T Commands

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.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	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.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	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.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	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. To disable this feature, use the **no** form of the command.

tacacs+ enable
no tacacs+ enable

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
NX-OS 4.1(1b)	This command was deprecated.

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:

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

Related Commands

Command	Description
show tacacs+	Displays TACACS+ server information.

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

time	Specifies the time interval in minutes. The range is 1 to 1440.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

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

Command	Description
deadtime	Sets a time interval for monitoring a nonresponsive TACACS+ server.
show tacacs-server	Displays all configured TACACS+ server parameters.

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.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

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

Command	Description
show tacacs-server	Displays all configured TACACS+ server parameters.
show tacacs-server directed request	Displays a directed request TACACS+ server configuration.

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-nameipv4-addressipv6-address*} [**key** [{**0** | **7**}] *shared-secret*] [**port** *port-number*] [**test** {**idle-time time** | **password password** | **username name**}] [**timeout** *seconds*]
no tacacs-server host {*server-nameipv4-addressipv6-address*} [**key** [{**0** | **7**}] *shared-secret*] [**port** *port-number*] [**test** {**idle-time time** | **password password** | **username name**}] [**timeout** *seconds*]

Syntax Description

server-name	Specifies the TACACS+ server DNS name. The maximum character size is 253.
ipv4-address	Specifies the TACACS+ server IP address. in the format *A.B.C.D* .
ipv6-address	Specifies the TACACS+ server IP address in the format *X:X::X* .
key	(Optional) Configures the TACACS+ server's shared secret key.
0	(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.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the TACACS+ client and server.
shared secret	(Optional) Configures a preshared key to authenticate communication between the TACACS+ client and server.
port *port-number*	(Optional) Configures a TACACS+ server port for authentication. The range is 1 to 65535.
test	(Optional) Configures parameters to send test packets to the TACACS+ server.
idle-time*time*	(Optional) Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.
password*password*	(Optional) Specifies a user password in the test packets. The maximum size is 32.
username*name*	(Optional) Specifies a user name in the test packets. The maximum size is 32.
timeout	(Optional) Configures a TACACS+ server timeout period.
seconds	(Optional) Specifies the timeout (in seconds) between retransmissions to the TACACS+ server. The range is 1 to 60 seconds.

Command Default

Idle-time is not set. Server monitoring is turned off.Timeout is 1 second.Username is test.Password is test.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Added the *ipv6-address* argument and the **test** option.

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

Command	Description
show tacacs-server	Displays TACACS+ server information.
tacacs+ enable	Enables 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	Specifies a global TACACS+ shared secret.
0	(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.
7	(Optional) 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.

Command Default

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

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

tacacs-server test

To configure a parameter to send test packets, use the tacacs-server test command. To disable this feature, use the no form of the command.

`tacacs-server test {{username` *username* `|{[password` *password* `[idle-time` *time*`]]|[idle-time` *time*`]}}|password` *password* `[idle-time` *time*`]|idle-time` *time*`}`

`no tacacs-server test {{username` *username* `|{[password` *password* `[idle-time` *time*`]]|[idle-time` *time*`]}}|password` *password* `[idle-time` *time*`]|idle-time` *time*`}`

Syntax Description

username	Specifies the username in test packets.
username	Specifies user name. The maximum size is 32 characters.
password	(Optional) Specifies the user password in test packets.
password	Specifies the user password. The maximun size is 32 characters.
idle-time	(Optional) Specifies the time interval for monitoring the server.
time period	Specifies the time period in minutes. The range is from 1 to 4440.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

Defaults will be used for anything not provided by CLI. Also doing a "no" of any parameters will revert it back to default.

Examples

The following example shows how to display the username in test packets:

```
switch# config t
switch(config)# tacacs-server test username test idle-time 0
switch(config)# tacacs-server test username test password test idle-time 1
switch(config)#
```

The following example shows how to display the time interval for monitoring the server:

```
switch(config)# tacacs-server test idle-time 0
switch(config)#
```

The following example shows how to display the user password in test packets:

```
switch(config)# tacacs-server test password test idle-time 0
switch(config)#
```

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 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.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(2)	This command was introduced.

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+.

tag

To correlate multiple events in an event manager applet, use the **tag** command. To remove the correlation, use the **no** form of the command.

tag tagname1 { **and** | **andnot** | **or** } **tagname2** [{ **and** | **andnot** | **or** } *tagname3* [{ **and** | **andnot** | **or** } *tagname4*]] **happens occurs in seconds**
no tag tagname1 { **and** | **andnot** | **or** } **tagname2** [{ **and** | **andnot** | **or** } *tagname3* [{ **and** | **andnot** | **or** } *tagname4*]] **happens occurs in seconds**

Syntax Description

tagname	The tag name of a tagged event. A maximum of 4 tag names may be specified. A tag name may comprise of any alphanumeric character (a-z, 0-9). The maximum length is 29 characters.
and	(Optional) Specifies to evaluate tagged events using boolean *and* logic.
andnot	(Optional) Specifies to evaluate tagged events using boolean *andnot* logic.
or	(Optional) Specifies to evaluate tagged events using boolean *or* logic.
happens	Specifies the number of occurrences of the tag combination that must occur before executing the applet actions.
occurs	Numbers of times the event combination occurs. The range is from 1 to 4294967295.
in	Specifies the number of occurrences that must occur within the given time period.
seconds	Maximum amount of time, in seconds, within which the complete event combination occurs. The range is from 0 to 4294967295 seconds.

Command Default

None

Command Modes

config-applet

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Tag names have scope only within the policy they are defined in. Tag names must be already configured in **event** commands before they can be used in a **tag** command.The evaluation of tag logic operators is from left to right since all operators are of equal precedence, that is:

```
((tagA operation1 tagB) operation2 tagC) operation3 tagD
```

When a **cli match** event is tagged, the behavior changes compared to untagged **cli match** events. Commands matching a tagged **cli match** event are executed immediately. If this were not the case, there may be a delay while waiting for other tagged events to match before an **event-default** command in the applet action block is executed.

Examples

The following example shows how to use the tag command. The goal in this example is to save the latest core dump to bootflash (it could also be sent to an SFTP server etc). The first policy is triggered when a process crash is about to generate a core file. It sleeps for 60 seconds while the core file is generated and then increments a counter. The second policy monitors the counter as well as system switchover events. If the counter is greater than 0 and no switchovers have occurred in the last 60 seconds then the latest core file is copied to bootflash and the counter reset to 0. No **exit-op** is specified for the counter so that the second policy can be triggered multiple times at once.

```
switch# configure terminal
switch(config)# event manager applet coreDump
switch(config-applet)# event syslog pattern "SERVICE_CRASHED.*core will be saved"
switch(config-applet)# action 10 cli local sleep 60
switch(config-applet)# action 20 counter name cores value 1 op inc
switch(config-applet)# event manager applet saveCore
switch(config-applet)# exit
switch(config)# event manager applet saveCore
switch(config-applet)# event counter tag coreDumped name cores entry-val 0 entry-op gt
switch(config-applet)# event syslog tag swDone pattern "SWITCHOVER_OVER"
switch(config-applet)# tag coreDumped andnot swDone happens 1 in 60
switch(config-applet)# action 10 cli local sh core | last 1 | sed 's/ \+/ /g' | sed
's_\([0-9]\+\) \([0-9]\+\) .* \([0-9]\+\) .*_copy core://\1/\3/\2 bootflash:_' | vsh
switch(config-applet)# action 20 counter name cores value 0 op set
switch(config-applet)# exit
```

Command	Description
action	Configures a command to be executed when an Embedded Event Manager (EEM) applet is triggered.
event	Configures a detectable condition for an EEM applet.
event manager applet	Registers an EEM applet with the EEM.

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.

Command Default

Displays the last 10 lines.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

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.

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.

Command Default

None.

Command Modes

Cisco SME cluster configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

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

Command	Description
clear sme	Clears Cisco SME configuration.
show sme cluster	Displays information about the Cisco SME cluster.
show sme cluster tape	Displays information about all tape volume groups or a specific group.

tape-bkgrp

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.

Command Default

None.

Command Modes

Cisco SME cluster configuration mode submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

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 c1
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 c1
switch(config-sme-cl)# no tape-bkgrp group1
switch(config-sme-cl-tape-bkgrp)#
```

Related Commands

Command	Description
clear sme	Clears Cisco SME configuration.
show sme cluster	Displays information about the Cisco SME cluster

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

device name	Specifies the name of the tape device.

Command Default

None.

Command Modes

Cisco SME tape volume configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

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 c1
switch(config-sme-cl)# tape-bkgrp group1
switch(config-sme-cl-tape-bkgrp)# tape-device devicename1
switch(config-sme-cl-tape-bkgrp-tapedevice)#
```

The following example removes a crypto tape device:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# tape-bkgrp group1
switch(config-sme-cl-tape-bkgrp)# no tape-device devicename1
switch(config-sme-cl-tape-bkgrp-tapedevice)#
```

Related Commands

Command	Description
clear sme	Clears Cisco SME configuration.
show sme cluster	Displays information about the Cisco SME cluster
show sme cluster tape	Displays information about all tape volume groups or a specific group

tape-keyrecycle

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.

Command Default

None.

Command Modes

Cisco SME cluster configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

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 c1
switch(config-sme-cl)#tape-keyrecycle
```

The following example disables tape key recycling:

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

Related Commands

Command	Description
clear sme	Clears Cisco SME configuration.
show sme cluster	Displays information about the Cisco SME cluster

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.

Command Default

Filemark frequency: 0.

Command Modes

SAN extension N port configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

To stop a continuous SCSI tape read 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 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
switch(san-ext-nport)# tape-
read command-id 100 target 22:22:22:22:22:22:22:22 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
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
```

```
switch(san-ext-nport)# tape-
read command-id 100 target 22:22:22:22:22:22:22:22 transfer-size 512000 continuous
filemark-frequency 32
```

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.
stop	Cancels a SCSI command in progress on a SAN extension tuner N port.

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.

tape-volgrp group name
no tape-volgrp group name

Syntax Description

group name	Specifies the tape volume group name.

Command Default

None.

Command Modes

Cisco SME crypto backup tape group configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

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:

```
switch# config t
switch(config))# sme cluster c1
switch(config-sme-cl)# tape-bkgrp tbg1
switch(config-sme-cl-tape-bkgrp)# tape-volgrp tv1
switch(config-sme-cl-tape-bkgrp-volgrp)#
```

The following example removes a crypto tape volume group:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# tape-bkgrp tbg1
switch(config-sme-cl-tape-bkgrp)# no tape-volgrp tv1
```

Related Commands

Command	Description
clear sme	Clears Cisco SME configuration.
show sme cluster tape	Displays information about tapes

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** *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.

Command Default

Filemark frequency: 0.

Command Modes

SAN extension N port configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

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 pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet 1/2
switch(san-ext-nport)# tape-
write command-id 100 target 22:22:22:22:22:22:22:22 transfer-size 512000 num-transactions
5000000 filemark-frequency 32
```

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

```
switch(san-ext-nport)# tape-
write command-id 100 target 22:22:22:22:22:22:22:22 transfer-size 512000 continuous
filemark-frequency 32
```

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.
stop	Cancels a SCSI command in progress on a SAN extension tuner N port.

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.

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-pwwn** *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-pwwn** *pWWN*}] [**sec-vsan** *sec-vsan-id*] [**sec-lun** *LUN*] [**iqn-name** *target-name*]

Syntax Description

device-alias *device-alias*	Specifies the device alias of the Fibre Channel target.
pwwn *pWWN*	Specifies the pWWN of the Fibre Channel target. The format is *hh:hh:hh:hh:hh:hh:hh:hh* .
vsan	(Optional) Assigns VSAN membership to the initiator target.
vsan-id	(Optional) Specifies the VSAN ID. The range is 1 to 4093.
no-zone	(Optional) Indicates no automatic zoning.
trespass	(Optional) Enables trespass support.
revert-primary-port	(Optional) Reverts to the primary port when it comes back up.
fc-lun *LUN*	(Optional) Specifies the Fibre Channel LUN of the Fibre Channel target. The format is 0xhhhh[:hhhh[:hhhh[:hhhh]]]
iscsi-lun *LUN*	(Optional) Specifies the iSCSI LUN. The format is 0xhhhh[:hhhh[:hhhh[:hhhh]]].
sec-device-alias	(Optional) Specifies the device alias of the secondary Fibre Channel target.
target-device-alias	(Optional) Specifies the initiator's target device alias. The maximum size is 64.
sec-pwwn *pWWN*	(Optional) Specifies the pWWN of the secondary Fibre Channel target. The format is *hh:hh:hh:hh:hh:hh:hh:hh* .
sec-vsan	(Optional) Assigns VSAN membership to the initiator.
sec-vsan-id	(Optional) Specifies the VSAN ID. The range is 1 to 4093.
sec-lun LUN	(optional) Specifies the FC LUN of the secondary Fibre Channel target. The format is 0xhhhh[:hhhh[:hhhh[:hhhh]]].
iqn-name	(Optional) Specifies the name of the target.
target-name	Specifies the initiator's target name. The maximum size is 223.

Command Default

None.

Command Modes

iSLB initiator configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

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
```

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
```

Related Commands

Command	Description
islb initiator	Assigns an iSLB name and IP address to the iSLB initiator and enters iSLB initiator configuration submode.
show islb initiator	Displays iSLB CFS information.
show islb initiator detail	Displays detailed iSLB initiator information.
show islb initiator summary	Displays iSLB initiator summary information.

tclquit

To exit Tcl, use the **tclquit** command.

tclquit

Syntax Description

None.

Command Default

None.

Command Modes

Interactive Tcl shell and Tcl script.

Command History

Release	Modification
NX-OS 5.1(1)	This command was introduced.

Usage Guidelines

Terminates the current Tcl process. Synonym for the **exit** command.

Examples

The following example terminates the current interactive Tcl shell:

```
switch-tcl# tclquit
switch#
```

Related Commands

Command	Description
exit	End the Tcl application (for a list of standard Tcl commands, see the Tcl documentation).

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*	(Optional) Specifies the burstsize ranging from 10 to 100 KB.

Command Default

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

Release	Modification
1.3(4)	This command was introduced.

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.

Command	Description
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.

Command Default

60 seconds.

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

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. For Cisco MDS 9250i Multiservice Fabric Switch, the range is 1000 to 10000000.
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.

Command Default

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** = 10000 Mbps (10Gbps), **min-available-bandwidth** = 8000 Mbps, and **round-trip-time** =1 ms.

Command Modes

FCIP profile configuration submode.

iSCSI interface configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.
6.2(5)	The IPStorage support was increased to 10G on the Cisco MDS 9250i Multiservice Fabric Switch.
6.2(13)	The maximum bandwidth of iSCSI was increased to 10G.

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.

When configuring tcp bandwidth using the **tcp maximum-bandwidth-kbps** and **tcp minimum-bandwidth-kbps** commands, the value should not exceed the maximum speed of the physical IPStorage port.

The maximum and minimum tcp bandwidth of all the FCIP and iSCSI interfaces that are using a specific Gigabit Ethernet or IPStorage port should not exceed the maximum speed of the physical IPStorage port.

For optimal performance the minimum-bandwidth-kbps should be 80%-90% of the maximum-bandwidth-kbps.

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
```

The following example configures an iSCSI profile:

```
switch# configure terminal
switch(config)# interface iscsi 1/1-2
switch(config-if)#
```

The following example configures the maximum available bandwidth at 9000000 Kbps, the minimum slow start threshold as 8000000 Kbps, and the round trip time as 20 milliseconds:

```
switch(config-if)# tcp max-bandwidth-kbps 9000000 min-available-bandwidth-kbps 8000000
round-trip-time-ms 20
```

The following example configures the maximum available bandwidth at 9000000 Kbps, the minimum slow start threshold as 8000000 Kbps, and the round trip time as 20 milliseconds:

```
switch(config-if)# tcp max-bandwidth-kbps 9000000 min-available-bandwidth-kbps 8000000
round-trip-time-ms 20
```

The following example reverts to the factory defaults:

```
switch(config-if)# no tcp max-bandwidth-kbps 10000000 min-available-bandwidth-kbps 8000000
round-trip-time-ms 20
```

The following example configures the maximum available bandwidth at 5000000 Kbps, the minimum slow start threshold as 4000000 Kbps, and the round trip time as 200 microseconds:

```
switch(config-if)# tcp max-bandwidth-kbps 5000000 min-available-bandwidth-kbps 4000000
round-trip-time-ms 200
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.
show fcip profile	Displays FCIP profile information.
show interface iscsi	Displays the iSCSI configuration for the port along with the tcp maximum and minimum bandwidth configuration.

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. For Cisco MDS 9250i Multiservice Fabric Switch, the range is 1 to 10000.
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.

Command Default

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** = 10000 Mbps (10Gbps), **min-available-bandwidth** = 8000 Mbps, and **round-trip-time** =1 ms.

Command Modes

FCIP profile configuration submode.

iSCSI interface configuration submode

Command History

Release	Modification
1.1(1)	This command was introduced.
6.2(5)	The IPStorage support was increased to 10G on the Cisco MDS 9250i Multiservice Fabric Switch.
6.2(13)	The maximum bandwidth of iSCSI was increased to 10G.

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.

When configuring tcp bandwidth using the **tcp maximum-bandwidth-mbps** and **tcp minimum-bandwidth-mbps** commands, the value should not exceed the maximum speed of the physical IPStorage port.

The maximum and minimum tcp bandwidth of all the FCIP and iSCSI interfaces that are using a specific Gigabit Ethernet or IPStorage port should not exceed the maximum speed of the physical IPStorage port.

For optimal performance the minimum-bandwidth-mbps should be 80%-90% of the maximum-bandwidth-mbps.

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
```

The following example configures an iSCSI profile:

```
switch# configure terminal
switch(config)# interface iscsi 1/1-2
switch(config-if)#
```

The following example configures the maximum available bandwidth at 9000 Mbps, the minimum slow start threshold as 8000 Mbps, and the round trip time as 20 milliseconds:

```
switch(config-if)# tcp max-bandwidth-mbps 9000 min-available-bandwidth-mbps 8000
round-trip-time-ms 20
```

The following example reverts to the factory defaults:

```
switch(config-if)# no tcp max-bandwidth-mbps 10000 min-available-bandwidth-mbps 8000
round-trip-time-ms 20
```

The following example configures the maximum available bandwidth at 5000 Mbps, the minimum slow start threshold as 4000 Mbps, and the round trip time as 200 microseconds:

```
switch(config-if)# tcp max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4000
round-trip-time-ms 200
```

Related Commands

Command	Description
fcip profile	Configures FCIP profile parameters.

Command	Description
show fcip profile	Displays FCIP profile information.
show interface iscsi	Displays the iSCSI configuration for the port along with the tcp maximum and minimum bandwidth configuration.

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.

Command Default

Enabled.

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

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 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.

Command	Description
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.

Command Default

Enabled.

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

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 a lost segment, 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. From Cisco MDS NX-OS Release 9.4(2) and later releases, the range is from 50 to 5000 milliseconds. Prior to Cisco MDS NX-OS Release 9.4(2), the range is from 200 to 5000 milliseconds.

Command Default

200 milliseconds

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
9.4(2)	The default TCP minimum retransmit timeout is changed to 50 from 200 milliseconds. The TCP minimum retransmit time range is changed to 50 to 5000 milliseconds from 200 to 5000 milliseconds.
1.1(1)	This command was introduced.

Usage Guidelines

Do not set the value to less than the minimum round trip time (including maximum jitter or variance) of the FCIP link. Such a setting does not allow the segment Ack to reach the switch before the segment is retransmitted. This causes unecessarily high FCIP link usage.

Examples

The following example configures a FCIP profile and specifies the minimum TCP retransmit timeout for lost TCP segments:

```
switch# config terminal
switch(config)# fcip profile 5
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.
show interface fcip	Displays FCIP information including round trip time.

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*	(Optional) Specifies the PMTU reset timeout. The range is 60 to 3600 seconds.

Command Default

Enabled.

3600 seconds.

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	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 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.

Command	Description
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.

Command Default

Enabled

Command Modes

FCIP profile configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

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 s *ize*
no tcp send-buffer-size *size*

Syntax Description

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

Command Default

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

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

tcp-connections

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

tcp-connections number
no tcp-connections number

Syntax Description

number	Enters the number of connections. Accepted values are 2 and 5 (For Cisco MDS 9250i Switch only).

Command Default

Two TCP connections.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.
6.2(5)	Added a value, 5 for the number of TCP connections.

Usage Guidelines

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

Use the **tcp-connections** option to specify the number of TCP connections contained in an FCIP link.

Set the TCP connections to 2 when:

- Both ends or peers of the FCIP tunnel are on Cisco MDS 9222i Switches or Cisco MDS 9000 18/4-Port Multiprotocol Services Modules (MSM) or Cisco MDS 9000 16-Port Storage Services Nodes (SSN).
- One end of the FCIP tunnel is on Cisco MDS 9222i switch, Cisco MDS 9000 18/4-Port Multiprotocol Services Module (MSM), or Cisco MDS 9000 16-Port Storage Services Node (SSN) and the other end is on Cisco MDS 9250i Switch.

Set the TCP connections to 5 when:

- Both ends of the FCIP tunnel are on Cisco MDS 9250i Switches.

Note When both ends of the FCIP tunnel are on Cisco MDS 9250i Switches, the TCP connections can be set to either 2 or 5, we recommend to set the TCP connections to 5 for higher bandwidth.

Examples

The following example configures the TCP connections:

```
switch# config terminal
switch(config)# interface fcip 50
switch(config-if)# tcp-connections 2
switch(config-if)# no tcp-connections 2
```

Related Commands

Command	Description
show interface fcip number	Displays an interface state and statistics.
show running-config interface fcip number	Displays an interface configuration for a specified FCIP interface.

telemetry

To enter SAN Telemetry Streaming (STS) configuration mode, use the **telemetry** command. To exit STS configuration mode, use the **no** form of this command.

telemetry

no telemetry

Syntax Description

This command has no arguments or keywords.

Command Default

Telemetry configuration mode is disabled by default.

Command Modes

Configuration mode (config)

Command History

Release	Modification
8.3(1)	This command was introduced.

Examples

This example shows how to enter STS configuration mode:

```
switch# configure
switch(config)# telemetry
```

This example shows how to exit STS configuration mode:

```
switch# configure
switch(config)# no telemetry
```

Related Commands

Command	Description
feature telemetry	Enables the SAN Telemetry Streaming feature.
show running-config telemetry	Displays the existing telemetry configuration.
show telemetry	Displays telemetry configuration.

telnet

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

telnet {*hostnameip-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.

Command Default

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example 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 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.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

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 alias

To display and define command aliases for a user session, use the **terminal alias** command. To remove the alias definition, use the **no** form of this command.

terminal alias [**persist**] [*alias-name* *alias-definition*]
no terminal alias [**persist**] [*alias-name* *alias-definition*]

Syntax Description

persist	(Optional) Makes the setting persistent for the current and future sessions for the current user.
alias-name	(Optional) Alias name.
alias-definition	(Optional) Alias definition.

Command Default

Displays the command aliases available to the user session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Aliases that you define with the **terminal alias** command are only available to the current user. Other users cannot use these command aliases. To create aliases that other users can access, use the **cli alias name** command.

The alias setting applies only to the current user session. Use the **persist** keyword to change the setting for the current and future session for the current user.

Examples

This example shows how to define a command alias only for the current user session:

```
switch# terminal alias shint show interface brief
```

This example shows how to define a command alias to persist across a session for the current user:

```
switch# terminal alias persist shver show version
```

This example shows how to display the command aliases available to the current user session:

```
switch# terminal alias
CLI alias commands
==================
shint  :show interface brief
------------------
alias  :show cli alias
```

This example shows how to remove a temporary command alias for the user session:

```
switch# no terminal alias shint
```

Related Commands

Command	Description
cli alias name	Defines a command alias name.

terminal ask-on-term

To enable all confirmation questions on the terminal, use the **terminal ask-on-term** command. To disable all confirmation questions, use the **no** form of this command.

terminal ask-on-term *term*
no terminal ask-on-term *term*

Syntax Description

term	Name of the session where you want to enable or disable the confirmation questions.

Command Default

All confirmation questions are enabled by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Confirmation questions are used in NX-OS to confirm actions that may cause traffic disruption. The **no terminal ask-on-term** command disables even the confirmation questions that are prompted during a reload operation.

Examples

This example shows how to enable all confirmation questions on terminal pts/0 only:

```
switch# terminal ask-on-term pts/0
```

This example shows how to disable all confirmation questions on terminal pts/0 only:

```
switch# no terminal ask-on-term pts/0
```

Related Commands

Command	Description
show users	Displays current user sessions and terminal names.
terminal dont-ask	Disables the terminal from asking you confirmation statements.

terminal color

To change the colors that are used when displaying the commands and outputs on the CLI for a user session, use the **terminal color** command. To revert to the default color, use the **no** form of this command.

terminal color [**persist**]
no terminal color [**persist**]

Syntax Description

persist	(Optional) Makes the setting persistent for the current and future sessions for the current user.

Command Default

All CLI prompts, commands, and command outputs display in colors that are defined by the terminal emulator.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The **terminal color** command changes the CLI colors as follows:

- Displays the command prompt in green if the previous command was successful.
- Displays the command prompt in red if an error occurred in the previous command.
- Displays the command in blue.
- Displays output in the default color that is defined by the terminal emulator.

The terminal color setting applies only to the current user session. Use the **persist** keyword to change the setting for the current and future session for the current user.

Examples

This example shows how to enable the terminal display colors for the current user session:

```
switch# terminal color
```

This example shows how to enable the terminal display colors for the current and future sessions for the current user:

```
switch# terminal color persist
```

This example shows how to revert to the default for the current user session:

```
switch# no terminal color
```

This example shows how to revert to the default for the current and future sessions for the current user:

```
switch# no terminal color persist
```

terminal deep-help

To enable the display of syntax of all possible options of a given command, use the **terminal deep-help** command. To disable detailed help, use the **no** form of this command.

terminal deep-help
no terminal deep-help

Command Default

Detailed help is disabled by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

To invoke detailed help for a command, enter the command followed by simultaneously pressing the **Alt** and the **?** keys (the **Alt** key is the **option** key on Mac).

Examples

This example shows the possible options of the zoneset command:

```
switch# terminal deep-help
switch# zoneset alt-?
: zoneset distribute vsan <i0>
: zoneset export vsan <i0>
: zoneset import interface <if0> vsan <i0>
```

terminal dont-ask

To disable confirmation prompts on the CLI, use the **terminal dont-ask** command. To revert to the default, use the **no** form of this command.

terminal dont-ask [**persist**]
no terminal dont-ask [**persist**]

Syntax Description

persist	(Optional) Makes the setting persistent for the current and future sessions for the current user.

Command Default

Confirmation prompts are enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The terminal confirmation prompt setting applies only to the current user session. Use the **persist** keyword to change the setting for the current and future session for the current user.

Examples

This example shows how to disable the CLI confirmation prompts for the current user session:

```
switch# terminal dont-ask
```

This example shows how to disable the CLI confirmation prompts for the current and future sessions for the current user:

```
switch# terminal dont-ask persist
```

This example shows how to enable the terminal to ask confirmation statements:

```
switch# no terminal dont-ask
```

This example shows how to enable the CLI confirmation prompts for the current and future sessions for the current user:

```
switch# no terminal dont-ask persist
```

Related Commands

Command	Description
terminal ask-on-term	Enables all confirmation questions on the terminal.

terminal edit-mode vi

To enable VI style editing of CLI history commands, use the **terminal edit-mode** command. To revert to the default editing mode, use the **no** form of this command.

terminal edit-mode vi [**persist**]
no terminal edit-mode vi [**persist**]

Syntax Description

persist	(Optional) Makes the setting persistent for the current and future sessions for the current user.

Command Default

The command line edit mode is set to EMACS by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The following table provides information about the difference between EMACS and VI mode editing commands:

Command	EMACS	VI
Delete line backward	Ctrl-u	dd
Delete word	Ctrl-w	dw **Note** This command deletes a word when the cursor is placed at the beginning of the word.
Back character	Ctrl-b	h
Forward character	Ctrl-f	l
Beginning of line	Ctrl-a	0
End of line	Ctrl-e	$
Back one word	Esc, b	b
Forward one word	Esc, f	w
Delete character at the cursor	Ctrl-d	x
Replace character at the cursor	—	r

The edit mode setting applies only to the current user session. Use the **persist** keyword to change the setting for the current and future session for the current user.

Examples

This example shows how to change the edit mode for recalled commands to VI style for the current user session:

```
switch# terminal edit-mode vi
```

This example shows how to change the edit mode for recalled commands to VI style for the current and future session for the current user:

```
switch# terminal edit-mode vi persist
```

This example shows how to revert the edit mode for recalled command to EMACS style for the current user session:

```
switch# no terminal edit-mode vi
```

This example shows how to revert the edit mode for recalled command to EMACS style for the current and future sessions for the current user:

```
switch# no terminal edit-mode vi persist
```

terminal event-manager bypass

To bypass all EEM policies that use **event cli match** statements to trap specific CLI commands, use **terminal event-manager bypass** command. To revert, use the **terminal no event-manager bypass** command.

terminal event-manager bypass
terminal no event-manager bypass

Command Default

EEM policies that match CLI commands are effective.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command allows the user to run commands that may be blocked or redirected by EEM policies.

Examples

This example shows a simple event manger applet that matches a CLI command and how to the **terminal event-manager bypass** command allows the user to bypass the EEM policy completely.

```
switch# show running-config eem
event manager applet noClockDetail
event cli match "show clock detail"
action 10 syslog priority critical msg "blocking sh clock detail"
switch# show clock detail
% Command blocked by event manager policy
2019 Jan 1 12:33:44 switch %EEM_ACTION-2-CRIT: blocking sh clock detail
switch# terminal event-manager bypass
switch# show clock detail
Time source is NTP
12:33:55 CET Fri Jan 01 2019
summer-time configuration:
--------------------------
timezone name: CEST
Starts : 5 Sun Mar at 02:00 hours
Ends : 5 Sun Oct at 02:00 hours
Minute offset:
```

This example shows how to restore matching of CLI commands by EEM policies:

```
switch# no terminal event-manager bypass
```

Related Commands

Command	Description
show running-config eem	Displays EEM policy configurations.

terminal exec prompt timestamp

To configure printing timestamps before each CLI command is executed, use the **terminal exec prompt timestamp** command. To remove the configuration, use the **no** form of this command.

terminal exec prompt timestamp
no terminal exec prompt timestamp

Command Default

Timestamp is not shown in the command output.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This setting will automatically print CPU usage and timestamp information before each command is run. This can be helpful in debugging issues.

Examples

This example shows the extra information that is displayed when this command is enabled:

```
switch# terminal exec prompt timestamp
switch# show banner motd
CPU utilization for five seconds: 2%/0%; one minute: 2%; five minutes: 2%
Time source is NTP
12:38:11.777 CET Sun Jan 06 2019
User Access Verification
```

terminal history no-exec-in-config

To exclude EXEC commands from the command history in config mode, use the **terminal history no-exec-in-config** command. To revert to the default, use the **no** form of this command.

terminal history no-exec-in-config
no terminal history no-exec-in-config

Command Default

The CLI command history always includes EXEC commands in configuration mode.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

By default, the Cisco NX-OS CLI history recalls all commands from the current command mode and higher command modes. For example, if you are working in global configuration mode, the command recall keystroke shortcuts recall both EXEC mode and global configuration mode commands. Using the **terminal history no-exec-in-config** command, you can avoid recalling any higher mode commands when you are in a configuration mode.

terminal home

To move the cursor to the line 1 and column 1 of the screen without erasing the screen output, use the **terminal home** command.

terminal home

Command Default

The cursor stays at the current line.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

terminal length

To set the number of lines used by the screen output pager, use the **terminal length** command. To revert to the default number of lines, use the **no** form of this command.

terminal length *lines*
terminal no length

Syntax Description

lines	Number of lines to display. Range is from 0 to 512. Enter 0 to disable paging.

Command Default

If the terminal emulator does not specify a screen length, then the default length is set to 24 lines. Most modern terminals propagate their window length to the switch so that the switch will automatically page output to match the number of lines of the user's window.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

If a command output exceeds the number of terminal lines, the session pauses after displaying the number of lines set in the terminal length. Press the space bar to display another screen of lines or press the **Enter** key to display another line. To return to the command prompt, press **Ctrl-C**.

The terminal length setting applies only to the current session.

Examples

This example shows how to set the number of lines of command output to display on the terminal before pausing:

```
switch# terminal length 28
```

This example shows how to revert to the default number of lines:

```
switch# terminal no length
```

Related Commands

Command	Description
show terminal	Displays the terminal session configuration.
terminal width	Sets the number of character columns for the current terminal session.

terminal monitor

To automatically display new syslog messages to the current session, use the **terminal monitor** command.

terminal monitor

Command Default

Logs are printed to the console session and no logs are printed to terminal sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command is helpful for monitoring of unexpected events during changes or debug messages during debugging. Be careful if this command is used for monitoring debugging as the session or system may be overloaded by the number of messages printed.

Related Commands

Command	Description
logging level	Configure different logging level for each facility.
show logging level	Displays the logging level of each syslog facility.

terminal output xml

To set the command output formatting to XML, use the **terminal output xml** command. To set the default output formatting, use the **no** form of this command.

terminal output xml [{**1.0***NX-OS-version*}]
no terminal output xml [{**1.0***NX-OS-version*}]

Syntax Description

1.0	(Optional) XML version 1.0.
NX-OS-version	(Optional) Specifies the XML version depending on the Cisco NX-OS version that is installed on your switch.

Command Default

Command outputs are in free form text for human consumption.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command is useful for scripts or other services that expect XML formatted output from CLI commands.

Examples

This example shows how to set the command output formatting to XML:

```
switch# terminal output xml
```

This example shows how to set the command output formatting to XML version 1.0:

```
switch# terminal output xml 1.0
```

This example shows how to set the command output formatting to XML version 8.1.1b:

```
switch# terminal output xml 8.1.1b
```

This example shows how to set the command output formatting to default:

```
switch# no terminal output xml
```

Related Commands

Command	Description
show terminal output xml version	Displays currently used XML version.

terminal password

To assign a password to be used in the **copy** {**ftp** | **scp** | **sftp**} commands, use the **terminal password** command. To remove the password, use the **no** form of this command.

terminal password
no terminal password

Command Default

There is no password set for the **copy** {**ftp** | **scp** | **sftp**} commands.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The password that is configured by this command is not restricted to the current username. It will be used for the user specified in any **copy** command, which allows another user other than the current user to be given.

This command has two modes: inline and interactive. In the inline mode, the password is echoed on the screen. In the interactive mode, the password is not echoed. To use interactive mode, type the help character ? instead of a password. When prompted, enter the desired password.

This command is not stored in the switch configuration and is not persistent between logins.

Examples

This example shows how to configure a password in inline mode:

```
switch# terminal password myScpFtpPassword
```

This example shows how to configure a password to be used in the **copy** {**scp** | **ftp** | **sftp**} commands:

```
switch# terminal password?
enter password and type return
```

This example shows how to remove the password that is configured for the **copy** {**scp** | **ftp** | **sftp**} commands:

```
switch# no terminal password
```

Related Commands

Command	Description
copy	Copy a file.

terminal redirection-mode

To configure the file format of the **show** command output that is redirected to a file, use the **terminal redirection-mode** command.

terminal redirection-mode {**ascii** | **zipped**}

Syntax Description

ascii	Sets the redirection mode to ASCII.
zipped	Sets the redirection mode to gzip.

Command Default

The file format of redirected the **show** command output is set to ASCII by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Some of the **show** commands have lengthy outputs, especially **show** commands for debugging such as the **show tech-support** command. You can use the **terminal redirection-mode** command to reduce the size of the file when you redirect the output from the command.

The terminal redirection mode setting applies only to the current session.

Examples

This example shows how automatic zipping of redirected output works. The mode is set to zip, a file is created and then unzipped. The size of each file is checked.

```
switch# terminal redirection-mode zipped
switch# show tech-support acl > shTechAcl.gz
switch# dir shTechAcl.gz
16346 Jan 01 12:34:56 2010 shTechAcl.gz
switch# gunzip shTechAcl.gz
switch# dir shTechAcl
236449 Jan 01 12:34:56 2010 shTechAcl
```

This example shows how to configure ASCII format for the terminal redirection mode:

```
switch# terminal redirection-mode ascii
```

terminal session-timeout

To set the terminal inactivity timeout period for the current session, use the **terminal session-timeout** command.

terminal session-timeout *minutes*

Syntax Description

minutes	Session timeout period in minutes. Range is 0 to 525600.

Command Default

Session timeout is disabled by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

A value of 0 minutes disables the session timeout.

The terminal session inactivity timeout setting applies only to the current session.

Examples

This example shows how to configure the terminal session timeout period to 1 minute:

```
switch# terminal session-timeout 1
```

This example shows how to disable the terminal session timeout:

```
switch# terminal session-timeout 0
```

Related Commands

Command	Description
show terminal	Displays the terminal session configuration.

terminal sticky-mode

To search for a command match in the current mode only, use the **terminal sticky-mode** command.

terminal sticky-mode
terminal no sticky-mode

Command Default

The current mode and all higher modes are searched for matching commands.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Examples

This example shows how commands are constrained to the current mode when this setting is enabled:

```
switch# configure
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# show clock?
*** No matching command found in current mode, matching in (exec) mode ***
  clock  Display current Date
switch(config)# exit
switch# terminal sticky-mode
switch# configure
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# show clock?
 ^
% Invalid command at '^' marker.
```

terminal terminal-type

To set the terminal type, use the **terminal terminal-type** command. To revert to the default type, use the **no** form of this command.

terminal terminal-type *type*
terminal no terminal-type

Syntax Description

type	Sets the terminal type. Maximum length is 80 characters. The supported types are: • ansi • dumb • linux • rxvt • screen • sun • vt100 • vt102 • vt200 • vt220 • vt52 • xterm • xterm-256color • xterm-color • xterm-xfree86

Command Default

The default terminal type is ansi.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Examples

This example shows how to set the terminal type to *xterm* :

```
switch# terminal terminal-type xterm
```

This example shows how to revert to the default terminal type:

```
switch# terminal no terminal-type
```

Related Commands

Command	Description
show terminal	Displays the terminal session configuration.

terminal time

To save the current time to a variable, use the **terminal time** command.

terminal time [*variable*] [**delta**]

Syntax Description

variable	(Optional) Variable name to store the time.
delta	(Optional) Displays the delta time to the currently saved time value.

Command Default

Current time is not saved.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Examples

This example shows how to save the current time to a variable:

```
switch# terminal time t1
```

This example shows how to display the delta time to the currently saved time:

```
switch# terminal time t1 delta
```

terminal verify-only

To verify if a user is permitted to run given commands, use the **terminal verify-only** command.

terminal verify-only [**username** *name*]
terminal no verify-only [**username** *name*]

Syntax Description

username	(Optional) Specifies a user.
name	(Optional) Specifies a username.

Command Default

Remote users are restricted from verifying commands.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

When configured, this command changes the CLI mode to verify if a given command is allowed to be executed but does not execute the command. The full command to be tested should be given. If a username is specified, the tests are for the specified user and not for the current user. Issue the **no** option to revert to normal command execution mode.

Examples

This example shows how to verify if the current user can execute the show clock command:

```
switch# terminal verify-only

switch# show clock
% Success
```

This example shows how to test which commands the user 'a123456' may execute:

```
switch# terminal verify-only username a123456
```

Related Commands

Command	Description
aaa authorization	Configures authorization.
show user-account	Displays information of switch users.

terminal width

To set the number of character columns for the current terminal session, use the **terminal width** command. To revert to the default, use the **no** form of this command.

terminal width *columns*
terminal no width

Syntax Description

columns	Number of columns. The range is from 24 to 511.

Command Default

If the terminal emulator does not specify a screen width, then the default number of character columns is 80. Most modern terminals propagate their window width to the switch so that the switch will automatically page output to match the width of the users window.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

The terminal width setting applies only to the current session.

Examples

This example shows how to set the number of columns to display on the terminal:

```
switch# terminal width 70
```

This example shows how to revert to the default number of columns:

```
switch# terminal no width
```

Related Commands

Command	Description
show terminal	Displays the terminal session configuration.
terminal length	Sets the number of lines on a screen for the current terminal session.

test aaa authorization

To verify if the authorization settings are correct or not, use the test aaa authorization command.

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

Syntax Description

command-type	Specifies the command type. You can use the keywords for the command type.
commands	Specifies authorization for all commands.
config-commands	Specifies authorization for configuration commands.
user	Specifies the user to be authorized. The maximum size is 32.
username	Specifies the user to be authorized.
cmd	Specifies command to be authorized.

Command Default

None.

Command Modes

EXEC mode.

Command History

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

Usage Guidelines

None.

Examples

```
The following example shows how to verify if the authorization setting s are correct or
not:
switch(config)# test aaa authorization command-type commands user u1 command "feature dhcp"
% Success
switch(config)#
```

Related Commands

Command	Description
show aaa authorization all	Displays all authorization information.

test pfm snmp test-trap fan

To generate a test SNMP trap for fan 1, use the **test pfm snmp test-trap fan** command.

test pfm snmp test-trap fan

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **test pfm snmp test-trap fan** command to generate a test SNMP trap message for fan 1 with status OK. The test traps are sent to all the configured trap receivers. You can configure a trap reciever by using the **snmp-server host** *ip-address* **traps version** command. This can be used to verify if the trap receivers are correctly configured to receive the traps.

Ensure that all the required SNMP trap receivers are configured with the **snmp-server host** *ip-address* **traps** command, before executing the **test pfm snmp test-trap fan** command.

Examples

The following example is one of the methods to verify the test SNMP trap messages for a fan in a device:

```
switch# test pfm snmp test-trap fan

pfm_cli_test_snmp_trap_fan: Sent dummy/test FAN SNMP Trap

!Check trap messages in the Device Manager Log!
2019.08.07 00:17:47 [snmp.trap] 00:17:47 10.106.29.18, 605 TRAP c=public
sysUpTime.0=7536993, snmpTrapOID.0=connUnitFabricID,
connUnitStatus.32.0.0.222.251.177.121.208.0.0.0.0.0.0.0.0=4,
connUnitState.32.0.0.222.251.177.121.208.0.0.0.0.0.0.0.0=2
2019.08.07 00:17:47 [snmp.trap] TrapChannel queueing 00:17:47 10.106.29.18, 605 TRAP
c=public sysUpTime.0=7536993, snmpTrapOID.0=connUnitFabricID,
connUnitStatus.32.0.0.222.251.177.121.208.0.0.0.0.0.0.0.0=4,
connUnitState.32.0.0.222.251.177.121.208.0.0.0.0.0.0.0.0=2
2019.08.07 00:17:47 [snmp.trap] 00:17:47 10.106.29.18, 606 TRAP c=public
sysUpTime.0=7537002, snmpTrapOID.0=cefcFanTrayStatusChange, cefcFanTrayOperStatus.534=2
2019.08.07 00:17:47 [snmp.trap] TrapChannel queueing 00:17:47 10.106.29.18, 606 TRAP
c=public sysUpTime.0=7537002, snmpTrapOID.0=cefcFanTrayStatusChange,
cefcFanTrayOperStatus.534=2
```

Related Commands

Command	Description
snmp-server host *ip-address* **traps version**	Sends SNMP traps to the configured hosts.
test pfm snmp test-trap powersupply	Displays the test SNMP traps to monitor power supply.

Command	Description
test pfm snmp test-trap temp_sensor	Displays the test SNMP traps to monitor tempertaure settings.

test pfm snmp test-trap powersupply

To generate a test SNMP trap for power supply on a Cisco device, use the **test pfm snmp test-trap powersupply** command.

test pfm snmp test-trap powersupply

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **test pfm snmp test-trap powersupply** command to generate a test SNMP trap message for power supply with status OK. The test traps are sent to all the configured trap receivers. You can configure a trap reciever by using the **snmp-server host** *ip-address* **traps version** command. This can be used to verify if the trap receivers are correctly configured to receive the traps.

Ensure that all the required SNMP trap receivers are configured with the **snmp-server host** *ip-address* **traps** command, before executing the **test pfm snmp test-trap powersupply** command.

Examples

The following example is one of the methods to verify the test SNMP trap messages for power supply in a device:

```
switch# test pfm snmp test-trap powersupply

pfm_cli_test_snmp_trap_powersupply: Sent dummy/test POW SNMP Trap

!Check trap messages in the Device Manager Log!
2019.08.07 00:45:35   [snmp.trap] 00:45:35 10.106.22.18, 620 TRAP c=public
sysUpTime.0=7703861, snmpTrapOID.0=connUnitFabricID,
connUnitStatus.32.0.0.222.251.177.121.208.0.0.0.0.0.0.0.0=4,
connUnitState.32.0.0.222.251.177.121.208.0.0.0.0.0.0.0.0=2
2019.08.07 00:45:35   [snmp.trap] TrapChannel queueing 00:45:35 10.106.22.18, 620 TRAP
c=public sysUpTime.0=7703861, snmpTrapOID.0=connUnitFabricID,
connUnitStatus.32.0.0.222.251.177.121.208.0.0.0.0.0.0.0.0=4,
connUnitState.32.0.0.222.251.177.121.208.0.0.0.0.0.0.0.0=2
2019.08.07 00:45:35   [snmp.trap] 00:45:35 10.106.22.18, 621 TRAP c=public
sysUpTime.0=7703871, snmpTrapOID.0=cefcPowerStatusChange, cefcFRUPowerOperStatus.470=5,
cefcFRUPowerAdminStatus.470=1
2019.08.07 00:45:35   [snmp.trap] TrapChannel queueing 00:45:35 10.106.22.18, 621 TRAP
c=public sysUpTime.0=7703871, snmpTrapOID.0=cefcPowerStatusChange,
cefcFRUPowerOperStatus.470=5, cefcFRUPowerAdminStatus.470=1
```

Related Commands

Command	Description
snmp-server host *ip-address* **traps version**	Sends SNMP traps to the configured hosts.
test pfm snmp test-trap fan	Displays the test SNMP traps to monitor fan traps.

Command	Description
test pfm snmp test-trap temp_sensor	Displays the test SNMP traps to monitor tempertaure settings.

test pfm snmp test-trap temp_sensor

To generate a test SNMP trap for temperature settings, use the **test pfm snmp test-trap temp_sensor** command.

test pfm snmp test-trap temp_sensor

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

Use the **test pfm snmp test-trap temp_sensor** command to generate a test SNMP trap message for temperature settings of a device. The test traps are sent to all the configured trap receivers. You can configure a trap reciever by using the **snmp-server host** *ip-address* **traps version** command. This can be used to verify if the trap receivers are correctly configured to receive the traps.

Ensure that all the required SNMP trap receivers are configured with the **snmp-server host** *ip-address* **traps** command, before executing the **test pfm snmp test-trap temp_sensor** command.

Examples

The following example is one of the methods to verify the test SNMP trap messages for temperature settings in a device:

```
switch# test pfm snmp test-trap temp_sensor

pfm_cli_test_snmp_trap_sensor: Sent dummy/test TEMP SNMP Trap

!Check trap messages in the Device Manager Log!
2019.08.07 00:50:33   [snmp.trap] 00:50:33 10.106.29.18, 622 TRAP c=public
sysUpTime.0=7733672, snmpTrapOID.0=entSensorThresholdNotification,
entSensorThresholdValue.21590.12=34, entSensorValue.21590=56,
entSensorThresholdSeverity.21590.12=10
2019.08.07 00:50:33   [snmp.trap] TrapChannel queueing 00:50:33 10.106.29.18, 622 TRAP
c=public sysUpTime.0=7733672, snmpTrapOID.0=entSensorThresholdNotification,
entSensorThresholdValue.21590.12=34, entSensorValue.21590=56,
entSensorThresholdSeverity.21590.12=10
```

Related Commands

Command	Description
snmp-server host *ip-address* **traps version**	Sends SNMP traps to the configured hosts.
test pfm snmp test-trap fan	Displays the test SNMP traps to monitor fan traps.
test pfm snmp test-trap powersupply	Displays the test SNMP traps to monitor power supply.

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.

Command Default

Disabled.

Command Modes

Scheduler job configuration submode.

Command History

Release	Modification
2.0(x)	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*	(Optional) Configures the acceptable time difference for timestamps in milliseconds. The range is 500 to 10000.

Command Default

Disabled.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

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

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. To disable the entries in an ALPA cache, use the no form of the 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.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(5)	This command was introduced.

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 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 [**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.

Command Default

None.

Command Modes

EXEC mode.

Command History

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

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# 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
```

transceiver-frequency

To set the interface clock to ethernet or Fibre Channel, use the transceiver-frequency command in interface configuration mode. To disable the ethernet clock for the port, use the no form of the command.

transceiver-frequency [**ethernet**] **force**
no transceiver-frequency [**ethernet**] **force**

Syntax Description

ethernet	(Optional) Specifies the ethernet transceiver frequency for an interface.
force	Specifies the force option.

Command Default

Fibre Channel.

Command Modes

Interface Configuration mode.

Command History

Release	Modification
5.0	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to set the interface clock to ethernet or Fibre Channel:

```
switch(config-if)# transceiver-frequency ethernet force
switch(config-if)#
```

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.

Command Default

None.

Command Modes

SAN extension N port configuration submode.

Command History

Release	Modification
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 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 e-mail address. For example: SJ-9500-1@xyz.com. The maximum length is 255 characters.
reply-to *email-address*	Specifies the reply to e-mail 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.

Command Default

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example 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 shows how to remove the callhome configuration for email smtp-server:

switch(config-callhome)# **transport email smtp-server none**

The following example configures the SMTP server and ports:

switch(config-callhome)# **transport email smtp-server**

```
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.

transport email mail-server

To configure an SMTP server address, use the transport email mail-server command. To disable this feature, use the no form of the command.

transport email mail-server {**ipv4** | **ipv6** | **hostname**} [**port** *port number*] [**priority** *priority number*]
no transport email mail-server {**ipv4** | **ipv6** | **hostname**} [**port** *port number*] [**priority** *priority number*]

Syntax Description

ipv4	Specifies IPV4 SMTP address.
ipv6	Specifies IPV6 SMTP address.
hostname	Specifies DNS or IPV4 or IPV6 address.
port port number	(Optional) Specifies SMTP server port. The range is from 1 to 65535.
priority priority number	(Optional) Specifies SMTP server priority. The range is from 1 to 100.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure an SMTP server port:

switch# callhome

```
switch(config-callhome)# transport email mail-server 192.168.10.23 port 4
switch# config t
```

The following example shows how to configure an SMTP server priority:

```
switch(config-callhome)# transport email mail-server 192.168.10.23 priority 60
switch# config t
```

Related Commands

Command	Description
callhome	Configures the Call Home function.

transport http proxy enable

To enable Smart Call Home to send all HTTP messages through the HTTP proxy server, use the transport http proxy enable command. To disable this feature, use the no form of the command.

transport http proxy enable
no transport http proxy enable

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Callhome Configuration mode.

Command History

Release	Modification
NX-OS 5.2(1)	This command was introduced.

Usage Guidelines

None.

Note You can execute this command only after the proxy server address has been configured.

Note The VRF used for transporting messages through the proxy server is the same as that configured using the transport http use-vrf command.

Examples

The following example shows how to enable Smart Call Home to send all HTTP messages through the HTTP proxy server:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.switch(config)# callhome
switch(config-callhome)# transport http proxy enable
Cannot enable proxy until configured
switch(config-callhome)#
```

Related Commands

Command	Description
callhome	Configures the Call Home function.

transport http proxy server

To configure proxy server address and port, use the transport http proxy server command. To disable this feature, use the no form of the command.

transport http proxy server *ip-address* [**port** *number*]
no transport http proxy server *ip-address* [**port** *number*]

Syntax Description

ip-address	HTTP Proxy server name or IP address (DNS name or IPv4 or IPv6 address)
port	(Optional) Specifies proxy server port.
number	(Optional) Port number. The range is from 1 to 65535.

Command Default

Default port number is 8080.

Command Modes

Callhome Configuration mode.

Command History

Release	Modification
NX-OS 5.2(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure proxy server address and port:

switch# config t

Enter configuration commands, one per line. End with CNTL/Z.switch(config)# callhome

switch(config-callhome)# transport http proxy server 192.0.2.1 port 2

switch(config-callhome)#

Related Commands

Command	Description
callhome	Configures the Call Home function.

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

Note Trunk protocol is enabled by default from Cisco MDS NX-OS Release 6.2(7) and later.

This command has no other arguments or keywords.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
6.2(7)	This command was deprecated.

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.

trustedcert

To set the trustedcert, use the trustedcert command. To disable this feature, use the no form of the command.

trustedcert attribute-name *attribute-name* **search-filter** *string* **base-DN** *string*
no trustedcert attribute-name *attribute-name* **search-filter** *string* **base-DN** *string*

Syntax Description

attribute-name attribute-name	Specifies LDAP attribute name. The maximum size is 128 characters.
search-filter	Specifies LDAP search filter. The maximum length is 128 characters.
string	Specifies search map search filter . The maximum length is 128 characters.
base-DN	Configure base DN to be used for search operation. The Maximum length is 63 characters.
string	Specifies search map base DN name. The Maximum length is 63 characters.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

```
The following example shows how to specify the LDAP trustcert :
switch(config)#ldap search-map s1
switch(config-ldap-search-map)# trusted attribute-name cACertificate
"(&(objectClass=certificationAuthority))" base-DN "CN=NTAuthCertificates,CN=Public Key
Services,CN=Services,CN=Configuration,DC=DCBU-ACS"
GROUP_NAME: map1
CRL
ATTR_NAME: map1
SEARCH_FLTR: map1
BASE_DN: DN1
Sending the SET_REQ
switch(config-ldap-search-map)#end
```

Related Commands

Command	Description
show ldap-server groups	Displays the configured LDAP server groups.

tune

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

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.

Command Default

None.

Command Modes

Configuration submode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to configure a IOA RSCN suppression 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 rscn-suppression 1
:switch(config-ioa-cl)#
```

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
switch(config-ioa-cl)#
```

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
switch(config-ioa-cl)#
```

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
switch(config-ioa-cl)#
```

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
switch(config-ioa-cl)#
```

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
switch(config-ioa-cl)#
```

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
switch(config-ioa-cl)#
```

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
```

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

switch(config-ioa-cl)#

Related Commands

Command	Description
flowgroup	Configures IOA flowgroup.

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_suppresion_timer_value** | **tgt_lb_timer** **tgt_lb_timer_value**}
no **tune-timer** {**global_lb_timer** **global_lb_timer_value** | **rscn_suppression_timer** **rscn_suppresion_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_suppresion_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.

Command Default

None.

Command Modes

Cisco SME cluster configuration submode.

Command History

Release	Modification
3.3(1a)	This command was introduced.

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 c1
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 c1
```

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

The following example configures a target load-balancing timer value:

```
switch# config t
switch(config))# sme cluster c1
switch(config-sme-cl)# tune-timer rscn_suppression_timer 2
switch(config-sme-cl)#
```