Managing FLOGI, Name Server, FDMI, and RSCN Databases

This chapter describes the fabric login (FLOGI) database, the name server features, the Fabric-Device Management Interface, and Registered State Change Notification (RSCN) information provided in the Cisco MDS 9000 Family. It includes the following sections:

About FLOGI

In a Fibre Channel fabric, each host or disk requires an Fibre Channel ID. Use the **show flogi database** command to verify if a storage device is displayed in the FLOGI table as in the next section. If the required device is displayed in the FLOGI table, the fabric login is successful. Examine the FLOGI database on a switch that is directly connected to the host HBA and connected ports.

FLOGI Scale Optimization

The FLOGI scale optimization feature enables MDS switches to support an increased number of FLOGIs for module and chassis. The FLOGI scale optimization preloads the routing information for devices after a switch or module reload. This can speed up the Accepts to FLOGIs. This feature is supported on all MDS switches, except Cisco MDS 9250i Multiservice Fabric Switch and Cisco MDS 9148S 16G Multilayer Fabric Switch, and is enabled by default, starting from Cisco MDS NX-OS Release 8.1(1). As of Cisco MDS Release 8.2(2), the higher FLOGI scale limits are published only for MDS 9718. For more information see the "Cisco MDS NX-OS Configuration Limits" documentation for the FLOGI limits.

FLOGI Quiesce Timeout

The FLOGI Quiesce Timeout feature causes the FLOGI process to delay notifications to the other Fibre Channel services such as Routing Information and Fibre Channel Name Server when a device logs out from a fabric or when an interface goes down. If the device logs back to the fabric within the FLOGI quiesce timeout value, the FLOGI Accept can be immediately returned without the other Fibre Channel services being notified. This feature must be disabled by setting the timeout value to zero when there are devices in the fabric that can share a pWWN at different times by logging into different switches within the fabric during failover situations.

Restrictions

- Downgrading from Cisco MDS NX-OS Release 8.1(1) to an earlier release is not supported when FLOGI Scale Optimization is enabled. This feature must be disabled before downgrading. For more information on disabling this feature, see the Disabling FLOGI Scale Optimization and Quiesce Timeout section.
- In Cisco MDS NX-OS Releases 8.1 and Release 8.2, the default FLOGI quiesce timeout value is 2000 ms.

  However, starting with Cisco MDS NX-OS Release 8.3(1), the default FLOGI quiesce timeout value was changed from 2000 ms to 0 ms. Any configured FLOGI quiesce timeout value will be maintained on upgrading. If the FLOGI quiesce timeout value is not configured when upgrading to Cisco MDS NX-OS Releases 8.3(1) or later release, the new default value of 0 ms will be used.
- This feature is supported on all MDS switches, except Cisco MDS 9250i Multiservice Fabric Switch and Cisco MDS 9148S 16G Multilayer Fabric Switch.
- Cisco DCNM and SNMP support is not available for this feature.
- This feature is supported only on the Fibre Channel ports on the Cisco MDS 24/10 port SAN Extension Module.

Enabling FLOGI Scale Optimization and Quiesce Timeout

To enable FLOGI scale optimization and quiesce timeout, perform the following steps:

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Enable FLOGI scale optimization:

switch(config)# **flogi scale enable**

Step 3 Set the FLOGI quiesce timeout value to retain device login information:

switch(config)# **flogi quiesce timeout** *milliseconds*

For information on the default FLOGI quiesce timeout value, see the Restrictions section.

Step 4 Exit global configuration mode:

switch(config)# **exit**

Step 5 (Optional) Verify that FLOGI scale optimization is enabled:

switch# **show flogi internal info | i scale**

switch# **show flogi internal info | i quiesce**

Example: Enabling FLOGI Scale Optimization

The following running configuration shows how to enable FLOGI scale optimization and set the quiesce timeout value to 2000 milliseconds:

```
configure terminal
 flogi scale enable
 flogi quiesce timeout 2000
 exit
```

Note For more information on FLOGI scale numbers, see the Cisco MDS NX-OS Configuration Limits document.

The following sample outputs from the **show flogi internal info | i scale** and **show flogi internal info | i quiesce** commands display details about FLOGI scale optimization:

```
switch# show flogi internal info | i scale
  Stats: fs_flogi_scale_enabled: 1
switch# show flogi internal info | i quiesce
  Stats: fs_flogi_quiesce_timerval: 2000
```

Disabling FLOGI Scale Optimization and Quiesce Timeout

To disable FLOGI scale optimization and quiesce timeout, perform the following steps:

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Disable FLOGI scale optimization:

switch(config)# **no flogi scale enable**

Step 3 Set the FLOGI quiesce timeout value to 0:

switch(config)# **flogi quiesce timeout** *0*

The default quiesce timeout value is 2000 milliseconds.

Step 4 Exit global configuration mode:

switch(config)# **exit**

Step 5 (Optional) Verify that FLOGI scale optimization is disabled:

switch# **show flogi internal info | i scale**

switch# **show flogi internal info | i quiesce**

Example: Disabling FLOGI Scale Optimization

The following running configuration shows how to disable FLOGI scale optimization and set the quiesce timeout value to 0 milliseconds:

```
configure terminal
 no flogi scale enable
 flogi quiesce timeout 0
 exit
```

The following sample outputs from the **show flogi internal info | i scale** and **show flogi internal info | i quiesce** commands display details about FLOGI scale optimization:

```
switch# show flogi internal info | i scale
  Stats: fs_flogi_scale_enabled: 0
switch# show flogi internal info | i quiesce
  Stats: fs_flogi_quiesce_timerval: 0
```

Displaying FLOGI Details

To view the FLOGI database details, use the show flogi database command. See Examples Displays Details on the FLOGI Database , on page 4 to Displays the FLOGI Database by FC ID, on page 5.

Displays Details on the FLOGI Database

```
switch# show flogi database
--------------------------------------------------------------------------------
INTERFACE  VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
sup-fc0    2     0xb30100  10:00:00:05:30:00:49:63  20:00:00:05:30:00:49:5e
fc9/13     1     0xb200e2  21:00:00:04:cf:27:25:2c  20:00:00:04:cf:27:25:2c
fc9/13     1     0xb200e1  21:00:00:04:cf:4c:18:61  20:00:00:04:cf:4c:18:61
fc9/13     1     0xb200d1  21:00:00:04:cf:4c:18:64  20:00:00:04:cf:4c:18:64
fc9/13     1     0xb200ce  21:00:00:04:cf:4c:16:fb  20:00:00:04:cf:4c:16:fb
fc9/13     1     0xb200cd  21:00:00:04:cf:4c:18:f7  20:00:00:04:cf:4c:18:f7
Total number of flogi = 6.
```

Displays the FLOGI Database by Interface

```
switch# show flogi database interface fc1/11
INTERFACE   VSAN    FCID        PORT NAME                   NODE NAME
----------  ------  ---------   ------------------------    ---------------------
fc1/11      1       0xa002ef    21:00:00:20:37:18:17:d2     20:00:00:20:37:18:17:d2
fc1/11      1       0xa002e8    21:00:00:20:37:38:a7:c1     20:00:00:20:37:38:a7:c1
fc1/11      1       0xa002e4    21:00:00:20:37:6b:d7:18     20:00:00:20:37:6b:d7:18
fc1/11      1       0xa002e2    21:00:00:20:37:18:d2:45     20:00:00:20:37:18:d2:45
fc1/11      1       0xa002e1    21:00:00:20:37:39:90:6a     20:00:00:20:37:39:90:6a
```

```
fc1/11      1       0xa002e0    21:00:00:20:37:36:0b:4d     20:00:00:20:37:36:0b:4d
fc1/11      1       0xa002dc    21:00:00:20:37:5a:5b:27     20:00:00:20:37:5a:5b:27
fc1/11      1       0xa002da    21:00:00:20:37:18:6f:90     20:00:00:20:37:18:6f:90
fc1/11      1       0xa002d9    21:00:00:20:37:5b:cf:b9     20:00:00:20:37:5b:cf:b9
fc1/11      1       0xa002d6    21:00:00:20:37:46:78:97     0:00:00:20:37:46:78:97
Total number of flogi = 10.
```

Displays the FLOGI Database by VSAN

```
switch# show flogi database vsan 1
--------------------------------------------------------------------------------
INTERFACE  VSAN    FCID            PORT NAME               NODE NAME
--------------------------------------------------------------------------------
fc1/3      1     0xef02ef  22:00:00:20:37:18:17:d2  20:00:00:20:37:18:17:d2
fc1/3      1     0xef02e8  22:00:00:20:37:38:a7:c1  20:00:00:20:37:38:a7:c1
fc1/3      1     0xef02e4  22:00:00:20:37:6b:d7:18  20:00:00:20:37:6b:d7:18
fc1/3      1     0xef02e2  22:00:00:20:37:18:d2:45  20:00:00:20:37:18:d2:45
fc1/3      1     0xef02e1  22:00:00:20:37:39:90:6a  20:00:00:20:37:39:90:6a
fc1/3      1     0xef02e0  22:00:00:20:37:36:0b:4d  20:00:00:20:37:36:0b:4d
fc1/3      1     0xef02dc  22:00:00:20:37:5a:5b:27  20:00:00:20:37:5a:5b:27
fc1/3      1     0xef02da  22:00:00:20:37:18:6f:90  20:00:00:20:37:18:6f:90
fc1/3      1     0xef02d9  22:00:00:20:37:5b:cf:b9  20:00:00:20:37:5b:cf:b9
fc1/3      1     0xef02d6  22:00:00:20:37:46:78:97  20:00:00:20:37:46:78:97
Total number of flogi = 10.
```

Displays the FLOGI Database by FC ID

```
switch# show flogi database fcid 0xef02e2
--------------------------------------------------------------------------------
INTERFACE  VSAN    FCID            PORT NAME               NODE NAME
--------------------------------------------------------------------------------
fc1/3      1     0xef02e2  22:00:00:20:37:18:d2:45  20:00:00:20:37:18:d2:45
Total number of flogi = 1.
```

For more information, see the Default Company ID List and refer to the “Loop Monitoring” section in the *Cisco MDS 9000 Family Troubleshooting Guide*.

Name Server

The name server functionality maintains a database containing the attributes for all hosts and storage devices in each VSAN. Name servers allow a database entry to be modified by a device that originally registered the information.

The proxy feature is useful when you want to modify (update or delete) the contents of a database entry that was previously registered by a different device.

This section includes the following topics:

Bulk Notification Sent from the Name Server

In order to improve the performance of the Fibre Channel protocols on the Cisco MDS 9000 switch, the name server optimizes the remote entry change notifications by sending multiple notifications in one MTS payload.

Nearly 10 other components that receive this MTS notification would have to function on the single bulk notification instead of multiple notifications.

Enabling Name Server Bulk Notification

For NX-OS Release 6.2(1) to 6.2(7), bulk notification is disabled by default. Enabling this feature in one switch has no bearing on the other switches in the same fabric.

Note From NX-OS Release 6.2(9) onwards, bulk notification is enabled by default.

Restrictions

- Whenever the intelligent applications such as the DMM, IOA, and SME are enabled, the bulk notification feature is not supported.
- Any configuration present in the FC-Redirect, conflicts with the bulk notification feature.

Note The above restrictions are applicable only to release 6.2.7.

To enable the name server bulk notification, follow these steps for NX-OS Release 6.2(1) to 6.2(7):

Step 1 switch# **config t**

Enters configuration mode.

Step 2 switch(config)# **fcns bulk-notify**

switch(config)#

Enables the transmission of multiple name server entry change notification in one Messaging and Transaction Services (MTS) payload.

Disabling Name Server Bulk Notification

To disable the name server bulk notification, follow these steps for NX-OS Release 6.2(1) to 6.2(7):

Step 1 switch# **config t**

Enters configuration mode.

Step 2 switch(config)# **no fcns bulk-notify**

switch(config)#

Disables the transmission of multiple name server entry change notification in one Messaging and Transaction Services (MTS) payload.

Disabling Name Server Bulk Notification for NX-OS Release 6.2(9)

To disable the name server bulk notification, follow these steps for NX-OS Release 6.2(9) and later:

Step 1 switch# **config t**

Enters configuration mode.

Step 2 switch(config)# **fcns no-bulk-notify**

switch(config)#

Disables the transmission of multiple name server entry change notification in one Messaging and Transaction Services (MTS) payload.

Re-enabling Name Server Bulk Notification

To re-enable once it is disabled already for NX-OS Release 6.2(9) and later, follow these steps:

Step 1 switch# **config terminal**

Enters configuration mode.

Step 2 switch(config)# **no fcns no-bulk-notify**

switch(config)#

Re-enables the transmission of multiple name server entry change notification in one Messaging and Transaction Services (MTS) payload.

Name Server Proxy Registration

All name server registration requests are sent from the same port with a parameter that is registered or changed. If the port that does not have the parameter, then the request is rejected.

This authorization enables WWNs to register specific parameters for another node.

Registering Name Server Proxies

To register the name server proxy, follow these steps:

Step 1 switch# **config terminal**

switch(config)#

Enters configuration mode.

Step 2 switch(config)# **fcns proxy-port 21:00:00:e0:8b:00:26:d0 vsan 2**

Configures a proxy port for the specified VSAN.

About Rejecting Duplicate pWWN

By FC standard, NX-OS will accept a login on any interface of a pwwn that is already logged in on the same switch, same vsan and same fcdomain. To prevent the same pwwn from logging in the same switch on a different interface, use the port security feature.

By default, any future flogi (with duplicate pwwn) on different switch in the same vsan, will be rejected and previous FLOGI retained, which does not follow FC standards. If you disable this option, any future flogi (with duplicate pwwn) on different switch in the same VSAN, would be allowed to succeed by deleting previous FCNS entry

Rejecting Duplicate pWWNs

To reject duplicate pWWNs, follow these steps:

Step 1 switch# **configure terminal**

switch(config)#

Enters configuration mode.

Step 2 switch(config)# **fcns reject-duplicate-pwwn vsan 1**

Any future flogi (with duplicate pwwn) on different switch, will be rejected and previous FLOGI retained. (default)

Step 3 switch(config)# **no fcns reject-duplicate-pwwn vsan 1**

Any future flogi (with duplicate pwwn) on different switch, will be allowed to succeed by deleting earlier FCNS entry.

But you can still see the earlier entry in FLOGI database in the other switch.

Name Server Database Entries

The name server stores name entries for all hosts in the FCNS database. The name server permits an Nx port to register attributes during a PLOGI (to the name server) to obtain attributes of other hosts. These attributes are deregistered when the Nx port logs out either explicitly or implicitly.

In a multiswitch fabric configuration, the name server instances running on each switch shares information in a distributed database. One instance of the name server process runs on each switch.

Optimizing Name Server Database Sync

If an end device doesn't register FC4 feature with Name Server database, VHBA (also called scsi-target) component would perform PRLI to the end device to discover FC4 feature and register with Name Server on behalf of end device. This discovery from VHBA was performed both for locally connected devices

as well as remotely connected devices. This discovery was unnecessary for remotely connected devices because, Name Server would get FC4 feature of remotely connected devices through regular Name Server sync protocol. So, the default behavior of VHBA component has been modified to discover only locally connected devices. To modify this behavior, follow these steps:

Step 1 switch(config)# scsi-target discovery

Enables a switch to discover fc4-feature for

remote devices also. But this would not be

the default behavior if the users reload or switchover the switch.

Step 2 switch(config)# scsi-target discovery local-only

Switches back to the default behavior.

Verifying the Number of Name Server Database Entries

To Verify the number of name server database entries, follow these steps:

Step 1 switch# show fcns internal info global

Displays the number of device entries in the name server database.

Step 2 switch# show fcns internal info

Displays the number of devices in the name server database at the end of the output.

Displaying Name Server Database Entries

Use the **show fcns** command to display the name server database and statistical information for a specified VSAN or for all VSANs (see Examples Displays the Name Server Database, on page 9 to Displays the Name Server Statistics, on page 11).

Displays the Name Server Database

```
switch# show fcns database
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x010000    N     50:06:0b:00:00:10:a7:80                   scsi-fcp fc-gs
```

```
0x010001    N     10:00:00:05:30:00:24:63 (Cisco)           ipfc
0x010002    N     50:06:04:82:c3:a0:98:52 (Company 1)       scsi-fcp 250
0x010100    N     21:00:00:e0:8b:02:99:36 (Company A)       scsi-fcp
0x020000    N     21:00:00:e0:8b:08:4b:20 (Company A)
0x020100    N     10:00:00:05:30:00:24:23 (Cisco)         ipfc
0x020200    N     21:01:00:e0:8b:22:99:36 (Company A)       scsi-fcp
```

Displays the Name Server Database for the Specified VSAN

```
switch# show fcns database vsan 1
VSAN 1:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x030001    N     10:00:00:05:30:00:25:a3 (Cisco)         ipfc
0x030101    NL    10:00:00:00:77:99:60:2c (Interphase)
0x030200    N     10:00:00:49:c9:28:c7:01
0xec0001    NL    21:00:00:20:37:a6:be:14 (Seagate)       scsi-fcp
Total number of entries = 4
```

Displays the Name Server Database Details

```
switch# show fcns database detail
------------------------
VSAN:1     FCID:0x030001
------------------------
port-wwn (vendor)     :10:00:00:05:30:00:25:a3 (Cisco)
node-wwn              :20:00:00:05:30:00:25:9e
class                 :2,3
node-ip-addr          :0.0.0.0
ipa                   :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:ipfc
symbolic-port-name    :
symbolic-node-name    :
port-type             :N
port-ip-addr          :0.0.0.0
fabric-port-wwn       :00:00:00:00:00:00:00:00
hard-addr             :0x000000
------------------------
VSAN:1     FCID:0xec0200
------------------------
port-wwn (vendor)     :10:00:00:5a:c9:28:c7:01
node-wwn              :10:00:00:5a:c9:28:c7:01
class                 :3
node-ip-addr          :0.0.0.0
ipa                   :ff ff ff ff ff ff ff ff
fc4-types:fc4_features:
symbolic-port-name    :
symbolic-node-name    :
port-type             :N
port-ip-addr          :0.0.0.0
fabric-port-wwn       :22:0a:00:05:30:00:26:1e
hard-addr             :0x000000
Total number of entries = 2
```

Displays the Name Server Statistics

```
switch# show fcns statistics

registration requests received = 27
deregistration requests received = 0
queries received = 57
queries sent = 10
reject responses sent = 14
RSCNs received = 0
RSCNs sent = 0
```

FDMI

Cisco MDS 9000 Family switches provide support for the Fabric-Device Management Interface (FDMI) functionality, as described in the FC-GS-4 standard. FDMI enables management of devices such as Fibre Channel host bus adapters (HBAs) through in-band communications. This addition complements the existing Fibre Channel name server and management server functions.

Using the FDMI functionality, the Cisco NX-OS software can extract the following management information about attached HBAs and host operating systems without installing proprietary host agents:

- Manufacturer, model, and serial number
- Node name and node symbolic name
- Hardware, driver, and firmware versions
- Host operating system (OS) name and version number

All FDMI entries are stored in persistent storage and are retrieved when the FDMI process is started.

Displaying FDMI

Use the **show fdmi** command to display the FDMI database information (see Examples Displays All HBA Management Servers, on page 11 to Displays Details for the Specified HBA Entry, on page 13).

Displays All HBA Management Servers

```
switch# show fdmi database
Registered HBA List for VSAN 1
  10:00:00:00:c9:32:8d:77
  21:01:00:e0:8b:2a:f6:54
switch# show fdmi database detail
Registered HBA List for VSAN 1
-------------------------------
HBA-ID: 10:00:00:00:c9:32:8d:77
-------------------------------
Node Name        :20:00:00:00:c9:32:8d:77
Manufacturer     :Emulex Corporation
Serial Num       :0000c9328d77
Model            :LP9002
Model Description:Emulex LightPulse LP9002 2 Gigabit PCI Fibre Channel Adapter
Hardware Ver     :2002606D
```

```
Driver Ver       :SLI-2 SW_DATE:Feb 27 2003, v5-2.20a12
ROM Ver          :3.11A0
Firmware Ver     :3.90A7
OS Name/Ver      :Window 2000
CT Payload Len   :1300000
  Port-id: 10:00:00:00:c9:32:8d:77
-------------------------------
HBA-ID: 21:01:00:e0:8b:2a:f6:54
-------------------------------
Node Name        :20:01:00:e0:8b:2a:f6:54
Manufacturer     :QLogic Corporation
Serial Num       :\74262
Model            :QLA2342
Model Description:QLogic QLA2342 PCI Fibre Channel Adapter
Hardware Ver     :FC5010409-10
Driver Ver       :8.2.3.10 Beta 2 Test 1 DBG (W2K VI)
ROM Ver          :1.24
Firmware Ver     :03.02.13.
OS Name/Ver      :500
CT Payload Len   :2040
  Port-id: 21:01:00:e0:8b:2a:f6:54
```

Displays HBA Details for a Specified VSAN

```
switch# show fdmi database detail vsan 1
Registered HBA List for VSAN 1
-------------------------------
HBA-ID: 10:00:00:00:c9:32:8d:77
-------------------------------
Node Name        :20:00:00:00:c9:32:8d:77
Manufacturer     :Emulex Corporation
Serial Num       :0000c9328d77
Model            :LP9002
Model Description:Emulex LightPulse LP9002 2 Gigabit PCI Fibre Channel Adapter
Hardware Ver     :2002606D
Driver Ver       :SLI-2 SW_DATE:Feb 27 2003, v5-2.20a12
ROM Ver          :3.11A0
Firmware Ver     :3.90A7
OS Name/Ver      :Window 2000
CT Payload Len   :1300000
  Port-id: 10:00:00:00:c9:32:8d:77
-------------------------------
HBA-ID: 21:01:00:e0:8b:2a:f6:54
-------------------------------
Node Name        :20:01:00:e0:8b:2a:f6:54
Manufacturer     :QLogic Corporation
Serial Num       :\74262
Model            :QLA2342
Model Description:QLogic QLA2342 PCI Fibre Channel Adapter
Hardware Ver     :FC5010409-10
Driver Ver       :8.2.3.10 Beta 2 Test 1 DBG (W2K VI)
ROM Ver          :1.24
Firmware Ver     :03.02.13.
OS Name/Ver      :500
CT Payload Len   :2040
  Port-id: 21:01:00:e0:8b:2a:f6:54
```

Displays Details for the Specified HBA Entry

```
switch# show fdmi database detail hba-id 21:01:00:e0:8b:2a:f6:54 vsan 1
Node Name        :20:01:00:e0:8b:2a:f6:54
Manufacturer     :QLogic Corporation
Serial Num       :\74262
Model            :QLA2342
Model Description:QLogic QLA2342 PCI Fibre Channel Adapter
Hardware Ver     :FC5010409-10
Driver Ver       :8.2.3.10 Beta 2 Test 1 DBG (W2K VI)
ROM Ver          :1.24
Firmware Ver     :03.02.13.
OS Name/Ver      :500
CT Payload Len   :2040
  Port-id: 21:01:00:e0:8b:2a:f6:54
```

VMID

Note The VMID feature is currently in preview (beta) status for use in non-production environment only. This preview (beta) status and restriction will change to regular production status in an upcoming release.

The switch-based Virtual Machine Identifier (VMID) feature allows identification of traffic sources at an individual virtual machine (VM) level by the SAN fabric infrastructure.

VMID on the MDS switch provides a range of identifiers to a host hypervisor. These identifiers can then be assigned to local VMs by the hypervisor. Supplemental information about the VM assigned to an identifier is reported back to the switch. The identifiers are then inserted into the CS_CTL field of traffic from the VMs by the hypervisor, allowing identification of the traffic source by the SAN fabric.

The VMID feature uses the following IDs:

- Virtual Entity (VE): Refers to any virtual device.
- Virtual Entities Manager (VEM): Refers to a hypervisor.
- Virtual Entity Identifier (VE ID): Refers to the different types of identifiers assigned to VEs. There are four types of VE IDs:
  - Local VE ID: Local VE ID is used to uniquely identify a VE within a VEM N_Port. Local VE IDs change when virtual machines come up, go down, or go through migration between VEMs.
  - Fabric VE ID: Fabric VE ID is used to uniquely identify a VE within a fabric. It is a combination of the VEM N_Port FCID and the Local VE ID.
  - Global VE ID: Global VE ID is used to uniquely identify a VE and is a 16-byte Universally Unique Identifier (UUID). The Global VE ID is assigned by a service outside the SAN fabric such as a VM management platform. Once a global VE ID is assigned, it does not expire.
  - VEM ID: VEM ID is used to uniquely identify a VEM and is a 16-byte UUID. The VEM ID is assigned by a service outside the SAN fabric such as a VM management platform.
- Fabric ports on a VEM comprise of the following N_Ports:

- Physical Network Port (PN_Port): A physical network port of a hypervisor host bus adapter (HBA).
- Virtual Network Port (VN_Port): An optional virtual network port that can be shared by a set of VEs. A PN_Port can have multiple VN_Ports. Each VN_Port is allocated a unique FCID.

- Physical Fabric Port (PF_Port): A physical fabric port of a switch.

When an HBA Port Comes Up

After an HBA driver has logged a physical or virtual HBA port into the fabric, the driver may request Local VE IDs from the fabric through the port. The Virtual Machine Identification Server (VMIS) on the locally attached switch provides the range of Local VE IDs (up to 255) in the response. The driver then assigns the identifiers to the port FCID.

When a VM Initially Accesses a Disk

Outside of a fabric, a VM is identified by a Global VE ID. Within a fabric, a VM is identified by a Fabric VE ID. When a VM initially accesses a virtual disk, the hypervisor starts accessing the corresponding physical disk through an HBA port. For each path to the physical disk an unused Local VE ID from the pool for the FCID is assigned. The FCID and Local VE ID are combined to create a unique Fabric VE ID by the HBA driver. The HBA driver then notifies the locally attached VMIS about the assigned VE ID to Global VE ID mapping. This mapping is done for each VM path to the fabric through the hypervisor and allows all VM traffic to be identified by SAN tools by path, such as Cisco MDS SAN Analytics.

When a VM Goes Down or Moves Within a Fabric

The difference between a Global VE ID and Local VE ID is seen when a VM migrates between VEMs. When a VM is deinstantiated or migrated between VEMs, the Local VE ID is returned to the pool by the HBA driver, but does not notify the switch VMIS. The switch will time out the Local VE ID or VM mapping after 1 to 4 hours of no traffic. If a VM reinstantiates on the same VEM, it may get a different Local VE ID from the pool of the same FCID because the previously assigned Local VE ID may have been allocated to another VM when this VM was down. When a VM migrates to a different VEM, the VM will likely utilize a different FCID and likely be assigned a different Local VE ID from the FCID's pool. Thus, when a VM reboots or migrates between VEMs, the Global VE ID remains constant but Local VE ID may change.

Figure 1: VMID Components, on page 15 show the components of VMID:

Figure 1: VMID Components

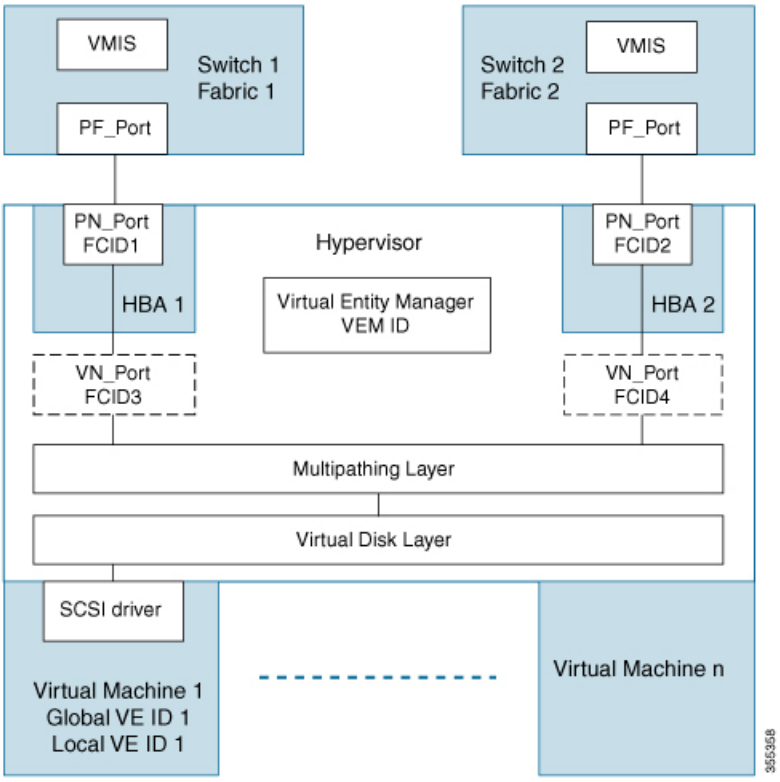
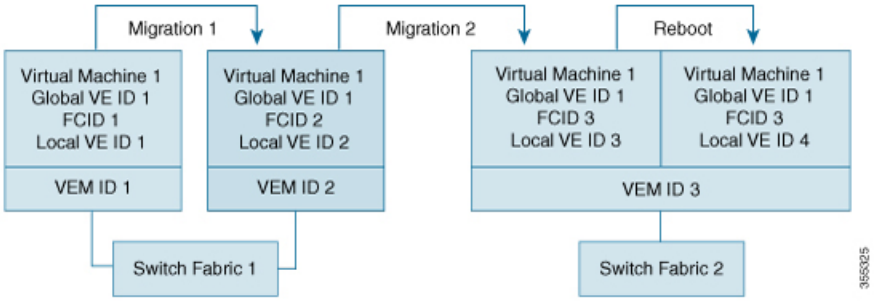


Figure 2: VE ID Life Cycle, on page 15 shows how VE ID changes during a VM life cycle:

Figure 2: VE ID Life Cycle



Guidelines and Limitations for VMID

- The VMID feature is not supported on Cisco N-Port Virtualizer (Cisco NPV) switches.
- There is no mechanism in the VMID protocol for the VMIS to notify the attached hypervisor HBA driver clients of a new VE ID range. For clients to detect a new range, they must query the VMIS again. To force the clients to query again after a range modification, the user must manually log the FCIDs out and back into the fabric. Consequently, local clients will continue to tag the VM traffic with the previous

range until this occurs. This restriction applies when enabling and disabling VMID, and changing the VE ID range of a VSAN.

- The Extended Receiver Ready (ER_RDY) feature uses CSCTL 1 to 15. The VMID feature uses CSCTL 16 to 255. If the VMID database has any interfaces that are configured in the VMIS range 1 to 15 and if you are upgrading to Cisco MDS NX-OS Release 9.2(1) or later releases, then you will prompted to change the range between 16 to 255 and flap the interfaces before upgrading.
- The VMID feature is not supported in any VSAN which has interoperability enabled. For more information about interoperability modes, see the Cisco MDS 9000 Series Switch-to-Switch Interoperability Configuration Guide.

Configuring the VMID Server

Enabling the VMID Server

To enable the VMID Server feature, perform these steps:

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Enable the VMID Server feature:

switch(config)# **feature vmis**

Disabling the VMID Server

To disable the VMID Server feature, perform these steps:

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Disable the VMID Server feature:

switch(config)# **no feature vmis**

Configuring a VMID Range

The VMID range is used to limit the Local VE IDs an HBA driver will use. By restricting the Local VE ID range to use a subset of bits in the CS_CTL field it can be partitioned and shared with future Fibre Channel features.

To configure a VMID range, perform these steps:

Step 1 Enter global configuration mode:

switch# **configure terminal**

Step 2 Configure VE ID range for use within a VSAN:

switch(config)# **vmis range** *range* **vsan** *id*

Examples: Configuring the VMID Server

This example shows how to enable the VMID Server feature:

```
switch# configure terminal
switch(config)# feature vmis
```

This example shows how to disable the VMID Server feature:

```
switch# configure terminal
switch(config)# no feature vmis
```

This example shows how to configure multiple Local VE ID ranges for use by hypervisor HBA drivers in a VSAN:

```
switch# configure terminal
switch(config)# vmis range 3-45,51-70 vsan 1
```

Verifying a VMID Configuration

This example shows the FCIDs that are capable of using the VMID Server feature. The letter *M* under the **FLAGS** field indicates that the corresponding FCID is capable of using the VMID Server feature.

```
switch# show flogi database details
--------------------------------------------------------------------------------------------
INTERFACE        VSAN    FCID           PORT NAME               NODE NAME            FLAGS

--------------------------------------------------------------------------------------------
fc1/7            1     0xef0000  20:07:8c:60:4f:10:0f:e0 20:01:8c:60:4f:10:0f:e1     P
fc1/7            1     0xef0001  20:19:8c:60:4f:19:bf:25 21:00:00:20:38:de:c3:9f     VPM

Total number of flogi = 2.
```

This example shows all the entries in a VMIS database. This is the database of all IDs in the SAN fabric. Locally connected IDs show the connecting interface; remotely connected IDs show the interface name as "--" in the output.

```
switch# show vmis database
Total 17 entries
-------------------------------------------------------------------------------------
INTERFACE         VSAN  FCID      LOCAL VEID           GLOBAL VEID
-------------------------------------------------------------------------------------
fc1/7             1     0xef000a  0x01        9a07686b-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x02        66fb6a4e-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x03        325de425-0405-0607-0809-0a0b0c0d0e0f
```

```
fc1/7             1     0xef000a  0x04        0d509b51-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x05        b7d71b43-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x32        1b231602-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x01        e8e9161f-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x02        e7cd9011-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x03        8d43ef66-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x04        760f0e14-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x05        5a255233-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x1e        1b231602-0405-0607-0809-0a0b0c0d0e0f
--                10    0x4c0020  0x1e        ba581b3d-0405-0607-0809-0a0b0c0d0e0f
--                10    0x4c0020  0x1f        abd77e50-0405-0607-0809-0a0b0c0d0e0f
--                10    0x4c0020  0x20        f241b12e-0405-0607-0809-0a0b0c0d0e0f
--                10    0x4c0020  0x21        fb1eb741-0405-0607-0809-0a0b0c0d0e0f
--                10    0x4c0020  0x22        e3a9e279-0405-0607-0809-0a0b0c0d0e0f
```

This example shows a VMIS database entries of a specified local VSAN domain:

```
switch# show vmis database local vsan 1
Total 12 entries
--------------------------------------------------------------------------------
INTERFACE         VSAN  FCID      LOCAL VEID           GLOBAL VEID
--------------------------------------------------------------------------------
fc1/7             1     0xef000a  0x01        9a07686b-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x02        66fb6a4e-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x03        325de425-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x04        0d509b51-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x05        b7d71b43-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x32        1b231602-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x01        e8e9161f-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x02        e7cd9011-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x03        8d43ef66-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x04        760f0e14-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x05        5a255233-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x1e        1b231602-0405-0607-0809-0a0b0c0d0e0f
```

This example shows the entries in a VSAN filtered by the hosting domain:

```
switch# show vmis database domain 0xef vsan 1
Total 12 entries
--------------------------------------------------------------------------------
INTERFACE         VSAN  FCID      LOCAL VEID           GLOBAL VEID
--------------------------------------------------------------------------------
fc1/7             1     0xef000a  0x01        9a07686b-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x02        66fb6a4e-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x03        325de425-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x04        0d509b51-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x05        b7d71b43-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x32        1b231602-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x01        e8e9161f-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x02        e7cd9011-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x03        8d43ef66-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x04        760f0e14-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x05        5a255233-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x1e        1b231602-0405-0607-0809-0a0b0c0d0e0f
```

This example shows the entries in a VSAN filtered by an interface:

```
switch# show vmis database interface fc1/7 vsan 1
Total 12 entries
--------------------------------------------------------------------------------
```

```
INTERFACE         VSAN  FCID      LOCAL VEID           GLOBAL VEID
--------------------------------------------------------------------------------
fc1/7             1     0xef000a  0x01        9a07686b-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x02        66fb6a4e-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x03        325de425-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x04        0d509b51-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x05        b7d71b43-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x32        1b231602-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x01        e8e9161f-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x02        e7cd9011-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x03        8d43ef66-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x04        760f0e14-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x05        5a255233-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000b  0x1e        1b231602-0405-0607-0809-0a0b0c0d0e0f
```

This example shows the entries in a VSAN:

```
switch# show vmis database vsan 10
Total 5 entries
--------------------------------------------------------------------------------
INTERFACE         VSAN  FCID      LOCAL VEID           GLOBAL VEID
--------------------------------------------------------------------------------
--                10    0x4c0020  0x1e        ba581b3d-0405-0607-0809-0a0b0c0d0e0f
--                10    0x4c0020  0x1f        abd77e50-0405-0607-0809-0a0b0c0d0e0f
--                10    0x4c0020  0x20        f241b12e-0405-0607-0809-0a0b0c0d0e0f
--                10    0x4c0020  0x21        fb1eb741-0405-0607-0809-0a0b0c0d0e0f
--                10    0x4c0020  0x22        e3a9e279-0405-0607-0809-0a0b0c0d0e0f
```

This example shows the entries filtered by FCIDs. This example is filtered by a remote hypervisor N_Port FCID.

```
switch# show vmis database fcid 0x4c0020 vsan 10
Total 5 entries
--------------------------------------------------------------------------------
INTERFACE         VSAN  FCID      LOCAL VEID           GLOBAL VEID
--------------------------------------------------------------------------------
--                10    0x4c0020  0x1e        ba581b3d-0405-0607-0809-0a0b0c0d0e0f
--                10    0x4c0020  0x1f        abd77e50-0405-0607-0809-0a0b0c0d0e0f
--                10    0x4c0020  0x20        f241b12e-0405-0607-0809-0a0b0c0d0e0f
--                10    0x4c0020  0x21        fb1eb741-0405-0607-0809-0a0b0c0d0e0f
--                10    0x4c0020  0x22        e3a9e279-0405-0607-0809-0a0b0c0d0e0f
```

This example shows the VMIS entries filtered by Global VM ID and VSAN:

```
switch# show vmis database global-vmid e8e9161f-0405-0607-0809-0a0b0c0d0e0f vsan 1
Total 1 entries
--------------------------------------------------------------------------------
INTERFACE         VSAN  FCID      LOCAL VEID           GLOBAL VEID
--------------------------------------------------------------------------------
fc1/7             1     0xef000b  0x01        e8e9161f-0405-0607-0809-0a0b0c0d0e0f
```

This example shows the VEM IDs registered in a VSAN:

```
switch# show vmis database vem vsan 1
Total 2 entries
-----------------------------------------------------------------------------
INTERFACE         VSAN  FCID               VEM ID
-----------------------------------------------------------------------------
```

```
fc1/7             1     0xef000a  11223344-5566-7788-99aa-bbccddeeffaa
fc1/7             1     0xef000b  00010203-0405-0607-0809-0a0b0cef000b
```

This example shows VM entries that have migrated between VEMs:

The output shows two entries correspond to a VM before and after a VM has migrated between VEMs. The IDs associated with the VM before migration are not deleted immediately. These IDs will be deleted in the VMIS database after the switch IO timer expires. Until the IO timer expires, you will see two entries of the same VM in the VMIS database.

```
switch# show vmis database vmotion vsan 1
Total 2 entries
--------------------------------------------------------------------------------
INTERFACE         VSAN  FCID      LOCAL VEID           GLOBAL VEID
--------------------------------------------------------------------------------
fc1/7             1     0xef000b  0x1e        1b231602-0405-0607-0809-0a0b0c0d0e0f
fc1/7             1     0xef000a  0x32        1b231602-0405-0607-0809-0a0b0c0d0e0f
```

This example shows a Local VE ID range that is configured for each VSAN:

```
switch# show vmis range
VSAN      VEID Range
--------------------
   1      1-255
  10      1-255
  20      1-255
  30      1-255
```

This example shows statistics of a local switch's VMIS exchanges with locally attached hypervisor HBA driver clients (host side) and with other VMIS agents on other switches in the fabric (switch side) by VSAN:

```
switch# show vmis statistics
VSAN : 1
-----Host Side-----
qfpa/qfpa_rsp/qfpa_rjt : 1/1/0
uvem/uvem_rsp/uvem_rjt : 1/1/0
ggvid/ggvid_rsp/ggvid_rjt : 0/0/0
gfvid/gfvid_rsp/gfvid_rjt : 0/0/0
gvemid/gvemid_rsp/gvemid_rjt : 0/0/0
gvem/gvem_rsp/gvem_rjt : 0/0/0

-----Switch Side-----
gvemd_tx/gvemd_rsp_tx/gvemd_rjt_tx : 0/0/0
gvemd_rx/gvemd_rsp_rx/gvemd_rjt_rx : 0/0/0
uvemd_tx/uvemd_rsp_tx/uvemd_rjt_tx : 0/0/0
uvemd_rx/uvemd_rsp_rx/uvemd_rjt_rx : 0/0/0
```

RSCN

The Registered State Change Notification (RSCN) is a Fibre Channel service that informs hosts about changes in the fabric. Hosts can receive this information by registering with the fabric controller (through SCR). These notifications provide a timely indication of one or more of the following events:

- Disks joining or leaving the fabric.

- A name server registration change.
- A new zone enforcement.
- IP address change.
- Any other similar event that affects the operation of the host.

This section includes the following topics:

About RSCN Information

Apart from sending these events to registered hosts, a switch RSCN (SW-RSCN) is sent to all reachable switches in the fabric.

Note The switch sends an RSCN to notify registered nodes that a change has occurred. It is up to the nodes to query the name server again to obtain the new information. The details of the changed information are not delivered by the switch in the RSCN sent to the nodes.

Displaying RSCN Information

Use the **show rscn** command to display RSCN information (see Examples Displays Register Device Information, on page 21 and Displays RSCN Counter Information, on page 21).

Displays Register Device Information

```
switch# show rscn scr-table vsan 1
SCR table for VSAN: 1
---------------------------------------------
FC-ID         REGISTERED FOR
---------------------------------------------
0x1b0300      fabric detected rscns
Total number of entries = 1
```

Note The SCR table is not configurable. It is populated when hosts send SCR frames with RSCN information. If hosts do not receive RSCN information, then the **show rscn scr-table** command will not return entries.

Displays RSCN Counter Information

```
switch(config)# show rscn statistics vsan 106
Statistics for VSAN: 106
-------------------------
Number of SCR received         = 0
Number of SCR ACC sent         = 0
Number of SCR RJT sent         = 0
Number of RSCN received        = 0
Number of RSCN sent            = 0
Number of RSCN ACC received    = 0
```

```
Number of RSCN ACC sent        = 0
Number of RSCN RJT received    = 0
Number of RSCN RJT sent        = 0
Number of SW-RSCN received     = 0
Number of SW-RSCN sent         = 0
Number of SW-RSCN ACC received = 0
Number of SW-RSCN ACC sent     = 0
Number of SW-RSCN RJT received = 0
Number of SW-RSCN RJT sent     = 0
Number of CSWR received        = 3137
Number of CSWR sent            = 0
Number of CSWR ACC received    = 0
Number of CSWR ACC sent        = 3137
Number of CSWR RJT received    = 0
Number of CSWR RJT sent        = 0
Number of CSWR RJT not sent    = 0
```

multi-pid Option

If the RSCN **multi-pid** option is enabled, then RSCNs generated to the registered Nx ports may contain more than one affected port IDs. In this case, zoning rules are applied before putting the multiple affected port IDs together in a single RSCN. By enabling this option, you can reduce the number of RSCNs. For example: Suppose you have two disks (D1, D2) and a host (H) connected to switch 1. Host H is registered to receive RSCNs. D1, D2 and H belong to the same zone. If disks D1 and D2 are online at the same time, then one of the following applies:

- The **multi-pid** option is disabled on switch 1: two RSCNs are generated to host H—one for the disk D1 and another for disk D2.
- The **multi-pid** option is enabled on switch 1: a single RSCN is generated to host H, and the RSCN payload lists the affected port IDs (in this case, both D1 and D2).

Note Some Nx ports may not understand multi-pid RSCN payloads. If not, disable the RSCN **multi-pid** option.

Configuring the multi-pid Option

To configure the **multi-pid** option, follow these steps:

Step 1 switch# **config terminal**

switch(config)#

Enters configuration mode.

Step 2 switch(config)# **rscn multi-pid vsan 105**

Sends RSCNs in a multi-pid format for VSAN 105.

Suppressing Domain Format SW-RSCNs

A domain format SW-RSCN is sent whenever the local switch name or the local switch management IP address changes. This SW-RSCN is sent to all other domains and switches over the ISLs. The remote switches can issue GMAL and GIELN commands to the switch that initiated the domain format SW-RSCN to determine what changed. Domain format SW-RSCNs can cause problems with some non-Cisco MDS switches (refer to the).

To suppress the transmission of these SW RSCNs over an ISL, follow these steps:

Step 1 switch# **config terminal**

switch(config)#

Enters configuration mode.

Step 2 switch(config)# **rscn suppress domain-swrscn vsan 105**

Suppresses transmission of domain format SW-RSCNs for VSAN 105.

Note You cannot suppress transmission of port address or area address format RSCNs.

Coalesced SW-RSCN

In order to improve the performance of the Fibre Channel protocols on the Cisco MDS 9000 switch, SW-RSCNs are delayed, collected and sent as a single coalesced SW-RSCN to all the switches in the fabric in a single Fibre Channel exchange.

Enabling Coalesced SW-RSCNs

Restrictions

- All the switches in the fabric should be running Cisco MDS 6.2(7) and above.
- This feature does not have interoperability with non-Cisco MDS switches.

To enable the coalesced SW-RSCNs, follow these step:

Step 1 switch# **config terminal**

Enters configuration mode.

Step 2 switch(config)# rscn coalesce swrscn vsan 1

switch(config)#

Enables coalescing of Switch Registered State Change Notification (SWRSCN) in VSAN 1. The default delay is 500 milliseconds.

Step 3 switch(config)# rscn coalesce swrscn vsan 1 delay 800

switch(config)#

Enables coalescing of Switch Registered State Change Notification (SWRSCN) in VSAN 1. Delays the SW-RSCNs maximum by 800 milliseconds.

Note All the switches running 6.2(7) and above are capable of processing coalesced SW-RSCN by default, but they are capable of sending coalesced SW-RSCN only after enabling through CLI.

Disabling Coalesced SW-RSCNs

To disable the coalesced SW-RSCNs, follow these steps:

Step 1 switch# **config terminal**

Enters configuration mode.

Step 2 switch(config)# no rscn coalesce swrscn vsan 1

switch(config)#

Disables coalescing of Switch Registered State Change Notification (SWRSCN) in VSAN 1.

Clearing RSCN Statistics

You can clear the counters and later view the counters for a different set of events. For example, you can keep track of how many RSCNs or SW-RSCNs are generated on a particular event (such as ONLINE or OFFLINE events). You can use these statistics to monitor responses for each event in the VSAN.

Use the **clear rscn statistics** command to clear the RSCN statistics for the specified VSAN.

```
switch# clear rscn statistics vsan 1
```

After clearing the RSCN statistics, you can view the cleared counters by issuing the **show rscn** command.

```
switch# show rscn statistics vsan 1
Statistics for VSAN: 1
------------------------
Number of SCR received         = 0
Number of SCR ACC sent         = 0
Number of SCR RJT sent         = 0
Number of RSCN received        = 0
Number of RSCN sent            = 0
Number of RSCN ACC received    = 0
Number of RSCN ACC sent        = 0
Number of RSCN RJT received    = 0
Number of RSCN RJT sent        = 0
Number of SW-RSCN received     = 0
Number of SW-RSCN sent         = 0
Number of SW-RSCN ACC received = 0
Number of SW-RSCN ACC sent     = 0
Number of SW-RSCN RJT received = 0
Number of SW-RSCN RJT sent     = 0
Number of CSWR received        = 0
Number of CSWR sent            = 0
```

```
Number of CSWR ACC received    = 0
Number of CSWR ACC sent        = 0
Number of CSWR RJT received    = 0
Number of CSWR RJT sent        = 0
Number of CSWR RJT not sent    = 0
```

RSCN Timer Configuration Distribution Using CFS

Because the timeout value for each switch is configured manually, a misconfiguration occurs when different switches time out at different times. This means different N ports in a network can receive RSCNs at different times. Cisco Fabric Services (CFS) alleviates this situation by automatically distributing configuration information to all switches in a fabric. This also reduces the number of SW-RSCNs.

RSCN supports two modes, distributed and nondistributed. In distributed mode, RSCN uses CFS to distribute configuration to all switches in the fabric. In nondistributed mode, only the configuration commands on the local switch are affected.

Note All configuration commands are not distributed. Only the **rscn event-tov tov vsan vsan** command is distributed.

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

Note Before performing a downgrade, make sure that you revert the RCSN timer value in your network to the default value. Failure to do so will disable the links across your VSANs and other devices.

Compatibility across various Cisco MDS NX-OS releases during an upgrade or downgrade is supported by **conf-check** provided by CFS. If you attempt to downgrade from Cisco MDS SAN-OS Release 3.0, you are prompted with a **conf-check** warning. You are required to disable RSCN timer distribution support before you downgrade.

By default, the RSCN timer distribution capability is disabled and is therefore compatible when upgrading from any Cisco MDS SAN-OS release earlier than Release 3.0.

Configuring the RSCN Timer

RSCN maintains a per-VSAN event list queue, where the RSCN events are queued as they are generated. When the first RSCN event is queued, a per VSAN timer starts. Upon time-out, all the events are dequeued and coalesced RSCNs are sent to registered users. The default timer values minimize the number of coalesced RSCNs sent to registered users. Some deployments require smaller event timer values to track changes in the fabric.

Note The RSCN timer value must be the same on all switches in the VSAN. See the RSCN Timer Configuration Distribution, on page 26.

Note Before performing a downgrade, make sure that you revert the RCSN timer value in your network to the default value. Failure to do so will disable the links across your VSANs and other devices.

To configure the RSCN timer, follow these steps:

Step 1 switch# **config t**

switch(config)#

Enters configuration mode.

Step 2 switch(config)# **rscn distribute**

Enables RSCN timer configuration distribution.

Step 3 switch(config)# **rscn event-tov 300 vsan 10**

Sets the event time-out value in milliseconds for the selected VSAN. In this example, the event time-out value is set to 300 milliseconds for VSAN 12. The range is 0 to 2000 milliseconds. Setting a zero (0) value disables the timer.

Step 4 switch(config)# **no rscn event-tov 300 vsan 10**

Reverts to the default value (2000 milliseconds for Fibre Channel VSANs or 1000 milliseconds for FICON VSANs).

Step 5 switch(config)# **rscn commit vsan 10**

Commits the RSCN timer configuration to be distributed to the switches in VSAN 10.

Verifying the RSCN Timer Configuration

You verify the RSCN timer configuration using the **show rscn event-tov vsan** command.

```
switch# show rscn event-tov vsan 10
Event TOV : 1000 ms
```

RSCN Timer Configuration Distribution

Because the timeout value for each switch is configured manually, a misconfiguration occurs when different switches time out at different times. This means different N-ports in a network can receive RSCNs at different times. Cisco Fabric Services (CFS) infrastructure alleviates this situation by automatically distributing the RSCN timer configuration information to all switches in a fabric. This also reduces the number of SW-RSCNs. Refer to the *Cisco MDS 9000 Family NX-OS System Management Configuration Guide* .

RSCN supports two modes, distributed and nondistributed. In distributed mode, RSCN uses CFS to distribute configuration to all switches in the fabric. In nondistributed mode, only the configuration commands on the local switch are affected.

Note All configuration commands are not distributed. Only the **rscn event-tov tov vsan vsan** command is distributed.

Note Only the RSCN timer configuration is distributed.

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

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

Note By default, the RSCN timer distribution capability is disabled and is compatible when upgrading from any Cisco MDS SAN-OS release earlier than 3.0.

Note For CFS distribution to operate correctly for the RSCN timer configuration, all switches in the fabric must be running Cisco SAN-OS Release 3.0(1) or later, or Cisco NX-OS 4.1(1b).

This section includes the following topics:

Enabling RSCN Timer Configuration Distribution

To enable RSCN timer configuration distribution, follow these steps:

Step 1 switch# **config terminal**

switch(config)#

Enters configuration mode.

Step 2 switch(config)# **rscn distribute**

Enables RSCN timer distribution.

Step 3 switch(config)# **no rscn distribute**

Disables (default) RSCN timer distribution.

Locking the Fabric

The first action that modifies the database creates the pending database and locks the feature in the VSAN. Once you lock the fabric, the following situations apply:

- No other user can make any configuration changes to this feature.
- A copy of the configuration database becomes the pending database along with the first active change.

Committing the RSCN Timer Configuration Changes

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

To commit RSCN timer configuration changes, follow these steps:

Step 1 switch# **config t**

switch(config)#

Enters configuration mode.

Step 2 switch(config)# **rscn commit vsan 10**

Commits the RSCN timer changes.

Discarding the RSCN Timer Configuration Changes

If you discard (terminate) the changes made to the pending database, the configuration database remains unaffected and the lock is released.

To discard RSCN timer configuration changes, follow these steps:

Step 1 switch# **config t**

switch(config)#

Enters configuration mode.

Step 2 switch(config)# **rscn abort vsan 10**

Discards the RSCN timer changes and clears the pending configuration database.

Clearing a Locked Session

If you have changed the RSCN timer configuration 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 pending database is 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 DPVM session, use the **clear rscn session vsan** command in EXEC mode.

```
switch# clear rscn session vsan 10
```

Displaying RSCN Configuration Distribution Information

Use the **show cfs application name rscn** command to display the registration status for RSCN configuration distribution.

```
switch# show cfs application name rscn
 Enabled        : Yes
 Timeout        : 5s
 Merge Capable  : Yes
 Scope          : Logical
```

Use the **show rscn session status vsan** command to display session status information for RSCN configuration distribution.

Note A merge failure results when the RSCN timer values are different on the merging fabrics.

```
switch# show rscn session status vsan 1
Session Parameters for VSAN: 1
------------------------------
Last Action                : Commit
Last Action Result         : Success
Last Action Failure Reason : None
```

Use the **show rscn pending** command to display the set of configuration commands that would take effect when you commit the configuration.

Note The pending database includes both existing and modified configuration.

```
switch# show rscn pending
rscn event-tov 2000 ms vsan 1
rscn event-tov 2000 ms vsan 2
rscn event-tov 300 ms vsan 10
```

Use the **show rscn pending-diff** command to display the difference between pending and active configurations. The following example shows the time-out value for VSAN 10 was changed from 2000 milliseconds (default) to 300 milliseconds.

```
switch# show rscn pending-diff
- rscn event-tov 2000 ms vsan 10
+ rscn event-tov 300 ms vsan 10
```

Default Settings

Table 1: Default RSCN Settings , on page 30 lists the default settings for RSCN.

Table 1: Default RSCN Settings

Parameters	Default
RSCN timer value	2000 milliseconds for Fibre Channel VSANs1000 milliseconds for FICON VSANs
RSCN timer configuration distribution	Disabled

Enabling Port Pacing

For detailed information, refer to the *Cisco MDS 9000 Family NX-OS System Management* .