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 “About the CLI Command Modes” section on page 1-3 to determine the appropriate mode for each command.
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0(x)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show tacacs+</td>
<td>Displays TACACS+ CFS distribution status and other details.</td>
</tr>
<tr>
<td>tacacs+ distribute</td>
<td>Enables CFS distribution for TACACS+.</td>
</tr>
<tr>
<td>tacacs+ enable</td>
<td>Enables TACACS+.</td>
</tr>
</tbody>
</table>
Send documentation comments to mdsfeedback-doc@cisco.com

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0(x)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show tacacs</code></td>
<td>Displays TACACS+ CFS distribution status and other details.</td>
</tr>
<tr>
<td><code>tacacs+ enable</code></td>
<td>Enables TACACS+.</td>
</tr>
<tr>
<td><code>tacacs+ distribute</code></td>
<td>Enables CFS distribution for TACACS+.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0(x)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show tacacs+</code></td>
<td>Displays TACACS+ CFS distribution status and other details.</td>
</tr>
<tr>
<td><code>tacacs+ commit</code></td>
<td>Commits TACACS+ database changes to the fabric.</td>
</tr>
<tr>
<td><code>tacacs+ enable</code></td>
<td>Enables TACACS+.</td>
</tr>
</tbody>
</table>
tacacs+ enable

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

```bash
  tacacs+ enable

  no tacacs+ enable
```

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

### Defaults
None.

### Command Modes
Configuration mode.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3(1)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>NX-OS 4.1(1b)</td>
<td>This command was deprecated.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
Additional 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
The following example shows how to enable TACACS+ in a switch:

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

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show tacacs+</td>
<td>Displays TACACS+ server information.</td>
</tr>
</tbody>
</table>
tacacs-server deadtime

To set a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness, use the `tacacs-server deadtime` command. To disable the monitoring of the nonresponsive TACACS+ server, use the `no` form of the command.

```
tacacs-server deadtime time

no tacacs-server deadtime time
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>time</code></td>
<td>Specifies the time interval in minutes. The range is 1 to 1440.</td>
</tr>
</tbody>
</table>

**Defaults**

Disabled.

**Command Modes**

Configuration mode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Setting the time interval to zero disables the timer. If the dead time interval for an individual TACACS+ server is greater than zero (0), that value takes precedence over the value set for the server group.

When the dead time interval is 0 minutes, TACACS+ server monitoring is not performed unless the TACACS+ server is part of a server group and the dead time interval for the group is greater than 0 minutes.

**Examples**

The following example shows how to set a duration of 10 minutes:

```
switch# config terminal
switch(config)# tacacs-server deadtime 10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>deadtime</code></td>
<td>Sets a time interval for monitoring a nonresponsive TACACS+ server.</td>
</tr>
<tr>
<td><code>show tacacs-server</code></td>
<td>Displays all configured TACACS+ server parameters.</td>
</tr>
</tbody>
</table>
tacacs-server directed-request

To specify a TACACS+ server to send authentication requests to when logging in, use the **tacacs-server directed-request** command. To revert to sending the authentication request to the configured group, use the **no** form of the command.

```
tacacs-server directed-request
no tacacs-server directed-request
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Disabled.

**Command Modes**

Configuration mode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The user can specify the `username@servername` during login. The user name is sent to the server name for authentication.

**Examples**

The following example shows how to specify a TACACS+ server to send authentication requests when logging in:

```
switch# config terminal
switch(config)# tacacs-server directed-request
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show tacacs-server</td>
<td>Displays all configured TACACS+ server parameters.</td>
</tr>
<tr>
<td>show tacacs-server directed request</td>
<td>Displays a directed request TACACS+ server configuration.</td>
</tr>
</tbody>
</table>
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 | ipv4-address | ipv6-address} [key [0|7] shared-secret] [port port-number] [test {idle-time time | password password | username name}] [timeout seconds]
```

```
no tacacs-server host {server-name | ipv4-address | ipv6-address} [key [0|7] shared-secret] [port port-number] [test {idle-time time | password password | username name}] [timeout seconds]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server-name</td>
<td>Specifies the TACACS+ server DNS name. The maximum character size is 256.</td>
</tr>
<tr>
<td>ipv4-address</td>
<td>Specifies the TACACS+ server IP address. in the format A.B.C.D.</td>
</tr>
<tr>
<td>ipv6-address</td>
<td>Specifies the TACACS+ server IP address in the format X:X::X.</td>
</tr>
<tr>
<td>key</td>
<td>(Optional) Configures the TACACS+ server’s shared secret key.</td>
</tr>
<tr>
<td>0</td>
<td>(Optional) Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ client and server. This is the default.</td>
</tr>
<tr>
<td>7</td>
<td>(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.</td>
</tr>
<tr>
<td>shared secret</td>
<td>(Optional) Configures a preshared key to authenticate communication between the TACACS+ client and server.</td>
</tr>
<tr>
<td>port port-number</td>
<td>(Optional) Configures a TACACS+ server port for authentication. The range is 1 to 65535.</td>
</tr>
<tr>
<td>test</td>
<td>(Optional) Configures parameters to send test packets to the TACACS+ server.</td>
</tr>
<tr>
<td>idle-time time</td>
<td>(Optional) Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.</td>
</tr>
<tr>
<td>password password</td>
<td>(Optional) Specifies a user password in the test packets. The maximum size is 32.</td>
</tr>
<tr>
<td>username name</td>
<td>(Optional) Specifies a user name in the test packets. The maximum size is 32.</td>
</tr>
<tr>
<td>timeout</td>
<td>(Optional) Configures a TACACS+ server timeout period.</td>
</tr>
<tr>
<td>seconds</td>
<td>(Optional) Specifies the timeout (in seconds) between retransmissions to the TACACS+ server. The range is 1 to 60 seconds.</td>
</tr>
</tbody>
</table>

**Defaults**

Idle-time is not set. Server monitoring is turned off.

Timeout is 1 second.

Username is test.

Password is test.

**Command Modes**

Configuration mode.
tacacs-server host

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3(1)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>3.0(1)</td>
<td>Added the ipv6-address argument and the test option.</td>
</tr>
</tbody>
</table>

Usage Guidelines

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

When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.

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
switch(config)# tacacs-server host 10.10.2.3 test idle-time 10
switch(config)# tacacs-server host 10.10.2.3 test username tester
switch(config)# tacacs-server host 10.10.2.3 test password 2B9ka5
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show tacacs-server</td>
<td>Displays TACACS+ server information.</td>
</tr>
<tr>
<td>tacacs+ enable</td>
<td>Enables TACACS+.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(Optional) Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ client and server. This is the default.</td>
</tr>
<tr>
<td>7</td>
<td>(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.</td>
</tr>
<tr>
<td>shared-secret</td>
<td>Configures a preshared key to authenticate communication between the TACACS+ client and server.</td>
</tr>
</tbody>
</table>

### Defaults

None.

### Command Modes

Configuration mode.

### Command History

```
Release   Modification
1.0(2)     This command was introduced.
```

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show tacacs-server</td>
<td>Displays TACACS+ server information.</td>
</tr>
<tr>
<td>tacacs+ enable</td>
<td>Enable TACACS+.</td>
</tr>
</tbody>
</table>
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 using the `no` form of the command.

```
tacacs-server timeout seconds

no tacacs-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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show tacacs-server</td>
<td>Displays TACACS+ server information.</td>
</tr>
<tr>
<td>tacacs+ enable</td>
<td>Enable TACACS+.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>filename</code></td>
<td>The name of the file for which you want to view the last lines.</td>
</tr>
<tr>
<td><code>number-of-lines</code></td>
<td>(Optional) The number of lines you want to view. The range is 0 to 80 lines.</td>
</tr>
</tbody>
</table>

**Defaults**

Displays the last 10 lines.

**Command Modes**

EXEC mode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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, enter 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, press `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, enter 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 entered in the first terminal.
To configure a crypto tape backup group, use the `tape-bkgrp` command. Use the `no` form of this command to disable this feature.

```
tape-bkgrp groupname
no tape-bkgrp groupname
```

**Syntax Description**

| `groupname` | Specifies the backup tape group. |

**Defaults**

None.

**Command Modes**

Cisco SME cluster configuration mode submode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A tape volume group is a group of tapes that are categorized by function. For example, HR1 could be designated tape volume group for all Human Resources backup tapes.

Adding tape groups allows you to select VSANs, hosts, storage devices, and paths that Cisco SME will use for encrypted data. For example, adding a tape group for HR data sets the mapping for Cisco SME to transfer data from the HR hosts to the dedicated HR backup tapes.

**Examples**

The following example adds a backup tape group:

```
switch# config t
switch(config)# sme cluster cl
switch(config-sme-cl)# tape-bkgrp group1
switch(config-sme-cl-tape-bkgrp)#
```

The following example removes a backup tape group:

```
switch# config t
switch(config)# sme cluster cl
switch(config-sme-cl)# no tape-bkgrp group1
switch(config-sme-cl-tape-bkgrp)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear sme</td>
<td>Clears Cisco SME configuration.</td>
</tr>
<tr>
<td>show sme cluster</td>
<td>Displays information about the Cisco SME cluster</td>
</tr>
</tbody>
</table>
tape compression

To configure tape compression, use the `tape-compression` command. To disable this feature, use the `no` form of the command.

```
tape-compression
no tape-compression
```

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

**Defaults**
None.

**Command Modes**
Cisco SME cluster configuration submode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use this command to compress encrypted data.

**Examples**
The following example enables tape compression:

```
switch#config t
switch(config)#sme cluster c1
switch(config-sme-cl)#tape-compression
```

The following example disables tape compression:

```
switch#config t
switch(config)#sme cluster c1
switch(config-sme-cl)#no tape-compression
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear sme</td>
<td>Clears Cisco SME configuration.</td>
</tr>
<tr>
<td>show sme cluster</td>
<td>Displays information about the Cisco SME cluster.</td>
</tr>
<tr>
<td>show sme cluster tape</td>
<td>Displays information about all tape volume groups or a specific group.</td>
</tr>
</tbody>
</table>
**tape-device**

To configure a crypto tape device, use the `tape-device` command. To disable this feature, use the `no` form of the command.

```
tape-device device name

no tape-device device name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>device name</code></td>
<td>Specifies the name of the tape device.</td>
</tr>
</tbody>
</table>

**Defaults**

None.

**Command Modes**

Cisco SME tape volume configuration submode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The tape device commands are available in the `(config-sme-cl-tape-bkgrp-tapedevice)` submode.

**Examples**

The following example configures a crypto tape device:

```
switch# config t
switch(config)# sme cluster cl
switch(config-sme-cl)# tape-bkgrp group1
switch(config-sme-cl-tape-bkgrp)# tape-device devicename1
```

The following example removes a crypto tape device:

```
switch# config t
switch(config)# sme cluster cl
switch(config-sme-cl)# tape-bkgrp group1
switch(config-sme-cl-tape-bkgrp)# no tape-device devicename1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear sme</td>
<td>Clears Cisco SME configuration.</td>
</tr>
<tr>
<td>show sme cluster</td>
<td>Displays information about the Cisco SME cluster</td>
</tr>
<tr>
<td>show sme cluster tape</td>
<td>Displays information about all tape volume groups or a specific group</td>
</tr>
</tbody>
</table>
To configure tape key recycle policy, use the `tape-keyrecycle` command. To disable this feature, use the `no` form of the command.

```
tape-keyrecycle
no tape-keyrecycle
```

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

**Defaults**
None.

**Command Modes**
Cisco SME cluster configuration submode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Cisco SME allows you to recycle the tape keys. If you enable tape key recycling, all the previous instances of the tape key will be deleted. If you do not enable tape key recycle, all the previous instances and the current instance of the tape key is maintained, and the current instance is incremented by 1.

**Examples**
The following example enables tape key recycling:

```
switch# config t
switch(config)#sme cluster cl
switch(config-sme-cl)#tape-keyrecycle
```

The following example disables tape key recycling:

```
switch# config t
switch(config)#sme cluster cl
switch(config-sme-cl)#no tape-keyrecycle
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear sme</td>
<td>Clears Cisco SME configuration.</td>
</tr>
<tr>
<td>show sme cluster</td>
<td>Displays information about the Cisco SME cluster</td>
</tr>
</tbody>
</table>
tape-read command-id

To configure a SCSI tape read command for a SAN tuner extension N port, use the **tape-read command-id** command.

```
tape-read command-id cmd-id target pwwn transfer-size bytes [continuous [filemark-frequency frequency] | num-transactions number [filemark-frequency frequency]]
```

**Syntax Description**

- **cmd-id** Specifies the command identifier. The range is 0 to 2147483647.
- **target pwwn** Specifies the target port WWN. The format is \( hh:hh:hh:hh:hh:hh:hh:hh \).
- **transfer-size bytes** Specifies the transfer size in multiples of 512 bytes. The range is 512 to 8388608.
- **continuous** (Optional) Specifies that the command is performed continuously.
- **filemark-frequency frequency** (Optional) Specifies the filemark frequency. The range is 1 to 2147483647.
- **num-transactions number** (Optional) Specifies a number of transactions. The range is 1 to 2147483647.

**Defaults**

Filemark frequency: 0.

**Command Modes**

SAN extension N port configuration submode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To stop a continuous SCSI tape read command in progress, use the **stop command-id** command.

There can be just one outstanding I/O at a time to the virtual N port that emulates the tape behavior.

**Examples**

The following example configures a single SCSI tape read command:

```
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
transfer-size 512000 num-transactions 5000000 filemark-frequency 32
```

The following example configures a continuous SCSI tape read command:

```
switch# san-ext-tuner
switch(san-ext)# nWWN 10:00:00:00:00:00:00:00
```
Send documentation comments to mdsfeedback-doc@cisco.com

```
switch(san-ext)# nport pwnn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nport pwnn</td>
<td>Configures a SAN extension tuner N port.</td>
</tr>
<tr>
<td>san-ext-tuner</td>
<td>Enables the SAN extension tuner feature.</td>
</tr>
<tr>
<td>show san-ext-tuner</td>
<td>Displays SAN extension tuner information.</td>
</tr>
<tr>
<td>stop</td>
<td>Cancels a SCSI command in progress on a SAN extension tuner N port.</td>
</tr>
</tbody>
</table>
tape-volgrp

To configure the crypto tape volume group, use the `tape-volgrp` command. To disable this command, use the `no` form of the command.

```plaintext
tape-volgrp group name
no tape-volgrp group name
```

**Syntax Description**

- **group name**: Specifies the tape volume group name.

**Defaults**

None.

**Command Modes**

Cisco SME crypto backup tape group configuration submode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The tape volume group commands are available in the Cisco SME crypto tape volume group (`config-sme-cl-tape-bkgrp-volgrp`) submode.

**Examples**

The following example configures a crypto tape volume group:

```plaintext
switch# config t
switch(config)# sme cluster cl
switch(config-sme-cl)# tape-bkgrp tbgl
switch(config-sme-cl-tape-bkgrp)# tape-volgrp tv1
```

The following example removes a crypto tape volume group:

```plaintext
switch# config t
switch(config)# sme cluster cl
switch(config-sme-cl)# tape-bkgrp tbgl
switch(config-sme-cl-tape-bkgrp)# no tape-volgrp tv1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear sme</td>
<td>Clears Cisco SME configuration.</td>
</tr>
<tr>
<td>show sme cluster tape</td>
<td>Displays information about tapes</td>
</tr>
</tbody>
</table>
tape-write command-id

To configure a SCSI tape write command for a SAN tuner extension N port, use the `tape-write command-id` command.

```
tape-write command-id cmd-id target pwnn transfer-size bytes [continuous [filemark-frequency frequency] | num-transactions number [filemark-frequency frequency]]
```

**Syntax Description**

- **cmd-id**: Specifies the command identifier. The range is 0 to 2147483647.
- **transfer-size bytes**: Specifies the transfer size in multiples of 512 bytes. The range is 512 to 8388608.
- **continuous**: (Optional) Specifies that the command is performed continuously.
- **filemark-frequency frequency**: (Optional) Specifies the filemark frequency. The range is 1 to 2147483647.
- **num-transactions number**: (Optional) Specifies a number of transactions. The range is 1 to 2147483647.

**Defaults**

Filemark frequency: 0.

**Command Modes**

SAN extension N port configuration submode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To stop a continuous SCSI tape write command in progress, use the `stop command-id` command.

**Note**

There can be just one outstanding I/O at a time to the virtual N port that emulates the tape behavior.

**Examples**

The following example configures a single SCSI tape write command:

```
switch# san-ext-tuner
switch(san-ext)# nwwn 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwnn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
```

The following example configures a continuous SCSI tape write command:

```
switch# san-ext-tuner
switch(san-ext)# nwwn 10:00:00:00:00:00:00:00
```
Send documentation comments to mdsfeedback-doc@cisco.com

switch(san-ext)# nport pwnn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>nport pwnn</td>
<td>Configures a SAN extension tuner N port.</td>
</tr>
<tr>
<td></td>
<td>san-ext-tuner</td>
<td>Enables the SAN extension tuner feature.</td>
</tr>
<tr>
<td></td>
<td>show san-ext-tuner</td>
<td>Displays SAN extension tuner information.</td>
</tr>
<tr>
<td></td>
<td>stop</td>
<td>Cancels a SCSI command in progress on a SAN extension tuner N port.</td>
</tr>
</tbody>
</table>
target (iSLB initiator configuration)

To configure an iSLB initiator target, use the `target` command in iSLB initiator configuration submode. To remove the target configuration, use the `no` form of the command.

```plaintext
target { device-alias device-alias | pwwn pWWN } [ vsan vsan-id ] [ no-zone ] [ trespass ]
[ revert-primary-port ] [ fc-lun LUN iscsi-lun LUN ] [ sec-device-alias device-alias | sec-pwnn pWWN ]
[ sec-vsan sec-vsan-id ] [ sec-lun LUN ] [ iqn-name target-name ]

no target { device-alias device-alias | pwwn pWWN } [ vsan vsan-id ] [ no-zone ] [ trespass ]
[ revert-primary-port ] [ fc-lun LUN iscsi-lun LUN ] [ sec-device-alias device-alias | sec-pwnn pWWN ]
[ sec-vsan sec-vsan-id ] [ sec-lun LUN ] [ iqn-name target-name ]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>device-alias</code></td>
<td>Specifies the device alias of the Fibre Channel target.</td>
</tr>
<tr>
<td><code>device-alias</code></td>
<td>Specifies the device alias of the Fibre Channel target.</td>
</tr>
<tr>
<td><code>vsan</code></td>
<td>(Optional) Assigns VSAN membership to the initiator target.</td>
</tr>
<tr>
<td><code>vsan-id</code></td>
<td>(Optional) Specifies the VSAN ID. The range is 1 to 4093.</td>
</tr>
<tr>
<td><code>no-zone</code></td>
<td>(Optional) Indicates no automatic zoning.</td>
</tr>
<tr>
<td><code>trespass</code></td>
<td>(Optional) Enables trespass support.</td>
</tr>
<tr>
<td><code>revert-primary-port</code></td>
<td>(Optional) Reverts to the primary port when it comes back up.</td>
</tr>
<tr>
<td><code>fc-lun LUN</code></td>
<td>(Optional) Specifies the Fibre Channel LUN of the Fibre Channel target. The format is <code>0xhhhh[:hhhh[:hhhh[:hhhh]]]</code>.</td>
</tr>
<tr>
<td><code>iscsi-lun LUN</code></td>
<td>(Optional) Specifies the iSCSI LUN. The format is <code>0xhhhh[:hhhh[:hhhh[:hhhh]]]</code>.</td>
</tr>
<tr>
<td><code>sec-device-alias</code></td>
<td>(Optional) Specifies the device alias of the secondary Fibre Channel target.</td>
</tr>
<tr>
<td><code>target-device-alias</code></td>
<td>(Optional) Specifies the initiator’s target device alias. The maximum size is 64.</td>
</tr>
<tr>
<td><code>sec-vsan</code></td>
<td>(Optional) Assigns VSAN membership to the initiator.</td>
</tr>
<tr>
<td><code>sec-vsan-id</code></td>
<td>(Optional) Specifies the VSAN ID. The range is 1 to 4093.</td>
</tr>
<tr>
<td><code>sec-lun LUN</code></td>
<td>(Optional) Specifies the FC LUN of the secondary Fibre Channel target. The format is <code>0xhhhh[:hhhh[:hhhh[:hhhh]]]</code>.</td>
</tr>
<tr>
<td><code>iqn-name</code></td>
<td>(Optional) Specifies the name of the target.</td>
</tr>
<tr>
<td><code>target-name</code></td>
<td>Specifies the initiator’s target name. The maximum size is 223.</td>
</tr>
</tbody>
</table>

**Defaults**

None.

**Command Modes**

iSLB initiator configuration submode.
Chapter 23 T Commands

target (iSLB initiator configuration)

Send documentation comments to mdsfeedback-doc@cisco.com

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You can configure an iSLB initiator target using the device alias or the pWWN. You have the option of specifying one or more of the following optional parameters:

- Secondary pWWN
- Secondary device alias
- LUN mapping
- IQN
- VSAN identifier

Note

The VSAN identifier is optional if the target is online. If the target is not online, the VSAN identifier is required.

If you configure an IQN for an initiator target, then that name is used to identify the initiator target. Otherwise, a unique IQN is generated for the initiator target.

Examples

The following example configures an iSLB initiator using an IP address and then enters iSLB initiator configuration submode:

```
switch# config t
switch(config)# islb initiator ip-address 209.165.200.226
```

The following example grants iSLB initiator access to the target using a pWWN with auto zoning enabled (default):

```
switch (config-islb-init)# target pwwn 26:00:01:02:03:04:05:06
```

The following example grants iSLB initiator access to the target using a pWWN with auto zoning disabled:

```
switch (config-islb-init)# target pwwn 26:00:01:02:03:04:05:06 no-zone
```

The following example grants iSLB initiator access to the target using a device alias and optional LUN mapping:

```
switch(config-islb-init)# target device-alias SampleAlias fc-lun 0x1234 iscsi-lun 0x2345
```

The following example grants iSLB initiator access to the target using a device alias and an optional IQN:

```
switch(config-islb-init)# target device-alias SampleAlias iqn-name
  iqn.1987-01.com.cisco.initiator
```

The following example grants iSLB initiator access to the target using a device alias and a VSAN identifier:

```
switch(config-islb-init)# target device-alias SampleAlias vsan 10
```
target (iSLB initiator configuration)

Note
The VSAN identifier is optional if the target is online. If the target is not online, the VSAN identifier is required.

The following example disables the configured iSLB initiator target.

switch (config-islb-init)# no target pwwn 26:00:01:02:03:04:05:06

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>islb initiator</td>
<td>Assigns an iSLB name and IP address to the iSLB initiator and enters iSLB initiator configuration submode.</td>
</tr>
<tr>
<td></td>
<td>show islb initiator</td>
<td>Displays iSLB CFS information.</td>
</tr>
<tr>
<td></td>
<td>show islb initiator detail</td>
<td>Displays detailed iSLB initiator information.</td>
</tr>
<tr>
<td></td>
<td>show islb initiator summary</td>
<td>Displays iSLB initiator summary information.</td>
</tr>
</tbody>
</table>
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` (Optional) 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3(4)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcip profile</td>
<td>Configures FCIP profile parameters.</td>
</tr>
<tr>
<td>show fcip profile</td>
<td>Displays FCIP profile information.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcip profile</td>
<td>Configures FCIP profile parameters.</td>
</tr>
<tr>
<td>show fcip profile</td>
<td>Displays FCIP profile information.</td>
</tr>
</tbody>
</table>
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 microseconds` 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 Mbps`, 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**

```
Release Modification
1.1(1) This command was introduced.
```

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcip profile</td>
<td>Configures FCIP profile parameters.</td>
</tr>
<tr>
<td>show fcip profile</td>
<td>Displays FCIP profile information.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bandwidth</code></td>
<td>Specifies the Mbps bandwidth. The range is 1 to 1000.</td>
</tr>
<tr>
<td><code>min-available-bandwidth-mbps</code></td>
<td>Configures the minimum slow start threshold.</td>
</tr>
<tr>
<td><code>threshold</code></td>
<td>Specifies the Mbps threshold. The range is 1 to 1000.</td>
</tr>
<tr>
<td><code>round-trip-time-ms milliseconds</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>round-trip-time-us microseconds</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Defaults**

Enabled.

The FCIP defaults are `max-bandwidth = 1G`, `min-available-bandwidth = 500 Mbps`, 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcip profile</td>
<td>Configures FCIP profile parameters.</td>
</tr>
<tr>
<td>show fcip profile</td>
<td>Displays FCIP profile information.</td>
</tr>
</tbody>
</table>
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**

- **Release**: 1.3(4)
  - **Modification**: This command was introduced.

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcip profile</td>
<td>Configures FCIP profile parameters.</td>
</tr>
<tr>
<td>show fcip profile</td>
<td>Displays FCIP profile information.</td>
</tr>
</tbody>
</table>
## 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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>Specifies the maximum number. The range is 1 to 8.</td>
</tr>
</tbody>
</table>

### Defaults

Enabled.

### Command Modes

FCIP profile configuration submode.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>fcip profile</code></td>
<td>Configures FCIP profile parameters.</td>
</tr>
<tr>
<td><code>show fcip profile</code></td>
<td>Displays FCIP profile information.</td>
</tr>
</tbody>
</table>
Send documentation comments to mdsfeedback-doc@cisco.com

**Chapter 23 T Commands**

## 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcip profile</td>
<td>Configures FCIP profile parameters.</td>
</tr>
<tr>
<td>show fcip profile</td>
<td>Displays FCIP profile information.</td>
</tr>
</tbody>
</table>
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]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>reset-timeout seconds</th>
<th>(Optional) Specifies the PMTU reset timeout. The range is 60 to 3600 seconds.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Defaults</th>
<th>Enabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3600 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>FCIP profile configuration submode.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1.1(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th>None.</th>
</tr>
</thead>
</table>

**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
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>fcip profile</td>
<td>Configures FCIP profile parameters.</td>
</tr>
<tr>
<td></td>
<td>show fcip profile</td>
<td>Displays FCIP profile information.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>value</code></td>
<td>Applies the control DSCP value to all outgoing frames in the control TCP connection.</td>
</tr>
</tbody>
</table>

### Defaults

0

### Command Modes

FCIP profile configuration submode.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcip profile</td>
<td>Configures FCIP profile parameters.</td>
</tr>
<tr>
<td>show fcip profile</td>
<td>Displays FCIP profile information.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>value</code></td>
<td>Applies the control DSCP value to all FCIP frames in the control TCP connection.</td>
</tr>
<tr>
<td><code>data value</code></td>
<td>Applies the data DSCP value applies to all FCIP frames in the data connection.</td>
</tr>
</tbody>
</table>

### Defaults

Enabled.

### Command Modes

FCIP profile configuration submode.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcip profile</td>
<td>Configures FCIP profile parameters.</td>
</tr>
<tr>
<td>show fcip profile</td>
<td>Displays FCIP profile information.</td>
</tr>
</tbody>
</table>
Send documentation comments to mdsfeedback-doc@cisco.com

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcip profile</td>
<td>Configures FCIP profile parameters.</td>
</tr>
<tr>
<td>show fcip profile</td>
<td>Displays FCIP profile information.</td>
</tr>
</tbody>
</table>
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**
```
Release       Modification
1.3(4)         This command was introduced.
```

**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**
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcip profile</td>
<td>Configures FCIP profile parameters.</td>
</tr>
<tr>
<td>show fcip profile</td>
<td>Displays FCIP profile information.</td>
</tr>
</tbody>
</table>
```
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface fcip</td>
<td>Displays an interface configuration for a specified FCIP interface.</td>
</tr>
</tbody>
</table>
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**

- **1.0(2)**: This command was introduced.

**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:xxxxxxxx
switch#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>telnet server enable</code></td>
<td>Enables the Telnet server.</td>
</tr>
</tbody>
</table>
**Send documentation comments to mdsfeedback-doc@cisco.com**

# telnet server enable

To enable the Telnet server if you want 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>telnet</td>
<td>Logs in to a host that supports Telnet.</td>
</tr>
</tbody>
</table>
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}

no terminal {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 mode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
terminal event-manager bypass

To bypass the CLI event manager, use the **terminal event-manager bypass** command. To disable this command, use the **no** form of the command.

```
terminal event-manager bypass
no terminal event-manager bypass
```

**Syntax Description**

This command has no arguments or keywords.

**Defaults**

Event manager is enabled.

**Command Modes**

Any

**Command History**

```
Release        Modification

NX-OS 4.2(1)    Added a note.
4.1(3)          This command was introduced.
```

**Usage Guidelines**

None.

**Note**

If you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the default action. For example, if you match a CLI command in a match statement, you must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute. You can use the **terminal event-manager bypass** command to allow all EEM policies with CLI matches to execute the CLI commands.

**Examples**

This example shows how to disable the CLI event manager:

```
switch# terminal event-manager bypass
switch#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show terminal</td>
<td>Displays terminal configuration.</td>
</tr>
</tbody>
</table>
To verify if the authorization settings are correct or not, use the `test aaa authorization` command.

```plaintext
test aaa authorization command-type {commands | config-commands} user {username} command {cmd}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>command-type</td>
<td>Specifies the command type. You can use the keywords for the command type.</td>
</tr>
<tr>
<td>commands</td>
<td>Specifies authorization for all commands.</td>
</tr>
<tr>
<td>config-commands</td>
<td>Specifies authorization for configuration commands.</td>
</tr>
<tr>
<td>user</td>
<td>Specifies the user to be authorized. The maximum size is 32.</td>
</tr>
<tr>
<td>username</td>
<td>Specifies the user to be authorized.</td>
</tr>
<tr>
<td>cmd</td>
<td>Specifies command to be authorized.</td>
</tr>
</tbody>
</table>

### Defaults
None.

### Command Modes
EXEC mode.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>NX-OS 4.2(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
None.

### Examples
The following example shows how to verify if the authorization settings are correct or not:

```plaintext
switch(config)# test aaa authorization command-type commands user u1 command "feature dhcp"
% Success
switch(config)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show aaa authorization all</td>
<td>Displays all authorization information.</td>
</tr>
</tbody>
</table>
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}
```

### Syntax Description

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

### Defaults

Disabled.

### Command Modes

Scheduler job configuration submode.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0(x)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheduler enable</td>
<td>Enables the command scheduler.</td>
</tr>
<tr>
<td>scheduler schedule name</td>
<td>Configures a schedule for the command scheduler.</td>
</tr>
<tr>
<td>show scheduler</td>
<td>Displays schedule information.</td>
</tr>
</tbody>
</table>
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** (Optional) Configures the acceptable time difference for timestamps in milliseconds. The range is 500 to 10000.

**Defaults**

Disabled.

**Command Modes**

Interface configuration submode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interface fcip</td>
<td>Displays the configuration for a specified FCIP interface.</td>
</tr>
</tbody>
</table>
To manually configure entries in an ALPA cache, use the `tlport alpa-cache` command. To disable the entries in an ALPA cache, use the `no` form of the command.

```
  tlport alpa-cache interface interface pwnn pwnn alpa alpa
  no tlport alpa-cache interface interface pwnn pwnn
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface interface</td>
<td>Specifies a Fibre Channel interface.</td>
</tr>
<tr>
<td>pwnn pwnn</td>
<td>Specifies the peer WWN ID for the ALPA cache entry.</td>
</tr>
<tr>
<td>alpa alpa</td>
<td>Specifies the ALPA cache to which this entry is to be added.</td>
</tr>
</tbody>
</table>

**Defaults**

Disabled.

**Command Modes**

Configuration mode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3(5)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Generally, ALPA cache entries are automatically populated when an ALPA is assigned to a device. Use this command only if you want to manually add additional 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 pwnn 22:00:00:20:37:46:09:bd alpa 0x02
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show tlport</td>
<td>Displays TL port information.</td>
</tr>
</tbody>
</table>
tracert

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

```
tracert [ipv6] [hostname [size packet-size] | ip-address] | hostname | ip-address]
```

### Syntax Description

- **ipv6**: (Optional) Traces a route to an IPv6 destination.
- **hostname**: (Optional) Specifies a host name. Maximum length is 64 characters.
- **size packet-size**: (Optional) Specifies a packet size. The range is 0 to 64.
- **ip-address**: (Optional) Specifies an IP address.

### Defaults

None.

### Command Modes

EXEC mode.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0(2)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>3.0(1)</td>
<td>Added the <code>ipv6</code> argument.</td>
</tr>
</tbody>
</table>

### 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) and 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 found. 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# tracert www.cisco.com
tracert 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-csm1.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**
  - 2.0(x) 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 pwnn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
switch(san-ext-nport)# transfer-ready-size 512000
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nport pwnn</td>
<td>Configures a SAN extension tuner N port.</td>
</tr>
<tr>
<td>san-ext-tuner</td>
<td>Enables the SAN extension tuner feature.</td>
</tr>
<tr>
<td>show san-ext-tuner</td>
<td>Displays SAN extension tuner information.</td>
</tr>
<tr>
<td>write command-id</td>
<td>Configures a SCSI write command for a SAN extension tuner N port.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>from email-address</td>
<td>Specifies the from e-mail address. For example: <a href="mailto:SJ-9500-1@xyz.com">SJ-9500-1@xyz.com</a>. The maximum length is 255 characters.</td>
</tr>
<tr>
<td>reply-to email-address</td>
<td>Specifies the reply to e-mail address. For e-mail, example: <a href="mailto:admin@xyz.com">admin@xyz.com</a>. The maximum length is 255 characters.</td>
</tr>
<tr>
<td>smtp-server ip-address</td>
<td>Specifies the SMTP server address, either DNS name or IP address. The maximum length is 255 characters.</td>
</tr>
<tr>
<td>port port-number</td>
<td>(Optional) Changes depending on the server location. The port usage defaults to 25 if no port number is specified.</td>
</tr>
</tbody>
</table>

**Defaults**

None.

**Command Modes**

Call Home configuration submode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>callhome</td>
<td>Configures the Call Home function.</td>
</tr>
<tr>
<td>callhome test</td>
<td>Sends a dummy test message to the configured destination(s).</td>
</tr>
<tr>
<td>show callhome</td>
<td>Displays configured Call Home information.</td>
</tr>
</tbody>
</table>
**terminal verify-user**

To verify the command and do not execute, use the `terminal verify-user` command.

```plaintext
terminal verify-user username {name}
```

### Syntax Description

- **username**: Specifies user name for AAA authorization.
- **name**: Specifies command to be authorized.

### Defaults

None.

### Command Modes

EXEC mode.

### Command History

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

### Usage Guidelines

You can verify the authorization profile for different commands. When enabled, all the commands are directed to the Access Control Server (ACS) for verification. The verification details are displayed once the verification is completed.

### Examples

The following example shows how to verify if the authorization settings are correct or not:

```plaintext
switch# terminal verify-only username user1
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# feature telnet
% Success
switch(config)# feature ssh
%Authorization Failed
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show aaa authorization all</td>
<td>Displays all authorization information.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show trunk protocol</td>
<td>Displays the trunk protocol status.</td>
</tr>
</tbody>
</table>

tune

To configure the tune IOA parameters, use the `tune` command. To delete the tune IOA parameter, use the `no` form of the command.

```plaintext
tune { lrtp-retx-timeout msec | round-trip-time ms | ta-buffer-size KB | timer load-balance { global | target seconds | rscn-suppression seconds | wa-buffer-size MB | wa-max-table-size KB } }
no tune { lrtp-retx-timeout msec | round-trip-time ms | ta-buffer-size KB | timer load-balance { global | target seconds | rscn-suppression seconds | wa-buffer-size MB | wa-max-table-size KB } }
```

**Syntax Description**

- **lrtp-retx-timeout msec**: Specifies LRTP retransmit timeout in milliseconds. The value can vary from 500 to 5000 msec. 2500 msec is the default.
- **round-trip-time ms**: Specifies round-trip time in milliseconds. The value can vary from 1 to 100 ms. 15 ms is the default.
- **ta-buffer-size KB**: Specifies tape acceleration buffer size in KB. The value can vary from 64 to 12288.
- **timer**: Specifies tune IOA timers.
- **load-balance**: Specifies IOA load-balance timers.
- **global seconds**: Specifies global load-balancing timer value. The value can vary from 5 to 30 seconds. 5 seconds is the default.
- **target seconds**: Specifies target load-balancing timer value. The value can vary from 2 to 30 seconds. 2 seconds is the default.
- **rscn-suppression seconds**: Specifies IOA RSCN suppression timer value. The value can vary from 1 to 10 seconds. 5 seconds is the default.
- **wa-buffer-size MB**: Specifies write acceleration buffer size in MB. The value can vary from 50 to 100 MB. 70 MB is the default.
- **wa-max-table-size KB**: Specifies Write Max Table size in KB. The value can vary from 4 to 64 KB. 4 KB is the default.

**Defaults**

None.

**Command Modes**

Configuration submode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>NX-OS 4.2(1)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None.

**Examples**

The following example shows how to configure a IOA RSCN suppression timer value:
tune

switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ioa cluster tape_vault
switch(config-ioa-cl)# tune timer rscn-suppression 1

The following example shows how to configure an IOA target load-balance timer value:

switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ioa cluster tape_vault
switch(config-ioa-cl)# tune timer load-balance target 2

The following example shows how to configure a global IOA target load-balance timer value:

switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ioa cluster tape_vault
switch(config-ioa-cl)# tune timer load-balance global 5

The following example shows how to configure the round-trip time in milliseconds:

switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ioa cluster tape_vault
switch(config-ioa-cl)# tune round-trip-time 15

The following example shows how to configure the tape acceleration buffer size in KB:

switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ioa cluster tape_vault
switch(config-ioa-cl)# tune ta-buffer-size 64

The following example shows how to configure the write acceleration buffer size in MB:

switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ioa cluster tape_vault
switch(config-ioa-cl)# tune wa-buffer-size 15

The following example shows how to configure the write Max Table Size in KB:

switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ioa cluster tape_vault
switch(config-ioa-cl)# tune wa-max-table-size 4

The following example shows how to configure the LRTP retransmit timeout in milliseconds:

switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ioa cluster tape_vault
**Send documentation comments to mdsfeedback-doc@cisco.com**

```plaintext
switch(config-ioa-cl)# tune lrtp-retx-timeout 2500
switch(config-ioa-cl)#
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flowgroup</td>
<td>Configures IOA flowgroup.</td>
</tr>
</tbody>
</table>
tune-timer

To tune the Cisco SME timers, use the `tune-timer` command. To disable this command, use the `no` form of the command.

```
tune-timer {global_lb_timer global_lb_timer_value | rscn_suppression_timer rscn_suppression_timer_value | tgt_lb_timer tgt_lb_timer_value}

no tune-timer {global_lb_timer global_lb_timer_value | rscn_suppression_timer rscn_suppression_timer_value | tgt_lb_timer tgt_lb_timer_value}
```

**Syntax Description**

- `global_lb_timer`: Specifies the global load-balancing timer value.
  - `global_lb_timer_value`: Identifies the timer value. The range is from 5 to 30 seconds. The default value is 5 seconds.
- `rscn_suppression_timer`: Specifies the Cisco SME Registered State Change Notification (RSCN) suppression timer value.
  - `rscn_suppression_timer_value`: Identifies the timer value. The range is from 1 to 10 seconds. The default value is 5 seconds.
- `tgt_lb_timer`: Specifies the target load-balancing timer value.
  - `tgt_lb_timer_value`: Identifies the timer value. The range is from 2 to 30 seconds. The default value is 2 seconds.

**Defaults**

None.

**Command Modes**

Cisco SME cluster configuration submode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3(1a)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `tune-timer` command is used to tune various Cisco SME timers such as the RSCN suppression, global load balancing and target load-balancing timers. These timers should be used only in large scaling setups. The timer values are synchronized throughout the cluster.

**Examples**

The following example configures a global load-balancing timer value:
```
switch# config t
switch(config)## sme cluster cl
switch(config-sme-cl)# tune-timer tgt_lb_timer 6
switch(config-sme-cl)#
```

The following example configures a Cisco SME RSCN suppression timer value:
```
switch# config t
switch(config)## sme cluster cl
```
The following example configures a target load-balancing timer value:

```
switch# config t
switch(config)# sme cluster cl
switch(config-sme-cl)# tune-timer rscn_suppression_timer 2
switch(config-sme-cl)#
```