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-server host

To configure RADIUS authentication related parameters, use the **radius** command.

radius-server host *server name or ip address* **[accounting] | [acct-port** ***port number*** **(accounting | authentication accounting) | primary accounting | authentication accounting] | [auth-port** *port number* **(accounting) (acct-port** *port number* **|accounting | authentication accounting | primary accounting | primary authentication)] | [authentication accounting] | [key** *shared secret***] | [primary accounting | primary authentication]**

no radius-server host *server name or ip address* **[accounting] | [acct-port** ***port number*** **(accounting | authentication accounting) | primary accounting | authentication accounting] | [auth-port** *port number* **(accounting) (acct-port** *port number* **|accounting | authentication accounting | primary accounting | primary authentication)] | [authentication accounting] | [key** *shared secret***] | [primary accounting | primary authentication]**

Syntax Description

server name or ip address	Enter RADIUS server's DNS name or its IP address. The maximum character size is 256.
accounting	Use for accounting.
acct-port	RADIUS server's port for accounting.
authentication	Use for authentication.
key	RADIUS shared secret.
primary	Whether this RADIUS server is a primary server or not.

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 examples provide various scenarios to configure RADIUS authentication.

```
switch# config t

switch(config)# radius host 10.10.0.0 primary

switch(config)# radius host 10.10.0.0 key HostKey

switch(config)# radius host 10.10.0.0 auth-port 2003

switch(config)# radius host 10.10.0.0 acct-port 2004

switch(config)# radius host 10.10.0.0 accounting

switch(config)# radius host radius1 primary

switch(config)# radius host radius2 key 0 abcd

switch(config)# radius host radius3 key 7 1234
```

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

key	Global RADIUS shared secret.
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 t

switch(config)# radius key AnyWord

switch(config)# radius key 0 AnyWord

switch(config)# radius key 7 public
```

radius-server retransmit

To specify the number of times that RADIUS servers should try to authenticate a user, use the **radius-server retransmit** command.

radius-server retransmit *count*

Syntax Description

retransmit	RADIUS server retransmit count.
count	Configures the number of times (3) the switch tries to connect to a RADIUS server(s) before reverting to local authentication.

Defaults

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

By default, a switch retries a RADIUS server connection only once. This number can be configured. The maximum is five retries per server. You can revert the retry number to its default by issuing the **no radius-server retransmit** command.

Examples

The following examples provide various scenarios to configure RADIUS authentication.

```
switch# config t

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

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 this command.

radius-server timeout *seconds*

no radius-server timeout *seconds*

Syntax Description

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

Defaults

None.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following examples provide various scenarios to configure RADIUS authentication.

```
switch# config t

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

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	Reloads a specific module or active/standby supervisor module.
module-number	Specifies a module, either 1 or 2.
force-dnld	Reloads, initiates netboot, and forces the download of the latest module firmware version to a specific module.

Defaults

None.

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.

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

This command has no default settings.

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.

```
switch# rmdir test
```

If the current directory is slot0:mydir, this command deletes the slot0:mydir/test directory.

Related Commands

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

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** *nam* **]**

Syntax Description

role name	Configures RADIUS server.
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 number 1-16.
number	Enter the rule number 1-16.
permit	Remove commands from the role.
deny	Add commands to 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 t
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 t
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 *value* **| supress interface fc** *slot-number* }

Syntax Description

multi-pid	Sends RSCNs in multi-PID format.
vsan	Configures VSAN information or membership.
vsan-id	The ID of the VSAN is from 1 to 4093.
fc	Fiber Channel interface. Slot number range is from 1 to 9.
slot-number	Specifies a slot number and port number.

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 t
excal-113(config)# rscn multi-pid vsan 1
```

Related Commands

Command	Description
show rscn internal	Displays RSCN internal information.
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

None.

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*

Syntax Description

rspan-tunnel	Configures the remote SPAN (RSPAN) tunnel.
interface	Specifies the interface to configure this tunnel.
fc-tunnel	Specifies the FC tunnel interface.
tunnel-id	Configures an ID that ranges from 1 to 255.

Defaults

None.

Command Modes

Configuration mode.

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
```