CHAPTER 2

A Commands

The commands in this chapter apply to the Cisco MDS 9000 Family of multilayer directors and fabric switches. All commands are shown here in alphabetical order regardless of command mode. See "About the CLI Command Modes" section on page 1-3 to determine the appropriate mode for each command. For more information, refer to the *Cisco MDS 9000 Family CLI Configuration Guide*.

aaa accounting logsize

To set the size of the local accounting log file, use the **aaa accounting logsize** command to set the size of the local accounting log file. To revert to the default logsize 250000 bytes, use the **no** form of the command.

aaa accounting logsize *integer*

no aaa accounting logsize

Syntax Description

aaa accounting	Configures accounting methods
logsize	Configures local accounting log file size (in bytes).
integer	Sets the size limit of the local accounting log file in bytes from 0 to 250000.

Defaults

25,0000.

Command Modes

Configuration mode.

Command History

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

Usage Guidelines

None.

Examples

The following example shows the log file size configured at 29000 bytes:

```
switch# config terminal
switch(config)# aaa accounting logsize 29000
```

Related Commands

Command	Description
show accounting logsize	Displays the configured log size.
show accounting log	Displays the entire log file.

aaa accounting default

To configure the default accounting method, use the **aaa accounting default** command. To revert to the default local accounting, use the **no** form of the command.

aaa accounting default {**group** *group-name* [**none**] | **none**} | **local** [**none**] | **none**}

no aaa accounting default {**group** *group-name* [**none**] | **none**} | **local** [**none**] | **none**}

Syntax Description

group *group-name*	Specifies the group authentication method. The group name is a maximum of 127 characters.
local	Specifies the local authentication method.
none	No authentication, everyone permitted.

Defaults

Local accounting.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Specify the currently configured command preceded by a **no** in order to revert to the factory default.

Examples

The following example enables accounting to be performed using remote TACACS+ servers which are member of the group called TacServer, followed by the local accounting method:

```
switch# config t
switch(config)# aaa accounting default group TacServer
```

The following example turns off accounting.

```
switch(config)# aaa accounting default none
```

The following example reverts to the local accounting (default).

```
switch(config)# no aaa accounting default group TacServer
```

Related Commands

Command	Description
show aaa accounting	Displays the configured accounting methods.

aaa authentication dhchap default

To configure DHCHAP authentication method, use the **aaa authentication dhchap default** command in configuration mode. To revert to factory defaults, use the **no** form of the command.

aaa authentication dhchap default {**group** *group-name* [**none**] | **none**} | **local** [**none**] | **none**}}

no aaa authentication dhchap default {**group** *group-name* [**none**] | **none**} | **local** [**none**] | **none**}

Syntax Description

group *group-name*	Specifies the group name authentication method. The group name is a maximum of 127 characters.
local	Specifies local user name authentication (default).
none	Specifies no authentication.

Defaults

Local user name authentication.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The **local** option disables other authentication methods and configures local authentication to be used exclusively.

Specify the currently configured command preceded by a **no** in order to revert to the factory default.

Examples

The following example enables all DHCHAP authentication to be performed using remote TACACS+ servers which are member of the group called TacServers, followed by the local authentication.

```
switch# config terminal
switch(config)# aaa authentication dhchap default group TacServer
```

The following example reverts to the local authentication method (default).

```
switch(config)# no aaa authentication dhcahp default group TacServer
```

Related Commands

Command	Description
show aaa authentication	Displays the configured authentication methods.

aaa authentication iscsi default

To configure the iSCSI authentication method, use the **aaa authentication iscsi default** command in configuration mode. To negate the command or revert to factory defaults, use the **no** form of this command.

aaa authentication iscsi default {**group** *group-name* [**none**] | **none**} | **local** [**none**] | **none**}}

no aaa authentication iscsi default {**group** *group-name* [**none**] | **none**} | **local** [**none**] | **none**}}

Syntax Description

group *group-name*	Specifies the group name. The group name is a maximum of 127 characters.
local	Specifies local user name authentication (default).
none	Specifies no authentication.

Defaults

Local user name authentication.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The **local** option disables other authentication methods and configures local authentication to be used exclusively.

Specify the currently configured command preceded by a **no** in order to revert to the factory default.

Examples

The following example enables all iSCSI authentication to be performed using remote TACACS+ servers which are member of the group called TacServers, followed by the local authentication:

```
switch# config terminal
switch(config)# aaa authentication iscsi default group TacServer
```

The following example reverts to the local authentication method (default).

```
switch(config)# no aaa authentication iscsi default group TacServer
```

Related Commands

Command	Description
show aaa authentication	Displays the configured authentication methods.

aaa authentication login

To configure the authentication method for a login, use the **aaa authentication login** command in configuration mode. To revert to local authentication, use the **no** form of the command.

aaa authentication login {**default** {**group** *group-name* [**none**] | **none**} | **local** [**none**] | **none**} | **console** {*group-name* [**none**] | **none**} | **local** [**none**] | **none**}| **error-enable** | **mschap enable**}

no aaa authentication login {**default** {**group** *group-name* [**none**] | **none**} | **local** [**none**] | **none**} | **console** {*group-name* [**none**] | **none**} | **local** [**none**] | **none**}| **error-enable** | **mschap enable**}

Syntax Description

default	Configures the default method.
console	Configures the console authentication login method.
group *group-name*	Specifies the group name. The group name is a maximum of 127 characters.
local	Specifies the local authentication method.
none	Sets no authentication; everyone is permitted.
error-enable	Enables login error message display.
mschap enable	Enables MS-CHAP authentication for login.

Defaults

Local user name authentication.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.
3.0(1)	Added the **mschap** option.

Usage Guidelines

Use the **console** option to override the console login method.

Specify the currently configured command preceded by a **no** to revert to the factory default.

Examples

The following example enables all login authentication to be performed using remote TACACS+ servers, which are members of the group called TacServer, followed by the local login method.

```
switch# config t
switch(config)# aaa authentication login default group TacServer
```

The following example enables console authentication to use the group called TacServer, followed by the local login method.

```
switch(config)# aaa authentication login console group TacServer
```

The following example turns off password validation.

```
switch(config)# aaa authentication login default none
```

The following example reverts to the local authentication method (default).

```
switch(config)# no aaa authentication login default group TacServer
```

The following example enables MS-CHAP authentication for login.

```
switch(config)# aaa authentication login mschap enable
```

The following example reverts to the default authentication method for login, which is the Password Authentication Protocol (PAP).

```
switch(config)# no aaa authentication login mschap enable
```

Related Commands

Command	Description
show aaa authentication	Displays the configured authentication methods.

aaa authentication login password-aging enable

To configure password aging notifcation from AAA server , use the **aaa authentication login password-aging enable** in configuration mode. To revert to factory defaults, use the **no** form of the command.

aaa authentication login password-aging enable

no aaa authentication login password-aging enable

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

Specify the currently configured command preceded by a **no** in order to revert to the factory defaults.

Note This command is supported by the TACACS+ protocol. If you try to use the RADIUS protocol by enabling this feature, RADIUS will generate a SYSLOG message and authentication will fall back to local.

Examples

The following example enables password aging notification from AAA server:

```
switch# config terminal
switch(config)# aaa authentication login password-aging enable

The following example reverts to the Password Authentication Password (PAP) authentication
method (default)

switch(config)# no aaa authentication login password-aging enable
```

Related Commands

Command	Description
show aaa authentication login password-aging	Displays the status of the password aging notification (enabled/disabled).

aaa group server

To configure one or more independent server groups, use the **aaa group server** command in configuration mode. To remove the server group, use the **no** form of this command to remove the server group.

aaa group server {**radius** | **tacacs+**} *group-name*
server *server-name*
no server *server-name*

no aaa group server {**radius** | **tacacs+**} *group-name*

Syntax Description

radius	Specifies the RADIUS server group.
tacacs+	Specifies the TACACS+ server group.
group-name	Identifies the specified group of servers with a user-defined name. The name is limited to 64 alphanumeric characters.
server *server-name*	Specifies the server name to add or remove from the server group.

Defaults

None.

Command Modes

Configuration.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

You can configure these server groups at any time but they only take effect when you apply them to a AAA service using the **aaa authentication login** or the **aaa accounting** commands.

Examples

You can configure these server groups at any time but they only take effect when you apply them to a AAA service using the **aaa authentication** or the **aaa accounting** commands:

```
switch# config terminal
switch(config)# aaa group server tacacs+ TacacsServer1
switch(config-tacacs+)# server ServerA
switch(config-tacacs+)# exit
switch(config)# aaa group server radius RadiusServer19
switch(config-radius)# server ServerB
switch(config-radius)# no server ServerZ
```

Related Commands

Command	Description
show aaa groups	Displays all configured server groups.
show radius-server groups	Displays configured RADIUS server groups
show tacacs-server groups	Displays configured TACACS server groups

abort

To discard a Call Home configuration session in progress, use the **abort** command in Call Home configuration submode.

abort

Syntax Description

This command has no other arguments or keywords.

Defaults

None.

Command Modes

Call Home configuration submode

Command History

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

Usage Guidelines

None.

Examples

The following example shows how to discard a Call Home configuration session in progress.

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

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

active equals saved

Enable the **active equals saved** command to automatically write any changes to the block, prohibit or port address name to the IPL file. To disable the configuration or to revert to factory defaults, use the **no** form of the command.

active equals saved

no active equals saved

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled.

Command Modes

FICON configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Enabling **active equals saved** ensures that you do not have to perform the **copy running-config startup-config** command to save the FICON configuration as well as the running configuration. If your switch or fabric consists of multiple FICON-enabled VSANs, and one of these VSANs has **active equals saved** enabled, changes made to the non-FICON configuration causes all FICON-enabled configurations to be saved to the IPL file.

Note Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* for further information.

Examples

The following example enables the automatic save feature for a VSAN.

```
switch(config)# ficon vsan 2
switch(config-ficon)# active equals saved
```

The following example disables the automatic save feature for this VSAN.

```
switch(config-ficon)# no active equals saved
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration.
ficon vsan	Enables FICON on the specified VSAN.
show ficon	Displays configured FICON details.

alert-group

To customize a Call Home alert group with user-defined **show** commands, use the **alert-group** command in Call Home configuration submode. To remove the customization, user the **no** form of the command.

alert-group *event-type* **user-def-cmd** *command*

no alert-group *event-type* **user-def-cmd** *command*

Syntax DescriptionT

event-type	Specifies event types by the following alert groups.
Avanti	Displays Avanti events.
Environmental	Displays power, fan, and temperature related events.
Inventory	Displays inventory status events.
License	Displays events related to licensing.
RMON	Displays events related to Remote Monitoring (RMON).
Supervisor-Hardware	Displays supervisor related events.
Syslog-group-port	Displays events relate to syslog messages filed by the the port manager.
System	Displays software related events.
test	Displays user-generated test events.
user-def-cmd *command*	Configures a CLI command for an alert-group. The maximum size is 512.

Defaults

None.

Command Modes

Call Home configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

The **user-def-cmd** argument allows you to define a command whose outputs should be attached to the callhome message being sent. Only **show** commands can be specified and they must be associated with an alert group. Five commands can be specified per alert group. Invalid commands are rejected.

Note Make sure the destination profiles for the non-Cisco-TAC alert group, with a predefined **show** command, and the Cisco-TAC alert group are not the same.

Examples

The following example configures a user-defined command, called **show license usage**, for an alert group license:

```
switch(config-callhome)# alert-group license user-def-cmd "show license usage"
```

The following example removes a user-defined command, called **show license usage**, for an alert group license.

```
switch(config-callhome)# no alert-group license user-def-cmd "show license usage"
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

arp

To enable the Address Resolution Protocol (ARP) for the switch, use the **arp** command.To disable ARP for the switch, use the **no** form of the command.

arp *hostname*

no arp *hostname*

Syntax Description

hostname	Specifies the name of the host. Maximum length is 20 characters.

Defaults

Enabled.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example disables the Address Resolution Protocol configured for the host with the IP address 10.1.1.1.

```
switch(config)# no arp 10.1.1.1
switch(config)#
```

Related Commands

Command	Description
show arp	Displays the ARP table.
clear arp	Deletes a specific entry or all entries from the ARP table.

attach

To connect to a specific module, use the **attach** command in EXEC mode.

attach module *slot-number*

Syntax Description

module *slot-number*	Specifies the slot number of the module.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can use the **attach module** command to view the standby supervisor module information, but you cannot configure the standby supervisor module using this command.

You can also use the **attach module** command on the switching module portion of the Cisco MDS 9216 supervisor module, which resides in slot 1 of this two-slot switch.

To disconnect, use the **exit** command at the `module-number#` prompt, or type **$.** to forcibly abort the attach session.

Examples

The following example connects to the module in slot 2. Note that after you connect to the image on the module using the **attach module** command, the prompt changes to module-number#.

```
switch# attach module 1
Attaching to module 1 ...
To exit type 'exit', to abort type '$.'
module-1# exit
switch#
```

Related Commands

Command	Description
exit	Disconnects from the module.
show module	Displays the status of a module.

attachpriv

To connect to a specific ILC linecard as a privilege, use the **attach module** command in EXEC mode.

attachpriv module *slot-number*

Syntax Description

module *slot-number*	Specifies the slot number of the module.

Defaults

None.

Command Modes

EXEC mode.

Command History

Release	Modification
3.1(3)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to connect to a specific ILC linecard as a privilege:

```
switch# attachpriv module 1
Attaching to module 1 ...
To exit type 'exit', to abort type '$.'
module-1# exit
```

Related Commands

Command	Description
exit	Disconnects from the module.
show module	Displays the status of a module.

attribute qos

To configure a QOS attribute, use the **attribute qos** command in Inter-VSAN Routing (IVR) zone configuration submode. To disable this feature, use the **no** form of this command.

attribute qos *{***high** | **low** | **medium***}*

no attribute qos *{***high** | **low** | **medium***}*

Syntax Description

high	Configures frames matching zone to get high priority.
low	Configures frames matching zone to get low priority (Default).
medium	Configures frames matching zone to get medium priority.

Defaults

Disabled.

Command Modes

IVR zone configuration submode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to configure an IVR zone QOS attribute to low priority:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ivr zone name IvrZone
switch(config-ivr-zone)# attribute qos priority low
```

Related Commands

Command	Description
show ivr zone	Displays IVR zone configuration.

authentication

To configure the authentication method for an IKE protocol policy, use the **authentication** command in IKE policy configuration submode. To revert to the default authentication method, use the **no** form of the command.

authentication *{***pre-share** | **rsa-sig***}*

no authentication *{***pre-share** | **rsa-sig***}*

Syntax Description

pre-share	Configures the preshared key as the authentication method.
rsa-sig	Configures RSA signatures as the authentication method.

Defaults

Preshared key.

Command Modes

IKE policy configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

To use this command, enable the IKE protocol using the **crypto ike enable** command. In addition, you must configure the identity authentication mode using the fully qualified domain name (FQDN) before you can use RSA signatures for authentication. Use the **identity hostname** command for this purpose.

Examples

The following example shows how to configure the authentication method using the preshared key.

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# policy 1
switch(config-ike-ipsec-policy)# authentication pre-share
```

The following example shows how to configure the authentication method using the RSA signatures.

```
switch(config-ike-ipsec-policy)# authentication rsa-sig
```

The following example shows how to revert to the default authentication method (preshared key).

```
switch(config-ike-ipsec-policy)# no authentication rsa-sig
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
identity hostname	Configures the identity for the IKE protocol.
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

autonomous-fabric-id (IVR topology database configuration)

To configure an autonomous fabric ID (AFID) into the Inter-VSAN Routing (IVR) topology database, use the **autonomous-fabric-id** command. To remove the fabric ID, use the **no** form of the command.

autonomous-fabric-id *fabric-id* **switch-wwn** *swwn* **vsan-ranges** *vsan-id*

no autonomous-fabric-id *fabric-id* **switch-wwn** *swwn* **vsan-ranges** *vsan-id*

Syntax Description

fabric-id	Specifies the fabric ID for the IVR topology. **Note** For Cisco MDS SAN-OS images prior to release 2.1(1a), the *fabric-id value is limited to 1*. For Releases 2.1(1a) and later images, the *fabric-id* range is 1 to 64.
switch-wwn *swwn*	Configures the switch WWN in dotted hex format.
vsan-ranges *vsan-id*	Configures up to five ranges of VSANs to be added to the database. The range is 1 to 4093.

Defaults

None.

Command Modes

IVR topology database configuration submode.

Command History

Release	Modification
1.3(1)	This command was introduced.
2.1(1a)	Modified range for *fabric-id*.

Usage Guidelines

The following rules apply to configuring AFIDs to VSANs:

- The default AFID of a VSAN is 1.
- Each VSAN belongs to one and only one AFID.
- A switch can be a member of multiple AFIDs.
- AFIDs at a switch must not share any VSAN identifier (for example, a VSAN at a switch can belong to only one AFID).
- A VSAN identifier can be reused in different AFIDs, without merging the VSANs, as long as those AFIDs do not share a switch.

You can have up to 64 VSANs (or 128 VSANs for Cisco MDS SAN-OS Release 2.1(1a) or later) in an IVR topology. Specify the IVR topology using the following information:

- The switch WWNs of the IVR-enabled switches.
- A minimum of two VSANs to which the IVR-enabled switch belongs.

- The autonomous fabric ID (AFID), which distinguishes two VSANs that are logically and physically separate, but have the same VSAN number. Cisco MDS SAN-OS Release 1.3(1) and later supports only one default AFID (AFID 1) and thus does not support non-unique VSAN IDs in the network. As of Cisco MDS SAN-OS Release 2.1(1a), you can specify up to 64 AFIDs.

Note Two VSANs with the same VSAN number but different fabric IDs are counted as two VSANs out o f the 128 total VSANs allowed in the fabric.

The following command enters the configuration mode, enables the IVR feature, enters the VSAN topology database, and configures the pWWN-VSAN association for VSANs 2 and 2000.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr enable
switch(config)# ivr vsan-topology database
switch(config-ivr-topology-db)# autonomous-fabric-id 1 switch 20:00:00:00:30:00:3c:5e
vsan-ranges 2,2000
```

Related Commands

Command	Description
ivr enable	Enables the Inter-VSAN Routing (IVR) feature.
ivr vsan-topology database	Configures a VSAN topology database.
show autonomous-fabric-id database	Displays the contents of the AFID database.
show ivr	Displays IVR feature information.

autonomous-fabric-id (IVR service group configuration)

To configure an autonomous fabric ID (AFID) into an IVR service group, use the **autonomous-fabric-id** command in IVR service group configuration submode. To remove the autonomous fabric ID, use the **no** form of the command.

autonomous-fabric-id *afid* **vsan-ranges** *vsan-id*

no autonomous-fabric-id *afid* **vsan-ranges** *vsan-id*

Syntax Description

afid	Specifies the AFID to the local VSAN.
vsan-ranges *vsan-id*	Configures up to five ranges of VSANs to be added to the service group. The range is 1 to 4093.

Defaults

None.

Command Modes

IVR service group configuration submode.

Command History

Release	Modification
2.1	This command was introduced.

Usage Guidelines

Before configuring an IVR service group, you must enable the following:

- IVR using the **ivr enable** command
- IVR distribution using the **ivr distribute** command
- Automatic IVR topology discovery using the **ivr vsan-topology auto command**

To change to IVR service group configuration submode, use the **ivr service-group activate command.**

Examples

The following command enters the IVR service group configuration submode and configures AFID 10 to be in IVR service group serviceGroup1.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr enable
switch(config)# ivr distribute
switch(config)# ivr vsan-topology auto
switch(config)# ivr service-group name serviceGroup1
switch(config-ivr-sg)# autonomous-fabric-id 10 vsan 1-4
```

Related Commands

Command	Description
ivr enable	Enables the Inter-VSAN Routing (IVR) feature.
ivr service-group name	Configures an IVR service group and changes to IVR service group configuration submode.
show autonomous-fabric-id database	Displays the contents of the AFID database.
show ivr	Displays IVR feature information.

autonomous-fabric-id database

To configure an autonomous fabric ID (AFID) database, use the **autonomous-fabric-id database** command. To remove the fabric AFID database, use the **no** form of the command.

autonomous-fabric-id database

no autonomous-fabric-id database

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Configuration mode.

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

You must configure the IVR VSAN topology to auto mode, using the **ivr vsan-topology auto** command, before you can use the **autonomous-fabric-id database** command to modify the database. The **autonomous-fabric-id database** command also enters AFID database configuration submode.

Note In user-configured VSAN topology mode, the AFIDs are specified in the IVR VSAN topology configuration itself and a separate AFID configuration is not needed.

Examples

The following example shows how to create an AFID database and enters AFID database configuration submode.

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# autonomous-fabric-id database
switch(config-afid-db)#
```

Related Commands

Command	Description
ivr vsan-topology auto	Configures a VSAN topology for Inter-VSAN Routing (IVR) to auto configuration mode.
switch-wwn	Configures a switch WWN in the autonomous fabric ID (AFID) database
show autonomous-fabric-id database	Displays the contents of the AFID database.
show ivr	Displays IVR feature information.

auto-volgrp

To configure the automatic volume grouping, use the **auto-volgrp** command. To disable this feature, use the **no** form of the command.

auto-volgrp

no auto-volgrp

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Cisco SME cluster configuration submode.

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

If Cisco SME recognizes that the tape's barcode does not belong to an existing volume group, then a new volume group is created when automatic volume grouping is enabled.

Examples

The following example enables automatic volume grouping:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# auto-volgrp
switch(config-sme-cl)#
```

The following example disables automatic volume grouping:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# auto-volgrp
switch(config-sme-cl)#
```

Related Commands

Command	Description
show sme cluster	Displays Cisco SME cluster information.