

EXEC

Command History

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

Usage Guidelines

Remember that all terminal parameter-setting commands are set locally and do not remain in effect after a session is ended. You must perform this task at the EXEC prompt at each session to see the debugging messages.

If the length is not 24 and the width is not 80, then you need to set a length and width.

Examples

The following example displays debug command output and error messages during the current terminal session.

```
switch# terminal monitor
Aug  8 10:32:42 sup48 % LOG_PLATFORM-5-PLATFORM_MOD_CFG_PWRDN: Module 1 powered down
Aug  8 10:32:42 sup48 % LOG_PLATFORM-5-PLATFORM_MOD_PWRDN: Module 1 powered down
Aug  8 10:32:42 sup48 % LOG_PLATFORM-5-PLATFORM_MOD_INSERT: Module 1 has been inserted
Aug  8 10:33:12 sup48 % LOG_PLATFORM-5-PLATFORM_MOD_PWRON: Module 1 powered up
Aug  8 10:33:13 sup48 % LOG_MODULE-5-MOD_REG_OK: LCM - Registration succeeded for module 1
Aug  8 10:38:15 sup48 % LOG_PLATFORM-5-PLATFORM_MOD_CFG_PWRDN: Module 1 powered down
Aug  8 10:38:15 sup48 % LOG_PLATFORM-5-PLATFORM_MOD_INSERT: Module 1 has been inserted
......
```

The following example stops the current terminal monitoring session.

```
switch# terminal no monitor
```

Related Commands

Command	Description
show terminal	Displays terminal configuration information.

time

To configure the time for the command schedule, use the **time** command. To disable this feature, use the **no** form of the command.

time {**daily** *daily-schedule* | **monthly** *monthly-schedule* | **start** {*start-time* | **now**} | **weekly** *weekly-schedule*}

no time

Syntax Description

daily *daily-schedule*	Configures a daily command schedule. The format is *HH*:*MM*, where *HH* is hours (0 to 23) and *MM* is minutes (0 to 59). Maximum length is 5 characters.
monthly *monthly-schedule*	Configures a monthly command schedule. The format is *dm*:*HH*:*MM*, where *dow* is the day of the month (1 to 31), *HH* is hours (0 to 23) and *MM* is minutes (0 to 59). Maximum length is 8 characters.
start	Schedules a job to run at a future time.
start-time	Specifies the future time to run the job. The format is *yyyy*:*mmm*:*dd*:*HH*:*MM*, where *yyyy* is the year, *mmm* is the month (jan to dec), *dd* is the day of the month (1 to 31), *HH* is hours (0 to 23) and *MM* is minutes (0 to 59). Maximum length is 18 characters.
now	Starts the job two minutes after the command is entered.
weekly *weekly-schedule*	Configures a weekly command schedule. The format is *dow*:*HH*:*MM*, where *dow* is the day of the week (1 to 7, Sun to Sat), *HH* is hours (0 to 23) and *MM* is minutes (0 to 59). Maximum length is 10 characters.

Defaults

Disabled.

Command Modes

Scheduler job configuration submode.

Command History

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

Usage Guidelines

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

Examples

The following example shows how to configure a command schedule job to run every Friday at 2200.

```
switch# config terminal
switch(config)# scheduler schedule name MySchedule
switch(config-schedule)# time weekly 6:22:00
```

The following example starts a command schedule job in two minutes and repeats every 24 hours.

```
switch(config-schedule)# time start now repeat 24:00
```

Related Commands

Command	Description
scheduler enable	Enables the command scheduler.
scheduler schedule name	Configures a schedule for the command scheduler.
show scheduler	Displays schedule information.

time-stamp

To enable FCIP time stamps on a frame, use the **time-stamp** command. To disable this command for the selected interface, use the **no** form of the command.

time-stamp [**acceptable-diff** *number*]

no time-stamp [**acceptable-diff** *number*]

Syntax Description

acceptable-diff *number*	Configures the acceptable time difference for timestamps in milliseconds. The range is 500 to 10000.

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.

The **time-stamp** option instructs the switch to discard frames that are older than a specified time.

Examples

The following example enables the timestamp for an FCIP interface.

```
switch# config terminal
switch(config)# interface fcip 50
switch(config-if)# time-stamp
switch(config-if)# time-stamp acceptable-diff 4000
```

Related Commands

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

tlport alpa-cache

To manually configure entries in an ALPA cache, use the **tlport alpa-cache** command

tlport alpa-cache interface *interface* **pwwn** *pwwn* **alpa** *alpa*

no tlport alpa-cache interface *interface* **pwwn** *pwwn*

Syntax Description

interface *interface*	Specifies a Fibre Channel interface.
pwwn *pwwn*	Specifies the peer WWN ID for the ALPA cache entry.
alpa *alpa*	Specifies the ALPA cache to which this entry is to be added.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

This command was introduced in Cisco MDS SAN-OS Release 1.3(5).

Usage Guidelines

Generally, ALPA cache entries are automatically populated when an ALPA is assigned to a device. Use this command only if you wish to manually add further entries.

Examples

The following example configures the specified pWWN as a new entry in this cache

```
switch# config terminal
switch(config)# tlport alpa-cache interface fc1/2 pwwn 22:00:00:20:37:46:09:bd alpa 0x02
```

Related Commands

Command	Description
show tlport	Displays TL port information.

traceroute

To print the route an IP packet takes to a network host, use the **traceroute** command in EXEC mode.

traceroute {*hostname* | *ip-address*}

Syntax Description

host name	Specifies a host name. Maximum length is 64 characters.
ip-address	Specifies an IP address.

Defaults

None.

Command Modes

EXEC mode.

Command History

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

Usage Guidelines

This command traces the route an IP packet follows to an internet host by launching UDP probe packets with a small TTL (time to live) then listening for an ICMP (Internet Control Message Protocol) "time exceeded" reply from a gateway.

Note Probes start with a TTL of one and increase by one until encountering an ICMP "port unreachable." This means that the host was accessed or a maximum flag was hit. A line is printed showing the TTL, address of the gateway and round trip time of each probe. If the probe answers come from different gateways, the address of each responding system is printed.

Examples

The following example prints the route IP packets take to the network host www.cisco.com.

```
switch# traceroute www.cisco.com
traceroute to www.cisco.com (171.71.181.19), 30 hops max, 38 byte packets
 1  kingfisher1-92.cisco.com (172.22.92.2)  0.598 ms  0.470 ms  0.484 ms
 2  nubulab-gw1-bldg6.cisco.com (171.71.20.130)  0.698 ms  0.452 ms  0.481 ms
 3  172.24.109.185 (172.24.109.185)  0.478 ms  0.459 ms  0.484 ms
 4  sjc12-lab4-gw2.cisco.com (172.24.111.213)  0.529 ms  0.577 ms  0.480 ms
 5  sjc5-sbb4-gw1.cisco.com (171.71.241.174)  0.521 ms  0.495 ms  0.604 ms
 6  sjc12-dc2-gw2.cisco.com (171.71.241.230)  0.521 ms  0.614 ms  0.479 ms
 7  sjc12-dc2-cec-css1.cisco.com (171.71.181.5)  2.612 ms  2.093 ms  2.118 ms
 8  www.cisco.com (171.71.181.19)  2.496 ms *  2.135 ms
```

transfer-ready-size

To configure the target transfer ready size for SCSI write commands on a SAN tuner extension N port, use the **transfer-ready-size** command.

transfer-ready-size *bytes*

Syntax Description

bytes	Specifies the transfer ready size in bytes. The range is 0 to 2147483647.

Defaults

None.

Command Modes

SAN extension N port configuration submode.

Command History

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

Usage Guidelines

For a SCSI **write command-id** command with a larger transfer size, the target performs multiple transfers based on the specified transfer size.

Examples

The following example configures the transfer ready size on a SAN extension tuner N port.

```
switch# san-ext-tuner
switch(san-ext)# nWWN 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
switch(san-ext-nport)# transfer-ready-size 512000
```

Related Commands

Command	Description
nport pwwn	Configures a SAN extension tuner N port.
san-ext-tuner	Enables the SAN extension tuner feature.
show san-ext-tuner	Displays SAN extension tuner information.
write command-id	Configures a SCSI write command for a SAN extension tuner N port.

transport email

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

transport email {**from** *email-address* | **reply-to** *email-address* | **smtp-server** *ip-address* [**port** *port-number*]

no transport email {**from** *email-address* | **reply-to** *email-address* | **smtp-server** *ip-address* [**port** *port-number*]

Syntax Description

from *email-address*	Specifies the from email address. For example: SJ-9500-1@xyz.com. The maximum length is 255 characters.
reply-to *email-address*	Specifies the reply-to email address. For address, example: admin@xyz.com. The maximum length is 255 characters.
smtp-server *ip-address*	Specifies the SMTP server address, either DNS name or IP address. The maximum length is 255 characters.
port *port-number*	(Optional) Changes depending on the server location. The port usage defaults to 25 if no port number is specified.

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 configures the from and reply-to e-mail addresses.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# transport email from user@company1.com
switch(config-callhome)# transport email reply-to person@place.com
```

The following example configures the SMTP server and ports.

```
switch(config-callhome)# transport email smtp-server 192.168.1.1
switch(config-callhome)# transport email smtp-server 192.168.1.1 port 30
```

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.

trunk protocol enable

To configure the trunking protocol, use the **trunk protocol enable** command in configuration mode. To disable this feature, use the **no** form of the command.

trunk protocol enable

no trunk protocol enable

Syntax Description

This command has no other arguments or keywords.

Defaults

Enabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

If the trunking protocol is disabled on a switch, no port on that switch can apply new trunk configurations. Existing trunk configurations are not affected—the TE port continues to function in trunking mode, but only supports traffic in VSANs that it negotiated previously (when the trunking protocol was enabled). Also, other switches that are directly connected to this switch are similarly affected on the connected interfaces. In some cases, you may need to merge traffic from different port VSANs across a non-trunking ISL. If so, you need to disable the trunking protocol.

Examples

The following example shows how to disable the trunk protocol feature.

```
switch# config terminal
switch(config)# no trunk protocol enable
```

The following example shows how to enable the trunk protocol feature.

```
switch(config)# trunk protocol enable
```

Related Commands

Command	Description
show trunk protocol	Displays the trunk protocol status.