Advanced Features and Concepts

This chapter describes the advanced features provided in switches in the Cisco MDS 9000 Family. It includes the following sections:

Common Information Model

Common Information Model (CIM) is an object-oriented information model that extends the existing standards for describing management information in a network/enterprise environment.

CIM messages are independent of platform and implementation because they are encoded in N Extensible Markup Language (XML). CIM consists of a specification and a schema. The specification defines the syntax and rules for describing management data and integrating with other management models. The schema provides the actual model descriptions for systems, applications, networks, and devices.

For more information about CIM, refer to the specification available through the Distributed Management Task Force (DMTF) website at the following URL: http://www.dmtf.org/

Note The CIM Functionality and SMI-S is now supported with Cisco Prime Data Center Network Manager (DCNM). Please refer to "Cisco Prime DCNM Installation Guide" and "SMI-S and Web Services Programming Guide, Cisco DCNM for SAN.

Fibre Channel Time-Out Values

You can modify Fibre Channel protocol related timer values for the switch by configuring the following time-out values (TOVs):

- Distributed services TOV (D_S_TOV)—The valid range is from 5,000 to 10,000 milliseconds. The default is 5,000 milliseconds.

- Error detect TOV (E_D_TOV)—The valid range is from 1,000 to 4,000 milliseconds. The default is 2,000 milliseconds. This value is matched with the other end during port initialization.

- Resource allocation TOV (R_A_TOV)—The valid range is from 5,000 to 10,000 milliseconds. The default is 10,000 milliseconds. This value is matched with the other end during port initialization.

Note The fabric stability TOV (F_S_TOV) constant cannot be configured.

This section includes the following topics:

Timer Configuration Across All VSANs

You can modify Fibre Channel protocol related timer values for the switch.

Caution The D_S_TOV, E_D_TOV, and R_A_ TOV values cannot be globally changed unless all VSANs in the switch are suspended.

Note If a VSAN is not specified when you change the timer value, the changed value is applied to all VSANs in the switch.

To configure Fibre Channel timers across all VSANs, follow these steps:

Step 1 switch# **config terminal**
switch(config)

Enters configuration mode.

Step 2 switch(config)# **fctimer R_A_TOV 6000**
Configures the R_A_TOV value for all VSANs to be 6000 msec. This type of configuration is not permitted unless all VSANs are suspended.

Timer Configuration Per-VSAN

You can also issue the fctimer for a specified VSAN to configure different TOV values for VSANs with special links like FC or IP tunnels. You can configure different E_D_TOV, R_A_TOV, and D_S_TOV values for individual VSANs. Active VSANs are suspended and activated when their timer values are changed.

⚠️

Caution You cannot perform a nondisruptive downgrade to any earlier version that does not support per-VSAN FC timers.

✎

Note This configuration must be propagated to all switches in the fabric—be sure to configure the same value in all switches in the fabric.

If a switch is downgraded to Cisco MDS SAN-OS Release 1.2 or 1.1 after the timer is configured for a VSAN, an error message is issued to warn against strict incompatibilities. Refer to the *Cisco MDS 9000 Family Troubleshooting Guide*.

To configure per-VSAN Fiber Channel timers, follow these steps:

Step 1 switch# **config terminal**
switch(config)#

Enters configuration mode.

Step 2 switch(config)# **fctimer D_S_TOV 6000 vsan 2**

```
Warning: The vsan will be temporarily suspended when updating the timer value This configuration
would impact whole fabric. Do you want to continue? (y/n) y

Since this configuration is not propagated to other switches, please configure the same value in all
 the switches
```

Configures the D_S_TOV value to be 6000 msec for VSAN 2. Suspends the VSAN temporarily. You have the option to end this command, if required.

About fctimer Distribution

You can enable per-VSAN fctimer fabric distribution for all Cisco MDS switches in the fabric. When you perform fctimer configurations, and distribution is enabled, that configuration is distributed to all the switches in the fabric.

You automatically acquire a fabric-wide lock when you issue the first configuration command after you enabled distribution in a switch. The fctimer application uses the effective and pending database model to store or commit the commands based on your configuration.

Refer to the *Cisco MDS 9000 Family NX-OS System Management Configuration Guide* for more information on the CFS application.

Enabling fctimer Distribution

To enable or disable fctimer fabric distribution, follow these steps:

Step 1   switch# **config terminal**
switch(config)#

Enters configuration mode.

Step 2   switch(config)# **fctimer distribute**
Enables fctimer configuration distribution to all switches in the fabric. Acquires a fabric lock and stores all future configuration changes in the pending database.

Step 3   switch(config)# **no fctimer distribute**
Disables (default) fctimer configuration distribution to all switches in the fabric.

Committing fctimer Changes

When you commit the fctimer configuration changes, the effective database is overwritten by the configuration changes in the pending database and all the switches in the fabric receive the same configuration. When you commit the fctimer configuration changes without implementing the session feature, the fctimer configurations are distributed to all the switches in the physical fabric.

To commit the fctimer configuration changes, follow these steps:

Step 1   switch# **config terminal**
switch(config)#

Enters configuration mode.

Step 2   switch(config)# **fctimer commit**
Distributes the fctimer configuration changes to all switches in the fabric and releases the lock. Overwrites the effective database with the changes made to the pending database.

Discarding fctimer Changes

After making the configuration changes, you can choose to discard the changes by discarding the changes instead of committing them. In either case, the lock is released.

To discard the fctimer configuration changes, follow these steps:

Step 1   switch# **config terminal**
switch(config)#

Enters configuration mode.

Step 2   switch(config)# **fctimer abort**
Discards the fctimer configuration changes in the pending database and releases the fabric lock.

Fabric Lock Override

If you have performed a fctimer fabric task and have forgotten to release the lock by either committing or discarding the changes, an administrator can release the lock from any switch in the fabric. If the administrator performs this task, your changes to the pending database are discarded and the fabric lock is released.

Tip   The changes are only available in the volatile directory and are subject to being discarded if the switch is restarted.

To use administrative privileges and release a locked fctimer session, use the **clear fctimer session** command.

```
switch# clear fctimer session
```

Database Merge Guidelines

For information about CFS merge support, refer to the *Cisco MDS 9000 Family NX-OS System Management Configuration Guide* .

When merging two fabrics, follow these guidelines:

- Be aware of the following merge conditions:

  ◦ The merge protocol is not implemented for distribution of the fctimer values—you must manually merge the fctimer values when a fabric is merged.The per-VSAN fctimer configuration is distributed in the physical fabric.

  ◦ The fctimer configuration is only applied to those switches containing the VSAN with a modified fctimer value.

  ◦ The global fctimer values are not distributed.

- Do not configure global timer values when distribution is enabled.

> **Note** The number of pending fctimer configuration operations cannot be more than 15. At that point, you must commit or abort the pending configurations before performing any more operations.

Displaying Configured fctimer Values

Use the **show fctimer** command to display the configured fctimer values (see the following examples).

Displays Configured Global TOVs

```
switch# show fctimer

F_S_TOV    D_S_TOV    E_D_TOV    R_A_TOV
---------------------------------------
5000 ms    5000 ms    2000 ms    10000 ms
```

> **Note** The F_S_TOV constant, though not configured, is displayed in the output of the **show fctimer** command.

Displays Configured TOVs for a Specified VSAN

```
switch# show fctimer vsan 10

vsan no.   F_S_TOV    D_S_TOV    E_D_TOV    R_A_TOV
--------------------------------------------------
10         5000 ms    5000 ms    3000 ms    10000 ms
```

Organizationally Unique Identifiers

Organizationally Unique Identifiers (OUIs) are unique 24 bit numbers that identify an organization globally. OUIs are extended by the organisation they are assigned to, to create 48 bit or 60 bit Extended Unique Identifiers (EUIs). Cisco obtains OUIs from IEEE and uses them to construct EUIs. These are assigned and burnt in to each system. A system may have one or more EUIs assigned to it. The EUIs are used in various forms such as MAC addresses, WWNs, SNMP identifiers, and so on.

Cisco MDS NX-OS software has an OUI database based on which certain software functionalities are made available. If a new Cisco device with an unrecognized OUI is added to a fabric, there is a possibility that some of these functionalities might be affected. To avoid this issue, the ability to manually add OUIs to the OUI database using the CLI is available.

Guidelines and Limitations

- ISSU—After an upgrade, there may be instances of duplicate OUIs in the default (built-in) and static (user defined) lists. In such a scenario, we recommend that you compare static OUIs with those in the default list and delete the duplicate static OUIs.

- ISSD—Delete all the configured or static OUIs before performing a downgrade to a release that does not support the **wwn oui** *oui-id* command.

For more information on deleting OUIs, see the section.

Adding and Deleting OUIs

To add an OUI to the OUI database, enter the **wwn oui** *oui-id* command in global configuration mode. To delete an OUI from the OUI database, enter the **no wwn oui** *oui-id* command in global configuration mode.

For detailed information about the **wwn oui** command, see the *Cisco MDS 9000 Family Command Reference*.

Configuration Examples for Adding and Deleting OUIs

Example: Adding and Deleting OUIs

```
switch# configure terminal
switch(config)# wwn oui 0x10001c
switch(config)# no wwn oui 0x10001c
switch(config)# end
```

Example: Displaying OUIs

```
switch# show wwn oui
OUI        Vendor             Default/Static
------------------------------------------------
0x0000fc   Cisco              Static
0x00000c   Cisco              Default
0x000196   Cisco              Default
0x000197   Cisco              Default
0x0001c7   Cisco              Default
0x0001c9   Cisco              Default
```

World Wide Names

The world wide name (WWN) in the switch is equivalent to the Ethernet MAC address. As with the MAC address, you must uniquely associate the WWN to a single device. The principal switch selection and the allocation of domain IDs rely on the WWN. The WWN manager, a process-level manager residing on the switch's supervisor module, assigns WWNs to each switch.

Cisco MDS 9000 Family switches support three network address authority (NAA) address formats (see Table 1: Standardized NAA WWN Formats , on page 7).

Table 1: Standardized NAA WWN Formats

NAA Address	NAA Type	WWW Format	
IEEE 48-bit address	Type 1 = 0001b	000 0000 0000b	48-bit MAC address
IEEE extended	Type 2 = 0010b	Locally assigned	48-bit MAC address
IEEE registered	Type 5 = 0101b	IEEE company ID: 24 bits	VSID: 36 bits

⚠️

Caution Changes to the world-wide names should be made by an administrator or individual who is completely familiar with switch operations.

This section includes the following topics:

Displaying WWN Information

Use the **show wwn** commands to display the status of the WWN configuration. See the following examples:

Displays the Status of All WWNs

```
switch# show wwn status
         Type 1 WWNs: Configured:     64 Available:     48 (75%) Resvd.: 16
     Types 2 & 5 WWNs: Configured: 524288 Available: 450560 (85%) Resvd.: 73728
NKAU & NKCR WWN Blks: Configured:   1760 Available:   1760 (100%)
         Alarm Status:      Type1:   NONE Types 2&5:   NONE
```

Displays Specified Block ID Information

```
switch# show wwn status block-id 51

WWNs in this block: 21:00:ac:16:5e:52:00:03 to 21:ff:ac:16:5e:52:00:03
Num. of WWNs:: Configured: 256 Allocated:    0 Available: 256
Block Allocation Status: FREE
```

Displays the WWN for a Specific Switch

```
switch# show wwn switch
Switch WWN is 20:00:ac:16:5e:52:00:00
```

Link Initialization WWN Usage

Exchange Link Protocol (ELP) and Exchange Fabric Protocol (EFP) use WWNs during link initialization. The usage details differ based on the Cisco NX-OS software release.

Both ELPs and EFPs use the VSAN WWN by default during link initialization. However, the ELP usage changes based on the peer switch's usage:

- If the peer switch ELP uses the switch WWN, then the local switch also uses the switch WWN.

- If the peer switch ELP uses the VSAN WWN, then the local switch also uses the VSAN WWN.

✎

Note As of Cisco SAN-OS Release 2.0(2b), the ELP is enhanced to be compliant with FC-SW-3.

Configuring a Secondary MAC Address

To allocate secondary MAC addresses, follow these steps:

Step 1   switch# **config terminal**
switch(config)#

Enters configuration mode.

Step 2   switch(config)# **wwn secondary-mac 00:99:55:77:55:55 range 64**

```
This command CANNOT be undone.


Please enter the BASE MAC ADDRESS again: 00:99:55:77:55:55

Please enter the mac address RANGE again: 64

From now on WWN allocation would be based on new MACs.

Are you sure? (yes/no) no

You entered: no. Secondary MAC NOT programmed
```
Configures the secondary MAC address. This command cannot be undone.

FC ID Allocation for HBAs

Fibre Channel standards require a unique FC ID to be allocated to an N port attached to a Fx port in any switch. To conserve the number of FC IDs used, Cisco MDS 9000 Family switches use a special allocation scheme.

Some HBAs do not discover targets that have FC IDs with the same domain and area. Prior to Cisco SAN-OS Release 2.0(1b), the Cisco SAN-OS software maintained a list of tested company IDs that do not exhibit this behavior. These HBAs were allocated with single FC IDs, and for others a full area was allocated.

The FC ID allocation scheme available in Release 1.3 and earlier, allocates a full area to these HBAs. This allocation isolates them to that area and are listed with their pWWN during a fabric login. The allocated FC IDs are cached persistently and are still available in Cisco SAN-OS Release 2.0(1b) (see the FC ID Allocation for HBAs, on page 9).

To allow further scalability for switches with numerous ports, the Cisco NX-OS software maintains a list of HBAs exhibiting this behavior. Each HBA is identified by its company ID (also known known as Organizational Unique Identifier, or OUI) used in the pWWN during a fabric login. A full area is allocated to the N ports with company IDs that are listed, and for the others a single FC ID is allocated. Regardless of the kind (whole area or single) of FC ID allocated, the FC ID entries remain persistent.

This section includes the following topics:

Default Company ID List

All switches in the Cisco MDS 9000 Family that ship with Cisco SAN-OS Release 2.0(1b) or later, or NX-OS 4.1(1) contain a default list of company IDs that require area allocation. Using the company ID reduces the number of configured persistent FC ID entries. You can configure or modify these entries using the CLI.

⚠️

Caution Persistent entries take precedence over company ID configuration. If the HBA fails to discover a target, verify that the HBA and the target are connected to the same switch and have the same area in their FC IDs, then perform the following procedure:1. Shut down the port connected to the HBA.2. Clear the persistent FC ID entry.3. Get the company ID from the Port WWN.4. Add the company ID to the list that requires area allocation.5. Bring up the port.

The list of company IDs have the following characteristics:

- A persistent FC ID configuration always takes precedence over the list of company IDs. Even if the company ID is configured to receive an area, the persistent FC ID configuration results in the allocation of a single FC ID.

- New company IDs added to subsequent releases are automatically added to existing company IDs.

- The list of company IDs is saved as part of the running and saved configuration.

- The list of company IDs is used only when the fcinterop FC ID allocation scheme is in auto mode. By default, the interop FC ID allocation is set to auto, unless changed.

🔍

Tip We recommend that you set the fcinterop FC ID allocation scheme to auto and use the company ID list and persistent FC ID configuration to manipulate the FC ID device allocation.

Use the **fcinterop FCID allocation auto** command to change the FC ID allocation and the **show running-config** command to view the currently allocated mode.

- When you issue a **write erase**, the list inherits the default list of company IDs shipped with a relevant release.

To allocate company IDs, follow these steps:

Step 1 switch# **config terminal**
switch(config)#
Enters configuration mode.

Step 2 switch(config)# **fcid-allocation area company-id 0x003223**
Adds a new company ID to the default list.

Step 3 switch(config)# **no fcid-allocation area company-id 0x00E069**
Deletes a company ID from the default list.

Step 4 switch(config)# **fcid-allocation area company-id 0x003223**
Adds a new company ID to the default list.

Verifying the Company ID Configuration

You can view the configured company IDs by issuing the **show fcid-allocation area** command (see Displays the List of Default and Configured Company IDs, on page 11). Default entries are listed first and the user-added entries are listed next. Entries are listed even if they were part of the default list and you later removed them.

Displays the List of Default and Configured Company IDs

```
switch# show fcid-allocation area
FCID area allocation company id info:
 00:50:2E <------------------- Default entry
 00:50:8B
 00:60:B0
 00:A0:B8
 00:E0:69
 00:30:AE + <----------------- User-added entry
 00:32:23 +
 00:E0:8B * <------------ Explicitly deleted entry (from the original default list)
Total company ids: 7
+ - Additional user configured company ids.
* - Explicitly deleted company ids from default list.
```

You can implicitly derive the default entries shipped with a specific release by combining the list of Company IDs displayed without any identification with the list of deleted entries.

You can also view or obtain the company IDs in a specific WWN by issuing the **show fcid-allocation company-id-from-wwn** command (see Displays the Company ID for the Specified WWN, on page 11). Some WWN formats do not support company IDs. In these cases, you many need to configure the FC ID persistent entry.

Displays the Company ID for the Specified WWN

```
switch# show fcid-allocation company-id-from-wwn 20:00:00:05:30:00:21:60
Extracted Company ID: 0x000530
```

Switch Interoperability

Interoperability enables the products of multiple vendors to interact with each other. Fibre Channel standards guide vendors towards common external Fibre Channel interfaces.

If all vendors followed the standards in the same manner, then interconnecting different products would become a trivial exercise. However, not all vendors follow the standards in the same way, thus resulting in interoperability modes. This section briefly explains the basic concepts of these modes.

Each vendor has a regular mode and an equivalent interoperability mode, which specifically turns off advanced or proprietary features and provides the product with a more amiable standards-compliant implementation.

Note For more information on configuring interoperability for the Cisco MDS 9000 Family switches, refer to the *Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide* .

This section includes the following topics:

About Interop Mode

Cisco NX-OS software supports the following four interop modes:

- Mode 1— Standards based interop mode that requires all other vendors in the fabric to be in interop mode.

- Mode 2—Brocade native mode (Core PID 0).

- Mode 3—Brocade native mode (Core PID 1).

- Mode 4—McData native mode.

For information about configuring interop modes 2, 3, and 4, refer to the *Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide* .

lists the changes in switch behavior when you enable interoperability mode. These changes are specific to switches in the Cisco MDS 9000 Family while in interop mode.

Table 2: Changes in Switch Behavior When Interoperability Is Enabled

Switch Feature	Changes if Interoperability Is Enabled
Domain IDs	Some vendors cannot use the full range of 239 domains within a fabric.
	Domain IDs are restricted to the range 97-127. This is to accommodate McData's nominal restriction to this same range. They can either be set up statically (the Cisco MDS switch accept only one domain ID, if it does not get that domain ID it isolates itself from the fabric) or preferred. (If it does not get its requested domain ID, it accepts any assigned domain ID.)
Timers	All Fibre Channel timers must be the same on all switches as these values are exchanged by E ports when establishing an ISL. The timers are F_S_TOV, D_S_TOV, E_D_TOV, and R_A_TOV.
F_S_TOV	Verify that the Fabric Stability Time Out Value timers match exactly.
D_S_TOV	Verify that the Distributed Services Time Out Value timers match exactly.
E_D_TOV	Verify that the Error Detect Time Out Value timers match exactly.
R_A_TOV	Verify that the Resource Allocation Time Out Value timers match exactly.

Switch Feature	Changes if Interoperability Is Enabled
Trunking	Trunking is not supported between two different vendor's switches. This feature may be disabled on a per port or per switch basis.
Default zone	The default zone behavior of permit (all nodes can see all other nodes) or deny (all nodes are isolated when not explicitly placed in a zone) may change.
Zoning attributes	Zones may be limited to the pWWN and other proprietary zoning methods (physical port number) may be eliminated. **Note** Brocade uses the **cfgsave** command to save fabric-wide zoning configuration. This command does not have any effect on Cisco MDS 9000 Family switches if they are part of the same fabric. You must explicitly save the configuration on each switch in the Cisco MDS 9000 Family.
Zone propagation	Some vendors do not pass the full zone configuration to other switches, only the active zone set gets passed. Verify that the active zone set or zone configuration has correctly propagated to the other switches in the fabric.
VSAN	Interop mode only affects the specified VSAN. **Note** Interop modes cannot be enabled on FICON-enabled VSANs.
TE ports and PortChannels	TE ports and PortChannels cannot be used to connect Cisco MDS to non-Cisco MDS switches. Only E ports can be used to connect to non-Cisco MDS switches. TE ports and PortChannels can still be used to connect an Cisco MDS to other Cisco MDS switches even when in interop mode.
FSPF	The routing of frames within the fabric is not changed by the introduction of interop mode. The switch continues to use src-id, dst-id, and ox-id to load balance across multiple ISL links.
Domain reconfiguration disruptive	This is a switch-wide impacting event. Brocade and McData require the entire switch to be placed in offline mode and/or rebooted when changing domain IDs.

Switch Feature	Changes if Interoperability Is Enabled
Domain reconfiguration nondisruptive	This event is limited to the affected VSAN. Only Cisco MDS 9000 Family switches have this capability—only the domain manager process for the affected VSAN is restarted and not the entire switch.
Name server	Verify that all vendors have the correct values in their respective name server database.
IVR	IVR-enabled VSANs can be configured in **no interop** (default) mode or in any of the **interop** modes.

Configuring Interop Mode 1

The interop mode1 in Cisco MDS 9000 Family switches can be enabled disruptively or nondisruptively.

Note Brocade's msplmgmtdeactivate command must explicitly be run prior to connecting from a Brocade switch to either Cisco MDS 9000 Family switches or to McData switches. This command uses Brocade proprietary frames to exchange platform information, which Cisco MDS 9000 Family switches or McData switches do not understand. Rejecting these frames causes the common E ports to become isolated.

To configure interop mode 1 in any switch in the Cisco MDS 9000 Family, follow these steps:

Step 1 Place the VSAN of the E ports that connect to the OEM switch in interoperability mode.

```
switch# config terminal
switch(config)# vsan database
switch(config-vsan-db)# vsan 1 interop 1
switch(config-vsan-db)# exit
switch(config)#
```

Note You cannot enable interop modes on FICON-enabled VSANs.

Step 2 Assign a domain ID in the range of 97 (0x61) through 127 (0x7F).

Note This is an limitation imposed by the McData switches.

```
switch(config)# fcdomain domain 100 preferred vsan 1
```

In Cisco MDS 9000 switches, the default is to request an ID from the principal switch. If the preferred option is used, Cisco MDS 9000 switches request a specific ID, but still join the fabric if the principal switch assigns a different ID. If the static option is used, the Cisco MDS 9000 switches do not join the fabric unless the principal switch agrees and assigns the requested ID.

Note When changing the domain ID, the FC IDs assigned to N ports also change.

Step 3 Change the Fibre Channel timers (if they have been changed from the system defaults).

Note The Cisco MDS 9000, Brocade, and McData FC Error Detect (ED_TOV) and Resource Allocation (RA_TOV) timers default to the same values. They can be changed if needed. The RA_TOV default is 10 seconds, and the ED_TOV default is 2 seconds. Per the FC-SW2 standard, these values must be the same on each switch within the fabric.

```
switch(config)# fctimer e_d_tov ?
  <1000-4000>  E_D_TOV in milliseconds(1000-4000)
switch(config)# fctimer r_a_tov ?
  <5000-100000>  R_A_TOV in milliseconds(5000-100000)
```

Step 4 When making changes to the domain, you may or may not need to restart the Cisco MDS domain manager function for the altered VSAN.

- Force a fabric reconfiguration with the **disruptive** option.

```
switch(config)# fcdomain restart disruptive vsan 1
```
or

- Do not force a fabric reconfiguration.

```
switch(config# fcdomain restart vsan 1
```

Configuring Interop Mode 1

commandsTo verify the resulting status of issuing the interoperability command in any switch in the Cisco MDS 9000 Family, follow these steps:

SUMMARY STEPS

1. Use the **show version** command to verify the version.
2. Use the **show interface brief** command to verify if the interface states are as required by your configuration.
3. Use the **show run** command to verify if you are running the desired configuration.
4. Use the **show vsan** command to verify if the interoperability mode is active.
5. Use the **show fcdomain vsan** command to verify the domain ID.
6. Use the **show fcdomain domain-list vsan** command to verify the local principal switch status.
7. Use the **show fspf internal route vsan** command to verify the next hop and destination for the switch.
8. Use the **show fcns data vsan** command to verify the name server information.

DETAILED STEPS

Step 1 Use the **show version** command to verify the version.

```
switch# show version

Cisco Storage Area Networking Operating System (NX-OS) Software
```

```
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2003, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
Cisco Systems, Inc. and/or other third parties and are used and
distributed under license. Some parts of this software are covered
under the GNU Public License. A copy of the license is available
at http://www.gnu.org/licenses/gpl.html.
Software
  BIOS:      version 1.0.8
  loader:    version 1.1(2)
  kickstart: version 2.0(1) [build 2.0(0.6)] [gdb]
  system:    version 2.0(1) [build 2.0(0.6)] [gdb]
  BIOS compile time:       08/07/03
  kickstart image file is: bootflash:///m9500-sf1ek9-kickstart-mzg.2.0.0.6.bin
  kickstart compile time:  10/25/2010 12:00:00
  system image file is:    bootflash:///m9500-sf1ek9-mzg.2.0.0.6.bin
  system compile time:     10/25/2020 12:00:00
Hardware
  RAM 1024584 kB
  bootflash: 1000944 blocks (block size 512b)
  slot0:          0 blocks (block size 512b)
  172.22.92.181 uptime is 0 days 2 hours 18 minute(s) 1 second(s)
  Last reset at 970069 usecs after Tue Sep 16 22:31:25 1980
    Reason: Reset Requested by CLI command reload
    System version: 2.0(0.6)
    Service:
```

Step 2   Use the **show interface brief** command to verify if the interface states are as required by your configuration.

```
switch# show int brief
Interface  Vsan  Admin  Admin  Status          Oper  Oper    Port-channel
                 Mode   Trunk                  Mode  Speed
                        Mode                         (Gbps)
-------------------------------------------------------------------
fc2/1      1     auto   on     up              E     2       --
fc2/2      1     auto   on     up              E     2       --
fc2/3      1     auto   on     fcotAbsent      --    --      --
fc2/4      1     auto   on     down            --    --      --
fc2/5      1     auto   on     down            --    --      --
fc2/6      1     auto   on     down            --    --      --
fc2/7      1     auto   on     up              E     1       --
fc2/8      1     auto   on     fcotAbsent      --    --      --
fc2/9      1     auto   on     down            --    --      --
fc2/10     1     auto   on     down            --    --      --
```

Step 3   Use the **show run** command to verify if you are running the desired configuration.

```
switch# show run
Building Configuration...
 interface fc2/1
no shutdown
 interface fc2/2
no shutdown
 interface fc2/3
 interface fc2/4
```

```
 interface fc2/5
 interface fc2/6
 interface fc2/7
no shutdown
 interface fc2/8
 interface fc2/9
 interface fc2/10

<snip>

interface fc2/32
 interface mgmt0
ip address 6.1.1.96 255.255.255.0
switchport encap default
no shutdown
vsan database
vsan 1 interop
boot system bootflash:/m9500-system-253e.bin sup-1
boot kickstart bootflash:/m9500-kickstart-253e.bin sup-1
boot system bootflash:/m9500-system-253e.bin sup-2
boot kickstart bootflash:/m9500-kickstart-253e.bin sup-2
callhome
fcdomain domain 100 preferred vsan 1
ip route 6.1.1.0 255.255.255.0 6.1.1.1
ip routing
line console
  databits 5
  speed 110
logging linecard
ssh key rsa 512 force
ssh server enable
switchname MDS9509
username admin password 5 $1$Li8/fBYX$SNc72.xt4nTXpSnR9OUFB/ role network-admin
```

Step 4 Use the **show vsan** command to verify if the interoperability mode is active.

```
switch# show vsan 1
vsan 1 information
        name:VSAN0001 stalactites
        interoperability mode:yes
<--------------------
verify mode
        loadbalancing:src-id/dst-id/oxid
        operational state:up
```

Step 5 Use the **show fcdomain vsan** command to verify the domain ID.

```
switch# show fcdomain vsan 1
The local switch is a Subordinated Switch.
Local switch run time information:
        State: Stable
        Local switch WWN:    20:01:00:05:30:00:51:1f
        Running fabric name: 10:00:00:60:69:22:32:91
        Running priority: 128
        Current domain ID: 0x64(100)
```

```
<--------------
verify domain id
Local switch configuration information:
        State: Enabled
        Auto-reconfiguration: Disabled
        Contiguous-allocation: Disabled
        Configured fabric name: 41:6e:64:69:61:6d:6f:21
        Configured priority: 128
        Configured domain ID: 0x64(100) (preferred)
Principal switch run time information:
        Running priority: 2
Interface              Role          RCF-reject
----------------    -------------   ------------
fc2/1                  Downstream     Disabled
fc2/2                  Downstream     Disabled
fc2/7                  Upstream       Disabled
----------------    -------------   ------------
```

Step 6   Use the **show fcdomain domain-list vsan** command to verify the local principal switch status.

```
switch# show fcdomain domain-list vsan 1
Number of domains: 5
Domain ID            WWN
---------    -----------------------
 0x61(97)    10:00:00:60:69:50:0c:fe
 0x62(98)    20:01:00:05:30:00:47:9f
 0x63(99)    10:00:00:60:69:c0:0c:1d
0x64(100)    20:01:00:05:30:00:51:1f [Local]
0x65(101)    10:00:00:60:69:22:32:91 [Principal]
---------    -----------------------
```

Step 7   Use the **show fspf internal route vsan** command to verify the next hop and destination for the switch.

```
switch# show fspf internal route vsan 1
FSPF Unicast Routes
---------------------------
 VSAN Number  Dest Domain   Route Cost   Next hops
------------------------------------------------
          1    0x61(97)          500       fc2/2
          1    0x62(98)         1000       fc2/1
                                           fc2/2
          1    0x63(99)          500       fc2/1
          1    0x65(101)        1000       fc2/7
```

Step 8   Use the **show fcns data vsan** command to verify the name server information.

```
switch# show fcns data vsan 1
VSAN 1:
--------------------------------------------------------------------
FCID       TYPE  PWWN                    (VENDOR) FC4-TYPE:FEATURE
--------------------------------------------------------------------
0x610400   N     10:00:00:00:c9:24:3d:90 (Emulex)    scsi-fcp
0x6105dc   NL    21:00:00:20:37:28:31:6d (Seagate)   scsi-fcp
0x6105e0   NL    21:00:00:20:37:28:24:7b (Seagate)   scsi-fcp
```

```
0x6105e1    NL     21:00:00:20:37:28:22:ea (Seagate)     scsi-fcp
0x6105e2    NL     21:00:00:20:37:28:2e:65 (Seagate)     scsi-fcp
0x6105e4    NL     21:00:00:20:37:28:26:0d (Seagate)     scsi-fcp
0x630400    N      10:00:00:00:c9:24:3f:75 (Emulex)      scsi-fcp
0x630500    N      50:06:01:60:88:02:90:cb               scsi-fcp
0x6514e2    NL     21:00:00:20:37:a7:ca:b7 (Seagate)     scsi-fcp
0x6514e4    NL     21:00:00:20:37:a7:c7:e0 (Seagate)     scsi-fcp
0x6514e8    NL     21:00:00:20:37:a7:c7:df (Seagate)     scsi-fcp
0x651500    N      10:00:00:e0:69:f0:43:9f (JNI)
Total number of entries = 12
```

Default Settings

Table 3: Default Settings for Advanced Features , on page 19 lists the default settings for the features included in this chapter.

Table 3: Default Settings for Advanced Features

Parameters	Default
CIM server	Disabled
CIM server security protocol	HTTP
D_S_TOV	5,000 milliseconds.
E_D_TOV	2,000 milliseconds.
R_A_TOV	10,000 milliseconds.
Timeout period to invoke fctrace	5 seconds.
Number of frame sent by the fcping feature	5 frames.
Remote capture connection protocol	TCP.
Remote capture connection mode	Passive.
Local capture frame limit s	10 frames.
FC ID allocation mode	Auto mode.
Loop monitoring	Disabled.
D_S_TOV	5,000 msec
E_D_TOV	2,000 msec

Parameters	Default
R_A_TOV	10,000 msec
Interop mode	Disabled