

R Commands

- radius abort, on page 3
- radius commit, on page 4
- radius distribute, on page 5
- radius-server deadtime, on page 6
- radius-server directed-request, on page 7
- radius-server host, on page 8
- radius-server key, on page 10
- radius-server retransmit, on page 11
- radius-server test, on page 12
- radius-server timeout, on page 14
- rate-mode bandwidth-fairness, on page 15
- rate-mode oversubscription-limit, on page 16
- read command-id, on page 18
- read-only, on page 19
- reload, on page 20
- renew lifetime, on page 22
- revocation-check, on page 23
- rlir preferred-cond fcid, on page 25
- rmdir, on page 27
- rmon alarm, on page 28
- rmon event, on page 30
- rmon hcalarm, on page 32
- role abort, on page 34
- role commit, on page 35
- role distribute, on page 36
- role name, on page 37
- rsakeypair, on page 39
- rscn, on page 41
- rscn abort vsan, on page 42
- rscn coalesce swrscn vsan, on page 43
- rscn commit vsan, on page 44
- rscn distribute, on page 45
- rscn event-tov, on page 46

- rscn permit type nport event switch-config, on page 48
- rspan-tunnel, on page 49
- rule, on page 50
- run-script, on page 51

radius abort

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

radius 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

None.

Examples

The following example shows how to discard a RADIUS CFS distribution session in progress:

```
switch# config terminal
switch(config)# radius abort
```

Related Commands

Command	Description
radius distribute	Enables CFS distribution for RADIUS.
show radius	Displays RADIUS CFS distribution status and other details.

radius commit

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

radius commit

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

After the "radius commit" is done the running configuration has been modified on all switches participating in radius distribution. You can then use the "copy running-config startup-config fabric" command to save the running-config to the startup-config on all the switches in the fabric.

Examples

The following example shows how to apply a RADIUS configuration to the switches in the fabric:

```
switch# config terminal
switch(config)# radius commit
```

Related Commands

Command	Description
radius distribute	Enables CFS distribution for RADIUS.
show radius	Displays RADIUS CFS distribution status and other details.

radius distribute

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

radius distribute
no radius 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

None.

Examples

The following example shows how to enable RADIUS fabric distribution:

```
switch# config terminal
switch(config)# radius distribute
```

Related Commands

Command	Description
radius commit	Commits temporary RADIUS configuration changes to the active configuration.
show radius	Displays RADIUS CFS distribution status and other details.

radius-server deadtime

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

radius-server deadtime *time*
no radius-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 RADIUS 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, RADIUS server monitoring is not performed unless the RADIUS 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)# radius-server deadtime 10
```

Related Commands

Command	Description
deadtime	Sets a time interval for monitoring a nonresponsive RADIUS server.
show radius-server	Displays all configured RADIUS server parameters.

radius-server directed-request

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

radius-server directed-request
no radius-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 RADIUS server to send authentication requests to when logging in:

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

Related Commands

Command	Description
show radius-server	Displays all configured RADIUS server parameters.
show radius-server directed request	Displays a directed request RADIUS server configuration.

radius-server host

To configure RADIUS server parameters, use the **radius-server host** command. Use the **no** form of this command to revert to the factory defaults.

radius-server host {*server-nameipv4-addressipv6-address*} [**key** [**0** | **7**] *shared-secret*] [**accounting**] [**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*] [**test** {**idle-time** *time* | **password** *password* | **username** *name*}] [**timeout** *seconds* [**retransmit** *count*]]
no radius-server host {*server-nameipv4-addressipv6-address*} [**key** [**0** | **7**] *shared-secret*] [**accounting**] [**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*] [**test** {**idle-time** *time* | **password** *password* | **username** *name*}] [**timeout** *seconds* [**retransmit** *count*]]

Syntax Description

server-name	Specifies the RADIUS server DNS name. Maximum length is 253 characters.
ipv4-address	Specifies the RADIUS server IP address in the format *A.B.C.D* .
ipv6-address	Specifies the RADIUS server IP address in the format *X:X::X* .
auth-port *port-number*	(Optional) Configures the RADIUS server port for authentication.
acct-port *port-number*	(Optional) Configures the RADIUS server port for accounting.
authentication	Configures authentication.
retransmit *count*	(Optional) Configures the number of times the switch tries to connect to a RADIUS server(s) before reverting to local authentication. The range is 1 to five times and the default is 1 time.
accounting	(Optional) Configures accounting.
key	(Optional) Configures the RADIUS server shared secret key.
0	(Optional) Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the RADIUS 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 RADIUS client and server.
shared-secret	Configures a preshared key to authenticate communication between the RADIUS client and server.
test	(Optional) Configures parameters to send test packets to the RADIUS server.
idle-time*time*	Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes.
password*password*	Specifies a user password in the test packets. The maximum size is 32.
username*name*	Specifies a user name in the test packets. The maximum size is 32.
timeout *seconds*	(Optional) Specifies the timeout (in seconds) between retransmissions to the RADIUS server. The default is 1 second and the valid 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
NX-OS 4.1(3)	Changed the command output.
1.0(2)	This command was introduced.
3.0(1)	Added the *ipv6-address* argument and the **test** option.

Usage Guidelines

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

Examples

The following example configures RADIUS server authentication parameters:

```
switch# config terminal
switch(config)# radius-server host 10.10.2.3 key HostKey
switch(config)# radius-server host 10.10.2.3 auth-port 2003

switch(config)# radius-server host 10.10.2.3 acct-port 2004
switch(config)# radius-server host 10.10.2.3 accounting
switch(config)# radius-server host radius2 key 0 abcd
switch(config)# radius-server host radius3 key 7 1234
switch(config)# radius-server host 10.10.2.3 test idle-time 10
switch(config)# radius-server host 1.1.1.1 test username user1 password pass idle-time 1
switch(config)# radius-server host 10.10.2.3 test username tester
switch(config)# radius-server host 10.10.2.3 test password 2B9ka5
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server key

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

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

Syntax Description

0	(Optional) Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the RADIUS 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 RADIUS client and server.
shared-secret	Configures a preshared key to authenticate communication between the RADIUS client and server.

Command Default

No RADIUS key is configured.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You need to configure the RADIUS preshared key to authenticate the switch to the RADIUS 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 RADIUS server configurations on the switch. You can override this global key assignment by explicitly using the **key** option in the **radius-server host** command. Global key configuration is exempted from CFS distribution.

Examples

The following examples provide various scenarios to configure RADIUS authentication:

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

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server retransmit

To globally specify the number of times the switch should try a request with a RADIUS server, use the **radius-server retransmit** command. To revert to default value, use the **no** form of the command.

radius-server retransmit *count*
no radius-server retransmit *count*

Syntax Description

count	Configures the number of times the switch tries to connect to a RADIUS server(s) before reverting to local authentication. The range is 1 to 5 times.

Command Default

1 retransmission

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures the number of retransmissions to 3:

```
switch# config terminal
switch(config)# radius-server retransmit 3
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server test

To configure the test parameter for an individual server, use the radius-server test command. To disable this feature, use the no form of the command.

radius-server test { {**username** *username* | {[**password** *password* [**idle-time** *time*]] | [**idle-time** *time*]}} | **password** *password* [**idle-time** *time*] | **idle-time** *time*}
no radius-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.
user name	Specifies the username. 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)# radius-server test username test idle-time 0
switch(config)# radius-server test username test password test idle-time 0
switch(config)#
```

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

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

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

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

Related Commands

Command	Description
show radius-server	Displays all configured RADIUS server parameters.

radius-server timeout

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

radius-server timeout *seconds*
no radius-server timeout *seconds*

Syntax Description

seconds	Specifies the time (in seconds) between retransmissions to the RADIUS server. The range is 1 to 60 seconds.

Command Default

1 second

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures the timeout value to 30 seconds:

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

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

rate-mode bandwidth-fairness

To enable or disable bandwidth fairness among ports in a port group, use the **rate-mode bandwidth-fairness** command in configuration mode. To disable bandwidth fairness, use the **no** form of the command.

rate-mode bandwidth-fairness module *module-id*
no rate-mode bandwidth-fairness module *module-id*

Syntax Description

module *module-id*	Specifies the module number.

Command Default

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.1(2)	This command was introduced.

Usage Guidelines

Enter the command separately for each module you want to enable or disable bandwidth fairness.

Note This feature is only supported on 48-port and 24-port 4-Gbps Fibre Channel switching modules.

Examples

The following example shows how to enable bandwidth fairness for a module:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rate-mode bandwidth-fairness module 1
```

The following example shows how to disable bandwidth fairness for a module:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# no rate-mode bandwidth-fairness module 1
```

Related Commands

Command	Description
show module bandwidth-fairness	Displays bandwidth fairness status.

rate-mode oversubscription-limit

To enable or disable restrictions on oversubscription ratios, use the rate-mode oversubscription-limit command.

rate-mode oversubscription-limit module *module number*
no rate-mode oversubscription-limit module *module number*

Syntax Description

module *module-number*	Identifies the specific module on which oversubscription ratio restrictions will be enabled or disabled.

Command Default

Oversubscription ratios are restricted for all 24-port and 48-port switching modules.

Command Modes

Configuration mode.

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When restrictions on oversubscription ratios are disabled, the bandwidth allocation among the shared ports is proportionate to the configured speed (if the configured speed is auto, then bandwidth is allocated assuming a speed of 4 Gbps).

You must explicitly shut down and take out of service shared ports before disabling oversubscription ratio restrictions on them.

The configuration is not saved to the startup configuration unless you explicitly enter the **copy running-config startup-config** command.



Caution You must enable restrictions on oversubscription ratios before you can downgrade modules to a previous release.

Examples

The following example disables restrictions on oversubscription ratios for a module (there are only dedicated ports, so a shutdown is not necessary):

```
switch# config t
switch(config)# no rate-mode oversubscription-limit module 2
```

The following example shows how to view the status of a module's oversubscription ratios:

```
switch# show running-config
version 3.1(1)
...
no rate-mode oversubscription-limit module 2
interface fc2/1
  switchport speed 2000
interface fc2/1
...
```

Related Commands

Command	Description
copy running-config startup-config	Saves the new oversubscription ratio configuration to the startup configuration.
show port-resources module	Displays the rate mode status of ports.

read command-id

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

read command-id *cmd-id* **target** *pwwn* **transfer-size** *bytes* [**outstanding-ios** *value* [**continuous** | **num-transactions** *number*]]

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.
outstanding-ios *value*	(Optional) Specifies the number of outstanding I/Os. The range is 1 to 1024.
continuous	(Optional) Specifies that the command is performed continuously.
num-transactions *number*	(Optional) Specifies a number of transactions. The range is 1 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

To stop a SCSI read command in progress, use the **stop** command.

Examples

The following example configures a continuous SCSI 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)# read command-id 100 target 22:22:22:22:22:22:22:22 transfer-size
512000 outstanding-ios 2 continuous
```

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.

read-only

To configure the read-only attribute in a zone attribute group, use the **read-only** command **in zone attribute configuration submode.** To revert to the default, use the **no** form of the command.

read-only
no read-only

Syntax Description

This command has no other arguments or keywords.

Command Default

Read-write.

Command Modes

Zone attribute configuration submode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

This command only configures the read-only attribute for enhanced zoning. To enable broadcast zoning for basic mode, use the **attribute read-only** subcommand after entering zone configuration mode using the **zone name** command.

Examples

The following example shows how to set the read-only attribute for a zone attribute group:

```
switch# config terminal
switch(config)# zone-attribute-group name admin-attributes vsan 10
switch(config-attribute-group)# read-only
```

Related Commands

Command	Description
show zone-attribute-group	Displays zone attribute group information.
zone mode enhanced vsan	Enables enhanced zoning for a VSAN.
zone name	Configures zone attributes.
zone-attribute-group name	Configures zone attribute groups.

reload

To reload the entire switch, an active supervisor module, a standby supervisor module, or a specific module, or to force a netboot on a given module, use the **reload** command in EXEC mode.

reload [**system** **non-disruptive** | **module** *number* [**force-dnld** | **non-disruptive**]]

Syntax Description

system	(Optional) Reloads the switch. **Note** This option is available only on the fabric switches.
module *number*	(Optional) Reloads a specific module or active or standby supervisor module. **Note** Fabric switches have only one module — module 1. Consequently, the entire switch is reloaded if we reload module 1.
force-dnld	(Optional) Reloads, initiates netboot, and forces the download of the latest module firmware version to a specific module.
non-disruptive	Reloads the switch or module nondisruptively with the same image.

Command Default

Reboots the entire switch.

Command Modes

EXEC mode.

Command History

Release	Modification
8.4(2)	Added the **system** and **non-disruptive** keywords.
1.0(2)	This command was introduced.

Usage Guidelines

Use the **reload** command to reboot the system, or to reboot a specific module, or to force a netboot on a specific module. The **reload** command used by itself, powers down all the modules and reboots the supervisor modules.

Use the **reload module** *module-number* command, if the given slot has a module or standby supervisor module, to power-cycle that module. If the given slot has an active supervisor module, then it causes the currently active supervisor module to reboot and the standby supervisor module becomes active.

The **reload module** *module-number* **force-dnld** command is similar to the previous command. This command forces netboot to be performed. If the slot contains a module, then the module netboots with the latest firmware and updates its corresponding flash with this image.

The **reload module** *module-number* **non-disruptive** and **reload system non-disruptive** commands are similar to the previous command. These commands nondisruptively netboots the module. If the slot contains a module, then the module netboots with the same image that it was using before the update. These commands are used to rectify any software issues that you may encounter by nondisruptively netbooting the module.

Examples

The following example shows how to reboot the entire switch:

```
switch# reload
This command will reboot the system. (y/n)? y
```

The following example shows how to reboot a fabric switch, for example Cisco MDS 9396T, nondisruptively:

```
switch# reload system non-disruptive
```

The following example show how to initiate netboot on a specific module:

```
switch# reload module 8 force-dnld
```

The following example shows how to reload module 8 with the same image on a Cisco MDS 9700 switch nondisruptively:

```
switch# reload module 8 non-disruptive
```

The following example shows how to reboot a specific module on a Cisco MDS 9700 switch:

```
switch# reload module 8
reloading module 8 ...
```

The following example shows how to reboot an active supervisor module on a Cisco MDS 9710 switch (if module 5 is the active supervisor):

```
switch# reload module 5
This command will cause supervisor switchover. (y/n)? y
```

Related Commands

Command	Description
copy system:running-config nvram:startup-config	Copies any file from a source to a destination.
install	Installs a new software image.

renew lifetime

Use the **renew lifetime** command to set the automatic certificate renewal period percentage. Use the **no** form of the command to return to the default renewal period.

renew lifetime *percentage*

no renew lifetime *percentage*

Syntax Description

lifetime *percentage*	Configures when to start certificate renewal. Default value is 95%.

Command Default

None

Command Modes

trustpoint-est configuration submode.

Command History

Release	Modification
9.4(5)	This command was introduced.

Usage Guidelines

This command sets the age threshold at which automatic certificate renewal will be started. The value is a percentage of the certificate's validity period (the period of the *notAfter* date minus the *notBefore* date in the certificate). Once EST-enabled certificate passes this fraction of its age the switch requests a new certificate from the Certificate Authority. Certificate lifetimes are checked once every 24 hours.

Some age buffer should be allowed in case the CA is initially uncontactable.

Examples

```
switch# configure terminal
switch(config)# crypto ca trustpoint engineering-est-tp
switch(config-trustpoint)# management-method est
switch(config-trustpoint-est)# enrollment
switch(config-trustpoint-est)# renew lifetime 98
```

Related Commands

Command	Description
client-trustpoint	Specifies the trustpoint containing the switch client certificates.
enrollment	Enable the certificate enrollment functionality for a specific trustpoint using the Enrollment over Secure Transport (EST) protocol.
management-method est	Enters EST configuration submode.
show crypto ca certificates	Displays installed switch identity certificates.
show crypto ca trustpoint	Displays CA profiles

revocation-check

To configure trust point revocation check methods, use the **revocation-check** command in trust point configuration submode. To discard the revocation check configuration, use the **no** form of the command.

revocation-check {**crl** [**none** | **ocsp** [**none**]] | **none** | **ocsp** [**crl** [**none**] | **none**]}
no revocation-check {**crl** [**none** | **ocsp** [**none**]] | **none** | **ocsp** [**crl** [**none**] | **none**]}

Syntax Description

crl	Specifies the locally stored certificate revocation list (CRL) as the place to check for revoked certificates.
none	(Optional) Specifies that no checking be done for revoked certificates.
ocsp	(Optional) Specifies the Online Certificate Status Protocol (OCSP) for checking for revoked certificates.

Command Default

By default, the revocation checking method for a trust point is CRL.

Command Modes

Trust point configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

You must authenticate the CA and configure the OCSP URL before configuring OCSP as a revocation checking method.

The revocation checking configuration allows one or more of the methods to be specified as an ordered list for revocation checking. During peer certificate verification, each method is tried in the specified order until one method succeeds by providing the revocation status. When none is specified as the method, it means that there is no need to check the revocation status, which treats the peer certificate as not revoked. If none is the first method specified in the method list, subsequent methods are not allowed to be specified because checking is not required.

Examples

The following example shows how to check for revoked certificates using OCSP on a URL that must have been previously configured:

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# revocation-check oscp
```

The following example shows how to check for revoked certificates in the locally stored CRL:

```
switch(config-trustpoint)# revocation-check crl
```

The following example shows how to check revocation status first using locally cached CRL and then, if needed, using OCSP. If CRL is not yet cached locally, only OCSP checking is attempted:

```
switch(config-trustpoint)# revocation-check crl ocsp
```

The following example shows how to do no checking for revoked certificates:

```
switch(config-trustpoint)# revocation-check none
```

Related Commands

Command	Description
crypto ca crl-request	Configures a CRL or overwrites the existing one for the trust point CA.
ocsp url	Configures details of the trust point OSCP.
show crypto ca crl	Displays configured CRLs.

rlir preferred-cond fcid

To specify a preferred host to receive Registered Link Incident Report (RLIR) frames, use the **rlir preferred-cond fcid** command in configuration mode. To remove a preferred host, use the **no** form of the command.

rlir preferred-cond fcid *fc-id* **vsan** *vsan-id*
no rlir preferred-cond fcid *fc-id* **vsan** *vsan-id*

Syntax Description

fcid *fc-id*	Specifies the FC ID. The format is **0x**>*hhhhhh* .
vsan *vsan-id*	Specifies a VSAN ID. The range is 1 to 4093.

Command Default

By default, the MDS switch sends RLIR frames to one of the hosts in the VSAN with the register function set to “conditionally receive” if no hosts have the register function set to “always receive.”

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(3)	This command was introduced.

Usage Guidelines

The MDS switch sends RLIR frames to the preferred host only if it meets the following conditions:

- No host in the VSAN is registered for RLIR with the registration function set to “always receive.” If one or more hosts in the VSAN are registered as “always receive,” then RLIR sends only to these hosts and not to the configured preferred host.
- The preferred host is registered with the registration function set to “conditionally receive.”



Note If all registered hosts have the registration function set to “conditionally receive,” then the preferred host receives the RLIR frames.

You can specify only one RLIR preferred host per VSAN.

Examples

The following example specifies FC ID 0x654321 as the RLIR preferred host for VSAN 2:

```
switch# config t
switch(config)# rlir preferred-cond fcid 0x654321 vsan 2
```

The following example removes FC ID 0x654321 as the RLIR preferred host for VSAN 2:

```
switch# config t
switch(config)# no rlir preferred-cond fcid 0x654321 vsan 2
```

Related Commands

Command	Description
show rlir	Displays information about RLIR, Link Incident Record Registration (LIRR), and Distribute Registered Link Incident Record (DRLIR) frames.
clear rlir	Clears the RLIRs.
debug rlir	Enables RLIR debugging.

rmdir

To delete an existing directory from the flash file system, use the **rmdir** command in EXEC mode.

rmdir [**bootflash:** | **slot0:** | **volatile:**] *directory*

Syntax Description

bootflash:	(Optional) Source or destination location for internal bootflash memory.
slot0:	(Optional) Source or destination location for the CompactFlash memory or PCMCIA card.
volatile:	(Optional) Source or destination location for volatile file system.
directory	Name of the directory to remove.

Command Default

Uses the current default directory.

Command Modes

EXEC Mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

This command is only valid on flash file systems.

The **rmdir** command deletes an existing directory at the current directory level or at a specified directory level. The directory must be empty to be deleted.

Examples

The following example deletes the directory called test in the slot0 directory:

```
switch# rmdir slot0:test
```

The following example deletes the directory called test at the current directory level. If the current directory is slot0:mydir, this command deletes the slot0:mydir/test directory.

```
switch# rmdir delete
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
mkir	Creates a new directory in the flash file system.

rmon alarm

To configure a 32 bit remote monitoring (RMON) alarm, use the **rmon alarm** command **in configuration mode.** To delete an RMON alarm, use the **no** form of the command.

rmon alarm *alarm-number mib-object sample-interval* {**absolute** | **delta**} **rising-threshold** *value* [*rising-event*] **falling-threshold** *value* [*falling-event*] [**owner** *alarm-owner*]
no rmon alarm *alarm-number*

Syntax Description

alarm-number	Specifies the RMON alarm number. The range is 1 to 65535.
mib-object	Specifies the MIB object to monitor. Maximum length is 80 characters. **Note** The MIB object identifier must be fully numbered, dotted-decimal notation, not the text string description.
sample-interval	Specifies the sample interval in seconds. The range is 1 to 2147483647.
absolute	Tests each sample directly.
delta	Tests the difference (delta) between the current and previous sample.
rising-threshold *value*	Specifies the rising threshold value. The range is –2147483648 to 2147483647.
rising-event	(Optional) Specifies the event to trigger on rising threshold crossing. The range is 1 to 65535. If no event is specified, event 0 is used.
falling-threshold *value*	Specifies the falling threshold value. The range is –2147483648 to 2147483647.
falling-event	(Optional) Specifies the event to trigger on rising threshold crossing. The range is 1 to 65535. If no event is specified, event 0 is used.
owner *alarm-owner*	(Optional) Specifies an owner for the alarm. Maximum size is 80 characters.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
2.0(x)	This command was introduced.

Usage Guidelines

Use the rmon event command to configure the events for alarms.

The maximum number of RMON alarms currently is only configurable through the device manager and threshold manager GUI. A CLI command is not available to change this maximum value.



Note We recommend setting alarm sample intervals to 30 seconds or higher to prevent excessive load on the system.

Examples

The following example configures a 32-bit alarm number 20 for ifInErrors (OID 1.3.6.1.2.1.2.2.1.14) on interface fc 1/1. The sample interval is 30 seconds and delta samples are tested. The rising threshold is 15 errors per sample window; reaching this level triggers event 1. The falling threshold is 0 errors in the sample window which triggers event 0 (no action). The owner is 'ifInErrors.fc1/1@test'.

```
switch# config terminal
switch(config)# rmon alarm 20 1.3.6.1.2.1.2.2.1.14.16777216 30 delta rising-threshold 15
1 falling-threshold 0 owner ifInErrors.fc1/1@test
```

Related Commands

Command	Description
rmon event	Configures an RMON event.
rmon hcalarm	Configures the 64-bit RMON alarm.
show rmon	Displays RMON configuration and logging information.
show snmp host	Displays the SNMP trap destination information.
snmp-server host	Specifies the recipient of an SNMP notification.

rmon event

To configure a remote monitoring (RMON) event, use the **rmon event** command **in configuration mode.** To delete an RMON event, use the **no** form of the command.

rmon event *event-number* [**description** *text* [**owner** *owner-name*] | **log** [**trap** *community-string*] [**description** *text*] [**owner** *owner-name*] | **trap** *community-string* [**description** *text*] [**owner** *owner-name*] | **owner** *owner-name*]
no rmon event *event-number*

Syntax Description

event-number	Specifies the RMON event number. The range is 1 to 65535.
description *text*	(Optional) Specifies a description of the event. Maximum length is 80 characters.
owner *owner-name*	(Optional) Specifies an owner for the alarm. Maximum length is 80 characters.
log	(Optional) Generates an RMON log entry in the onboard RMON log when the event is triggered by an alarm.
trap *community-string*	(Optional) Generates an SNMP trap with the specified community name when the event is triggered by an alarm. The maximum length is 32 characters.

Command Default

Disabled.

Command Modes

Configuration mode

Command History

Release	Modification
4.1(1b)	Modified the command output.
2.0(x)	This command was introduced.

Usage Guidelines

You can trigger the events created by this command with alarms configured using the **rmon alarm** or **rmon hcalarm** commands

The log option logs the event to a local log file on the MDS switch. The trap option uses the onboard SNMP agent to send an SNMP trap to a remote NMS.



Note Events can be used by both **rmon alarm** (32-bit) and **hcalarm** (64-bit) commands.

Examples

The following example configures RMON event1 to log the onboard RMON log and send an SNMP trap to public community trap destinations. The description is public and is owned by switchname.

```
switch# config terminal
rmon event 1 log trap public description FATAL(1) owner !switchname
switch(config)#
```

The following example configures RMON event3 to log the onboard RMON log and send an SNMP trap to public community trap destinations. The description is error and is owned by switchname:

```
switch# config terminal
rmon event 3 log trap public description ERROR(3) owner !switchname
switch(config)#
```

The following example configures RMON event4 to log the onboard RMON log and send an SNMP trap to public community trap destinations. The description is warning and is owned by switchname:

```
switch# config terminal
rmon event 4 log trap public description WARNING(4) owner !switchname
switch(config)#
```

The following example configures RMON event5 to log the onboard RMON log and send an SNMP trap to public community trap destinations. The description is information and is owned by switchname:

```
switch# config terminal
rmon event 4 log trap public description INFORMATION(5) owner !switchname
switch(config)#
```

The following example configures RMON event 2 to log the onboard RMON log and send an SNMP trap to public community trap destinations. The description is CriticalErrors and is owned by test:

```
switch# config terminal
switch(config)# rmon event 2 log trap public description CriticalErrors owner
 test
```

Related Commands

Command	Description
rmon alarm	Configures a 32-bit RMON alarm.
rmon hcalarm	Configures a 64-bit RMON alarm.
show rmon	Displays RMON configuration and logging information.

rmon hcalarm

To configure a 64-bit remote monitoring (RMON) high-capacity alarm (hcalarm), use the **rmon hcalarm** command in configuration mode. To delete an RMON hcalarm, use the **no** form of the command.

rmon hcalarm *alarm-number mib-object sample-interval* {**absolute** | **delta**} {**rising-threshold-high** *value* **rising-threshold-low** *value* [*rising-event*] [**falling-threshold-high** *value* **falling-threshold-low** *value* [*falling-event*]] | **falling-threshold-high** *value* **falling-threshold-low** *value* [*falling-event*]} [**owner** *alarm-owner*]
no rmon hcalarm *alarm-number mib-object sample-interval* {**absolute** | **delta**} {**rising-threshold-high** *value* **rising-threshold-low** *value* [*rising-event*] [**falling-threshold-high** *value* **falling-threshold-low** *value* [*falling-event*]] | **falling-threshold-high** *value* **falling-threshold-low** *value* [*falling-event*]} [**owner** *alarm-owner*]

Syntax Description

alarm-number	Specifies the RMON hcalarm number. The range is 1 to 65535.
mib-object	Specifies the MIB object to monitor. Maximum length is 80 characters. **Note** The MIB object identifier must be fully numbered, dotted-decimal notation, not the text string description.
sample-interval	Specifies the sample interval in seconds. The range is 1 to 65535.
absolute	Tests each sample directly.
delta	Tests the difference (delta) between the current and previous sample.
rising-threshold-high *value*	Configures the upper 32 bits of the 64-bit rising threshold value. The range is 0 to 4294967295.
rising-threshold-low *value*	Configures the lower 32 bits of the 64-bit rising threshold value. The range is 0 to 4294967295.
rising-event	(Optional) Specifies the event to trigger on rising threshold crossing. The range is 1 to 65535.
falling-threshold-high *value*	Configures the upper 32 bits of the 64-bit falling threshold value. The range is 0 to 4294967295.
falling-threshold-low *value*	Configures the lower 32 bits of the 64-bit falling threshold value. The range is 0 to 4294967295.
falling-event	(Optional) Specifies the event to trigger on falling threshold crossing. The range is 0 to 65535.
owner *alarm-owner*	(Optional) Specifies an owner for the alarm. Maximum size is 80 characters.

Command Default

64-bit alarms.

Command Modes

Configuration mode

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Event number 0 is a predefined null (or no operation) event. When no event is specified by the user in an alarm this event is automatically used by the system. The event causes no action to be taken when triggered, however, the alarm is still reset. The event cannot be redefined by the user. It is a predefined event and you can only create events in the range from 1 to 65535.

To configure a high-capacity RMON alarm, use the CISCO-HC-ALARM-MIB.

The maximum number of RMON alarms is currently configurable through the device manager and threshold manager GUI. A CLI command is not available to change this maximum value.



Note We recommand setting alarm sample intervals to 30 seconds or higher to prevent excessive load on the system.

Examples

The following example configures 64-bit alarm number 2 for ifHCInOctets (OID 1.3.6.1.2.1.31.1.1.1.6) on interface fc 12/1. The sample interval is 30 seconds and delta samples are tested. The rising threshold is 240,000,000,000 bytes per sample window (an average of 8,000,000,000 bytes per second); reaching this level triggers event 4. The falling threshold is 180,000,000,000 bytes in the sample window (an average of 6,000,000,000 bytes per second) which triggers event 0 (no action) and resets the alarm. The owner is 'ifHCInOctets.fc12/1@test'.

```
switch# config terminal
switch#(config) rmon hcalarm 2 1.3.6.1.2.1.31.1.1.1.6.22544384 30 delta  rising-threshold-high
 55 rising-threshold-low 3776798720 4 falling-threshold-high 41  falling-threshold-low
3906340864 owner ifHCInOctets.fc12/1@test
```

Related Commands

Command	Description
rmon alarm	Configures a 32-bit RMON alarm.
rmon event	Configures an RMON event.
rmon hcalarm	Configures a 64-bit RMON alarm.
show rmon	Displays RMON configuration and logging information.
show snmp host	Displays the SNMP trap destination information.
snmp-server host	Specifies the recipient of an SNMP notification.

role abort

To discard an authorization role Cisco Fabric Services (CFS) distribution session in progress, use the **role abort** command in configuration mode.

role 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

None.

Examples

The following example shows how to discard an authorization role CFS distribution session in progress:

```
switch# config terminal
switch(config)# role abort
```

Related Commands

Command	Description
role distribute	Enables CFS distribution for authorization roles.
show role	Displays authorization role information.

role commit

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

role 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

None.



Note Once the "role commit" is done the running configuration has been modified on all switches participating in the role distribution. You can then use the "copy running-config startup-config fabric" command to save the running-config to the startup-config on all the switches in the fabric.

Examples

The following example shows how to apply an authorization role configuration to the switches in the fabric:

```
switch# config terminal
switch(config)# role commit
```

Related Commands

Command	Description
role distribute	Enables CFS distribution for authorization roles.
show role	Displays authorization roles information.

role distribute

To enable Cisco Fabric Services (CFS) distribution for authorization roles, use the **role distribute** command. To disable this feature, use the **no** form of the command.

role distribute
no role 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

None.

Examples

The following example shows how to enable fabric distribution for authorization roles:

```
switch# config terminal
switch(config)# role distribute
```

Related Commands

Command	Description
role commit	Commits temporary to the authorization role configuration changes to the active configuration.
show role	Displays authorization role information.

role name

To configure and assign users to a new role or to modify the profile for an existing role, use the **role name** command in configuration mode. Use the **no** form of this command to delete a configured role.

role name [**max-length 64**] [*name*] [**description** *user description*] [**rule** *number* **attribute-admin** **permit clear feature** *name* | **permit config feature** *name* | **permit debug feature** *name* | **permit show feature** *name*] [**rule** *number* **deny clear feature** *name* | **deny config feature** *name* | **deny debug feature** *name* | **deny exec feature** *name* | **deny show feature** *name*]
no role name *name* [**description** *user description*] [**rule** *number* **permit clear feature** *name* | **permit config feature** *name* | **permit debug feature** *name* | **permit show feature** *name*] [**rule** *number* **deny clear feature** *name* | **deny config feature** *name* | **deny debug feature** *name* | **deny exec feature** *name* | **deny show feature** *name*]

Syntax Description

max-length 64	(Optional) Allows the user to configure role name length of 64 characters. The default role name length is 16 characters.
name	Name of the role to be created or modified. The maximum string length is 64.
description	(Optional) Adds a description for the role. The maximum size is 128.
user description	(Optional) Adds description of users to the role.
rule *number*	(Optional) Enters the rule keyword. The rule number is from 1 to 256.
attribute-admin	Grants network-admin privileges to the role.
permit	(Optional) Adds commands to the role.
deny	(Optional) Removes commands from the role.
clear	(Optional) Clears the commands.
feature *name*	Enters the feature name. The maximum size of the feature name is 32.
config	(Optional) Configures commands.
debug	(Optional) Debug commands
show	(Optional) Show commands
exec	(Optional) Exec commands

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
8.3(1)	This command was modified. The **attribute-admin** keyword was added.

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

Users are assigned roles. Roles are assigned rules. Roles are a group of rules defining a user's access to certain commands. The rules within roles can be assigned to permit or deny access to the following commands:

- **clear**— Clear commands
- **config**— Configuration commands
- **debug**— Debug commands
- **exec**— EXEC commands
- **show**— Show commands

These commands can have **permit** or **deny** options within that command line.

Examples

The following example shows how to assign users to a new role:

```
switch# config terminal
switch(config)#role name max-length 64
switch(config)# role name techdocs
switch(config-role)#
switch(config)#
switch(config-role)# description Entire Tech. Docs. group
switch(config-role)# no
 description
switch# config terminal
switch(config)# role name sangroup
switch(config-role)#
switch(config-role)# rule 1 permit config
switch(config-role)# rule 2 deny config feature fspf
switch(config-role)# rule 3 permit debug feature zone
switch(config-role)# rule 4 permit exec feature fcping
switch(config-role)# no rule 4
switch(config)# no role name sangroup
switch(config)# no role name max-length 64
Role: network-operator
Description: Predefined Network Operator group. This role cannot be modified
Access to Show commands and selected Exec commands
```

Related Commands

Command	Description
show role	Displays all roles configured on the switch including the rules based on each role.

rsakeypair

To configure and associate the RSA key pair details to a trust point, use the **rsakeypair** command in trust point configuration submode. To disassociate the RSA key pair from the trust point, use the **no** form of the command.

rsakeypair *key-pair-label* [*key-pair-size*]
no rsakeypair *key-pair-label* [*key-pair-size*]

Syntax Description

key-pair-label	Specifies a name for the RSA key pair. The maximum size is 64 characters.
key-pair-size	(Optional) Specifies a size for the RSA key pair. The size can range from 512 to 2048.

Command Default

The default key pair size is 512 if the key pair is not already generated.

Command Modes

Trust point configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Only one RSA key pair can be associated with a trust point CA, even though the same key pair can be associated with many trust point CAs. This association must occur before enrolling with the CA to obtain an identity certificate. If the key pair had been generated previously (using the **crypto key generate** command), then the key pair size, if specified, should be the same as that was used during generation. If the specified key pair is not yet generated, it will be generated during enrollment using the **crypto ca enroll** command.

The **no** form of the **rsakeypair** command disassociates (but never destroys) the key pair from the trust point. Before issuing the **no rsakeypair** command, first remove the identity certificate, if present, from the trust point CA. Doing so ensures the consistency of the association between the identity certificate and the key pair for a trust point

Examples

The following example shows how to associate an RSA key pair to a trust point:

```
switch# config terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# rsakeypair adminid-key
```

The following example shows how to disassociate an RSA key pair from a trust point:

```
switch(config-trustpoint)# no rsakeypair adminid-key
```

Related Commands

Command	Description
crypto ca enroll	Requests certificates for the switch's RSA key pair created for the trust point CA.

Command	Description
crypto key generate rsa	Configures RSA key pair information.
show crypto key mypubkey rsa	Displays information about configured RSA key pairs.

rscn

To configure a registered state change notification (RSCN), a Fibre Channel service that informs Nx ports about changes in the fabric, use the **rscn** command in configuration mode.

rscn {**multi-pid** | **suppress domain-swrscn**} **vsan** *vsan-id*

Syntax Description

multi-pid	Sends RSCNs in multi-PID format.
suppress domain-swrscn	Suppresses transmission of domain format SW-RCSNs.
vsan *vsan-id*	Configures VSAN information or membership. The ID of the VSAN is from 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example configures RSCNs in multi-PID format:

```
switch# config terminal
switch(config)# rscn multi-pid vsan 1
```

Related Commands

Command	Description
show rscn src-table	Displays state change registration table.
show rscn statistics	Displays RSCN statistics.

rscn abort vsan

To cancel a Registered State Change Notification (RSCN) configuration on a VSAN, use the **rscn abort vsan** command in configuration mode. To reverse the cancellation, use the **no** form of the command.

rscn abort vsan *vsan-id*
no rscn abort vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN where the RSCN configuration should be cancelled. The ID of the VSAN is from 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

The following example cancels an RSCN configuration on VSAN 1:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn abort vsan 1
```

Related Commands

Command	Description
clear rscn session vsan	Clears the RSCN session for a specified VSAN.
rscn commit vsan	Commits a pending RSCN configuration on a specified VSAN.
rscn distribute	Enables the distribution of an RSCN configuration.
rscn event-tov	Configures an RSCN event timeout.
show rscn	Displays the RSCN configuration information.

rscn coalesce swrscn vsan

To enable coalescing of Switch Registered State Change Notification (SWRSCN) before sending, use the **rscn coalesce swrscn vsan** command in configuration mode. To disable coalesce SWRSCN, use the **no** form of the command.

rscn coalesce swrscn vsan *vsan-id* [**delay** *milliseconds*]
no rscn coalesce swrscn vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN ID range. The range is from 1 to 4093.
delay	Specifies the delay in milliseconds to achieve swrscn coalesce.
milliseconds	Specifies the Swrscn coalesce delay in milliseconds (default 500ms). The range is from 100 to 2000.

Command Default

Disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
6.2(7)	This command was introduced.

Usage Guidelines

This feature can be enabled in a fabric where all the switches are MDS and are running 6.2(7) and above.

Examples

The following example shows how to enable coalesce SWRSCN:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn coalesce swrscn vsan 1
```

switch(config)#

The following example shows how to configure 100 milliseconds delay for coalesce SWRSCN:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn coalesce swrscn vsan 1 delay 100
switch(config)#
```

rscn commit vsan

To apply a pending Registered State Change Notification (RSCN) configuration, use the **rscn commit vsan** command in configuration mode. To discard a pending RSCN configuration, use the **no** form of the command.

rscn commit vsan *vsan-id*
no rscn commit vsan *vsan-id*

Syntax Description

vsan-id	Specifies a VSAN where the RSCN configuration should be committed. The ID of the VSAN is from 1 to 4093.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

If you commit the changes made to the active database, the configuration is committed to all the switches in the fabric. On a successful commit, the configuration change is applied throughout the fabric and the lock is released.

Note Once the "rscn commit" is done the running configuration has been modified on all switches participating in rscn distribution. You can then use the "copy running-config startup-config fabric" command to save the running-config to the startup-config on all the switches in the fabric.

Examples

The following example commits an RSCN configuration on VSAN 1:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn commit vsan 1
```

Related Commands

Command	Description
clear rscn session vsan	Clears the RSCN session for a specified VSAN.
rscn abort vsan	Cancels a pending RSCN configuration on a specified VSAN.
rscn distribute	Enables the distribution of an RSCN configuration.
rscn event-tov	Configures an RSCN event timeout.
show rscn	Displays RSCN configuration information.

rscn distribute

To enable distribution of a Registered State Change Notification (RSCN) configuration, use the **rscn distribute** command in configuration mode. To disable the distribution, use the **no** form of the command.

rscn distribute
no rscn distribute

Syntax Description

This command has no arguments or keywords.

Command Default

RSCN timer distribution is disabled.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The RSCN timer configuration must be the same on all switches in the VSAN; otherwise, the link will not come up. Cisco Fabric Service (CFS) automatically distributes the RSCN timer configuration to all switches in a fabric. Only the RSCN timer configuration distributed.



Note For the CFS distribution to operate correctly for the RSCN timer configuration, all switches in the fabric must be running Cisco SAN-OS Release 3.0(1) or later.

Examples

The following example enables the distribution of an RSCN configuration:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn distribute
```

Related Commands

Command	Description
clear rscn session vsan	Clears the RSCN session for a specified VSAN.
rscn abort vsan	Cancels a pending RSCN configuration on a specified VSAN.
rscn commit vsan	Applies a pending RSCN configuration.
rscn event-tov	Configures an RSCN event timeout.
show rscn	Displays RSCN configuration information.

rscn event-tov

To configure an event timeout value for a Registered State Change Notification (RSCN) on a specified VSAN, use the **rscn event-tov** command in configuration mode. To cancel the event timeout value and restore the default value, use the **no** form of the command.

rscn event-tov *timeout* **vsan** *vsan-id*
no rscn event-tov *timeout* **vsan** *vsan-id*

Syntax Description

timeout	Specifies an event timeout value in milliseconds. The range is 0 to 2000.
vsan-id	Specifies a VSAN where the RSCN event timer should be used. The ID of the VSAN is from 1 to 4093.

Command Default

The default timeout values are 2000 milliseconds for Fibre Channel VSANs and 1000 milliseconds for FICON VSANs.

Command Modes

Configuration mode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

Before changing the timeout value, you must enable RSCN configuration distribution using the **rscn distribute** command.

The RSCN timer is registered with Cisco Fabric Services (CFS) during initialization and switchover. For high availability, if the RSCN timer distribution crashes and restarts or a switchover occurs, it resumes normal functionality from the state prior to the crash or switchover.



Note You can determine configuration compatibility when downgrading to an earlier Cisco MDS SAN-OS release using the **show incompatibility system** command. You must disable RSCN timer distribution support before downgrading to an earlier release.

Examples

The following example configures an RSCN event timeout value on VSAN 1:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn event-tov 20 vsan 1
Successful. Commit should follow for command to take effect.
```

Related Commands

Command	Description
rscn abort vsan	Cancels a pending RSCN configuration on a specified VSAN.

Command	Description
rscn commit vsan	Applies a pending RSCN configuration.
rscn distribute	Enables distribution of an RSCN configuration.
clear rscn session vsan	Clears the RSCN session for a specified VSAN.
show rscn	Displays RSCN configuration information.

rscn permit type nport event switch-config

To enable Registered State Change Notification (RSCN) on management port IP address changes or switch name changes, use the **rscn permit type nport event switch-config** command. To disable RSCN, use the **no** form of the command.

rscn permit type nport event switch-config vsan *vsan-id*
no rscn permit type nport event switch-config vsan *vsan-id*

Syntax Description

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

Command Default

RSCN will not be sent on management port IP address changes or switch name changes.

Command Modes

Configuration mode.

Command History

Release	Modification
5.2(8)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable RSCN on management port changes:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# rscn permit type nport event switch-config vsan 1
switch(config)#
```

Related Commands

Command	Description
show rscn	Displays RSCN configuration information.

rspan-tunnel

To associate and bind the SPAN tunnel (ST) port with the RSPAN tunnel, use the **rspan-tunnel** command.

rspan-tunnel interface fc-tunnel *tunnel-id*
rspan-tunnel interface fc-tunnel *tunnel-id*

Syntax Description

rspan-tunnel	Configures the remote SPAN (RSPAN) tunnel.
interface	Specifies the interface to configure this tunnel.
fc-tunnel *tunnel-id*	Specifies the FC tunnel interface. The range is 1 to 255.

Command Default

None.

Command Modes

Interface configuration submode.

Command History

Release	Modification
1.2(1)	This command was introduced.

Usage Guidelines

The interface is not operationally up until the Fibre Channel tunnel mapping is configured in the source and destination switches.

Examples

The following example configures an interface to associate and bind the ST port with the RSPAN tunnel and enables traffic flow trough this interface:

```
switchS# config t
switchS(config)# interface fc2/1
switchS(config-if)# rspan-tunnel interface fc-tunnel 100
switchS(config-if)# no shutdown
```

rule

show rscn	Displays RSCN configuration information.

To specify the tape volume group regular expression, use the **rule** command. To disable this feature, use the **no** form of the command.

rule {*range* **range** | **regexp** *regular expression*}
no rule {**range** *range* | **regexp** *regular expression*}

Syntax Description

range *range*	Specifies the crypto tape volume barcode range. The maximum length is 32 characters.
regexp *regular expression*	Specifies the volume group regular expression. The maximum length is 32 characters.

Command Default

None.

Command Modes

Cisco SME crypto tape volume group configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example specifies the volume group regular expression:

```
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)#rule regexp r1
```

Related Commands

Command	Description
show sme cluster	Displays information about Cisco SME cluster.
tape-bkgrp *groupname*	Configures crypto backup group.
tape-volgrp *volume groupname*	Configures crypto backup volume group.

run-script

To execute the commands specified in a file, use the **run-script** command.

run-script [**bootflash:** | **slot0:** | **volatile:**] *filename*

Syntax Description

bootflash:	(Optional) Source or destination location for internal bootflash memory.
slot0:	(Optional) Source or destination location for the CompactFlash memory or PCMCIA card.
volatile:	(Optional) Source or destination location for volatile file system.
filename	Name of the file containing the commands.

Command Default

Uses the current default directory.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
3.0(1)	Updated the Usage Guidelines and Examples with information about user-defined variables.

Usage Guidelines

To use this command, be sure to create the file and specify commands in the required order.

The **run-script** command accepts user-defined variables as parameters.

Examples

The following example executes the CLI commands specified in the testfile that resides in the slot0 directory:

```
switch# show file slot0:testfile
conf t
interface fc 1/1
no shutdown
end
sh interface fc1/1
```

In response to the **run-script** command, this is the file output:

```
switch# run-script slot0:testfile
'conf t'
Enter configuration commands, one per line. End with CNTL/Z.
'interface fc 1/1'
'no shutdown'
'end'
'sh interface fc1/1'
fc1/1 is down (Fcot not present)
    Hardware is Fibre Channel
    Port WWN is 20:01:00:05:30:00:48:9e
    Admin port mode is auto, trunk mode is on
```

```
    vsan is 1
    Beacon is turned off
    Counter Values (current):
      0 frames input, 0 bytes, 0 discards
      0 runts, 0 jabber, 0 too long, 0 too short
      0 input errors, 0 CRC, 0 invalid transmission words
      0 address id, 0 delimiter
      0 EOF abort, 0 fragmented, 0 unknown class
      0 frames output, 0 bytes, 0 discards
      Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
      Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits
    Counter Values (5 minute averages):
      0 frames input, 0 bytes, 0 discards
      0 runts, 0 jabber, 0 too long, 0 too short
      0 input errors, 0 CRC, 0 invalid transmission words
      0 address id, 0 delimiter
      0 EOF abort, 0 fragmented, 0 unknown class
      0 frames output, 0 bytes, 0 discards
      Received 0 OLS, 0 LRR, 0 NOS, 0 loop inits
    Transmitted 0 OLS, 0 LRR, 0 NOS, 0 loop inits
```

The following example shows how you can pass user-defined variables to the **run-script** command:

```
switch# run-script bootflash:test2.vsh var1="fc1/1" var2="brief"
switch # show interface $(var1) $(var2)
--------------------------------------------------------------------------------
Interface Vsan Admin Admin Status SFP Oper Oper Port
Mode Trunk Mode Speed Channel
Mode (Gbps)
--------------------------------------------------------------------------------
fc1/1 1 auto on sfpAbsent -- -- --
```