CHAPTER 19

R Commands

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

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.

Defaults

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to discard a 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 other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to 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.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to 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 host

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

radius-server host {*server-name* | *ip-address*}
[**key** [**0** | **7**] *shared-secret*] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**timeout** *seconds* [**retransmit** *count*]]

no radius-server host {*server-name* | *ip-address*}
[**key** [**0** | **7**] *shared-secret*] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**timeout** *seconds* [**retransmit** *count*]]

Syntax Description

server-name	Specifies the RADIUS server DNS name. Maximum length is 256 characters.
ip-address	Specifies the RADIUS server IP address.
auth-port *port-number*	Configures the RADIUS server port for authentication
acct-port *port-number*	Configures the RADIUS server port for accounting.
authentication	Use for authentication.
accounting	Use for accounting.
key	RADIUS server shared key.
0	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	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.
retransmit *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 five times and the default is 1 time.
timeout *seconds*	Specifies the time (in seconds) between retransmissions to the RADIUS server. The default is 1 second and the valid range is 1 to 60 seconds.

Defaults

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

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
```

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	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	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.

Defaults

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

You need to configure the 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.

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.

Defaults

1 retransmission

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example 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 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.

Defaults

1 second

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example 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.

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 [**module** *module-number* **force-dnld**]

Syntax Description

module *module-number*	Reloads a specific module or active/standby supervisor module.
force-dnld	Reloads, initiates netboot, and forces the download of the latest module firmware version to a specific module.

Defaults

Reboots the entire switch.

Command Modes

EXEC mode.

Command History

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

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.

The **reload module** *module-number* command is used if the given slot has a module or standby supervisor module. It then power-cycles 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.

Examples

The following example uses **reload** to reboot the system.

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

The following example uses **reload** to initiate netboot on a specific module.

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

The following example uses **reload** to reboot a specific module.

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

The following example uses **reload** to reboot an active supervisor module.

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

Related Commands

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

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*	Specifies the number of outstanding I/Os. The range is 1 to 1024.
continuous	Specifies that the command is performed continuously.
num-transactions *number*	Specifies a number of transactions. The range is 1 to 2147483647.

Defaults

None.

Command Modes

SAN extension N port configuration submode.

Command History

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

Usage Guidelines

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.

Defaults

Read-write.

Command Modes

Zone attribute configuration submode.

Command History

Release	Modification
2.0(1b)	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.

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

Defaults

Uses the current default directory.

Command Modes

EXEC

Command History

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

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 test
```

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 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 delta (or difference) between samples.
rising-threshold *value*	Specifies the rising threshold value. The range is –2147483648 to 2147483647.
rising-event	Specifies the event to trigger on rising threshold crossing. The range is 1 to 65535.
falling-threshold *value*	Specifies the falling threshold value. The range is –2147483648 to 2147483647.
failing-event	Specifies the event to trigger on rising threshold crossing. The range is 1 to 65535.
owner *alarm-owner*	Specifies an owner for the alarm. Maximum size is 80 characters.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

The events that can be triggered are configured using the **rmon event** command.

Examples

The following example configures an RMON alarm.

```
switch# config terminal
switch(config)# rmon alarm 20 1.3.6.1.2.1.2.2.1.14.16777216 900 delta rising-threshold 15
1 falling-threshold 0 owner test
```

Related Commands

Command	Description
rmon event	Configures an RMON event.
show rmon	Displays RMON configuration information.

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** *trap-name*] [**description** *text*] [**owner** *owner-name*] | **owner** *owner-name* | **trap** *community-string* [**description** *text*] [**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*	Specifies a description of the event. Maximum length is 80 characters.
owner *owner-name*	Specifies an owner for the alarm. Maximum length is 80 characters
log	Generates an RMON log entry when the event is triggered by an alarm.
trap *community-string*	Generates an SNMP notification when event is triggered by an alarm. Maximum length is 32 characters.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

The events created by this command can be triggered by alarms configured using the **rmon alarm** command.

Examples

The following example configures an RMON event.

```
switch# config terminal
switch(config)# rmon event 2 log trap eventtrap description CriticalErrors owner Test2
```

Related Commands

Command	Description
rmon alarm	Configures an RMON alarm.
show rmon	Displays RMON configuration information.

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.

Defaults

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to discard 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.

Defaults

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to 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.

Defaults

Disabled.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to 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 *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*]

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

name	Adds RADIUS server. The maximum size is 32.
description	Add a description for the role. The maximum size is 80.
user description	Add description of users to the role.
exit	Exit from this submode
no	Negate a command or set its defaults
rule	Enter the rule keyword.
number	Enter the rule number 1-16.
permit	Add commands to the role.
deny	Remove commands from the role.
clear	Clear commands
config	Configuration commands
debug	Debug commands
show	Show commands
feature	Enter the feature name
exec	Exec commands
name	Enter the feature name (Max Size - 32)

Defaults

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

Roles are assigned rules. Roles are a group of rules defining a user's access to certain commands. Users are assigned roles. 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 techdocs
switch(config-role)#
switch(config)# no role name techdocs
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

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.

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.

Defaults

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example configures RSCNs in multi-PID format.

```
switch# config terminal
excal-113(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.

run-script

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

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

Syntax Description

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

Defaults

Uses the current default directory.

Command Modes

EXEC mode.

Command History

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

Usage Guidelines

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

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
```

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

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.

Defaults

None.

Command Modes

Interface configuration submode.

Command History

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

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
```