



CHAPTER 40

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 (FDMI), and Registered State Change Notification (RSCN) information provided in Cisco Nexus 5000 Series switches. It includes the following sections:

- [Information About Fabric Login, page 40-1](#)
- [Name Server Proxy, page 40-2](#)
- [FDMI, page 40-4](#)
- [Displaying FDMI, page 40-4](#)
- [RSCN, page 40-4](#)
- [Default Settings, page 40-10](#)

Information About Fabric Login

In a Fibre Channel fabric, each host or disk requires an FC ID. Use the **show flogi** command to verify if a storage device is displayed in the fabric login (FLOGI) table as in the following examples. 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.

The following example shows how to verify the storage devices in the fabric login (FLOGI) table:

```
switch# show flogi database
```

INTERFACE	VSAN	FCID	PORT NAME	NODE NAME
fc2/3	1	0xb200e2	21:00:00:04:cf:27:25:2c	20:00:00:04:cf:27:25:2c
fc2/3	1	0xb200e1	21:00:00:04:cf:4c:18:61	20:00:00:04:cf:4c:18:61
fc2/3	1	0xb200d1	21:00:00:04:cf:4c:18:64	20:00:00:04:cf:4c:18:64
fc2/3	1	0xb200ce	21:00:00:04:cf:4c:16:fb	20:00:00:04:cf:4c:16:fb
fc2/3	1	0xb200cd	21:00:00:04:cf:4c:18:f7	20:00:00:04:cf:4c:18:f7
vfc3/1	2	0xb30100	10:00:00:05:30:00:49:63	20:00:00:05:30:00:49:5e

Total number of flogi = 6.

The following example shows how to verify the storage devices attached to a specific interface:

```
switch# show flogi database interface vfc1/1
```

INTERFACE	VSAN	FCID	PORT NAME	NODE NAME
vfc1/1	1	0x870000	20:00:00:1b:21:06:58:bc	10:00:00:1b:21:06:58:bc

[Send feedback to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

Total number of flogi = 1.

The following example shows how to verify the storage devices associated with VSAN 1:

```
switch# show flogi database vsan 1
```

Name Server Proxy

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 need 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:

- [About Registering Name Server Proxies, page 40-2](#)
- [Registering Name Server Proxies, page 40-2](#)
- [About Rejecting Duplicate pWWNs, page 40-2](#)
- [Rejecting Duplicate pWWNs, page 40-3](#)
- [About Name Server Database Entries, page 40-3](#)
- [Displaying Name Server Database Entries, page 40-3](#)

About Registering Name Server Proxies

All name server registration requests come from the same port whose parameter is registered or changed. If it does not, 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, perform this task:

	Command	Purpose
Step 1	switch# configuration terminal switch(config)#	Enters configuration mode.
Step 2	switch(config)# fcns proxy-port <i>wwn-id</i> vsan <i>vsan-id</i>	Configures a proxy port for the specified VSAN.

About Rejecting Duplicate pWWNs

You can prevent malicious or accidental log in using another device's pWWN by enabling the **reject-duplicate-pwwn** option. If you disable this option, these pWWNs are allowed to log in to the fabric and replace the first device in the name server database.

[Send feedback to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

Rejecting Duplicate pWWNs

To reject duplicate pWWNs, perform this task:

	Command	Purpose
Step 1	switch# configuration terminal switch(config)#	Enters configuration mode.
Step 2	switch(config)# fcns reject-duplicate-pwwn vsan vsan-id	Logs out devices when they log into the fabric if the pWWNs already exist.
	switch(config)# no fcns reject-duplicate-pwwn vsan vsan-id	Overwrites the first device's entry in the name server database with the new device having the same pWWN (default).

About 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.

Displaying Name Server Database Entries

The following example shows how to display the name server database for all VSANs:

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

The following example shows how to display the name server database and statistical information for a 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

The following example shows how to display the name server database details for all VSANs:

```
switch# show fcns database detail
```

Send feedback to nx5000-docfeedback@cisco.com

The following example shows how to display the name server database statistics for all VSANs:

```
switch# show fcns statistics
```

FDMI

Cisco Nexus 5000 Series 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 switch 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

The following example shows how to display all HBA details for a specified VSAN:

```
switch# show fDMI database detail vsan 1
```

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, page 40-5](#)
- [Displaying RSCN Information, page 40-5](#)
- [About the multi-pid Option, page 40-5](#)
- [Configuring the multi-pid Option, page 40-6](#)

Send feedback to nx5000-docfeedback@cisco.com

- [Suppressing Domain Format SW-RSCNs, page 40-6](#)
- [Clearing RSCN Statistics, page 40-6](#)
- [Configuring the RSCN Timer, page 40-7](#)
- [Verifying the RSCN Timer Configuration, page 40-7](#)
- [RSCN Timer Configuration Distribution, page 40-8](#)

About RSCN Information

A switch RSCN (SW-RSCN) is sent to registered hosts and 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

The following example shows how to display registered device information:

```
switch# show rscn scr-table vsan 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.

About the 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, 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, one of the following actions 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 support multi-pid RSCN payloads. If so, disable the RSCN **multi-pid** option.

[Send feedback to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

Configuring the multi-pid Option

To configure the **multi-pid** option, perform this task:

	Command	Purpose
Step 1	switch# configuration terminal switch(config)#	Enters configuration mode.
Step 2	switch(config)# rscn multi-pid vsan <i>vsan-id</i>	Sends RSCNs in a multi-pid format for the specified VSAN.

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 SAN switches (see the [Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide](#)).

To suppress the transmission of these SW-RSCNs over an ISL, perform this task:

	Command	Purpose
Step 1	switch# configuration terminal switch(config)#	Enters configuration mode.
Step 2	switch(config)# rscn suppress domain-swrsn vsan <i>vsan-id</i>	Suppresses transmission of domain format SW-RSCNs for the specified VSAN.



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

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.

The following example shows how 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 entering the **show rscn statistics** command:

```
switch# show rscn statistics vsan 1
```

[Send feedback to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

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”](#) section on page 40-8.



Note Before performing a downgrade, make sure that you revert the RSCN 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, perform this task:

	Command	Purpose
Step 1	switch# configuration terminal switch(config)#	Enters configuration mode.
Step 2	switch(config)# rscn distribute	Enables RSCN timer configuration distribution.
Step 3	switch(config)# rscn event-tov timeout vsan <i>vsan-id</i>	Sets the event time-out value in milliseconds for the specified VSAN. The range is 0 to 2000 milliseconds. Setting a zero (0) value disables the timer.
	switch(config)# no rscn event-tov timeout vsan <i>vsan-id</i>	Reverts to the default value (2000 milliseconds for Fibre Channel VSANs).
Step 4	switch(config)# rscn commit vsan <i>vsan-id</i>	Commits the RSCN timer configuration to be distributed to the switches in the specified VSAN.

In this example the event time-out value is set to 300 milliseconds for VSAN 12.

```
switch# rscn event-tov 300 vsan 12
```

Verifying the RSCN Timer Configuration

You verify the RSCN timer configuration using the **show rscn event-tov vsan** command. The following example shows how to clear the RSCN statistics for VSAN 10:

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

[Send feedback to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

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. For additional information, see [Chapter 21, “Using Cisco Fabric Services.”](#)

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.

This section includes the following topics:

- [Enabling RSCN Timer Configuration Distribution, page 40-8](#)
- [Locking the Fabric, page 40-9](#)
- [Committing the RSCN Timer Configuration Changes, page 40-9](#)
- [Discarding the RSCN Timer Configuration Changes, page 40-9](#)
- [Clearing a Locked Session, page 40-9](#)
- [Displaying RSCN Configuration Distribution Information, page 40-10](#)

Enabling RSCN Timer Configuration Distribution

To enable RSCN timer configuration distribution, perform this task:

	Command	Purpose
Step 1	switch# configuration terminal switch(config)#	Enters configuration mode.
Step 2	switch(config)# rscn distribute	Enables RSCN timer distribution.
	switch(config)# no rscn distribute	Disables (default) RSCN timer distribution.

Send feedback to nx5000-docfeedback@cisco.com

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, perform this task:

	Command	Purpose
Step 1	switch# configuration terminal switch(config)#	Enters configuration mode.
Step 2	switch(config)# rscn commit vsan timeout	Commits the RSCN timer changes.

Discarding the RSCN Timer Configuration Changes

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

To discard RSCN timer configuration changes, perform this task:

	Command	Purpose
Step 1	switch# configuration terminal switch(config)#	Enters configuration mode.
Step 2	switch(config)# rscn abort vsan timeout	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. The following example shows how to clear the RSCN session for VSAN 10:

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

[Send feedback to nx5000-docfeedback@cisco.com](mailto:nx5000-docfeedback@cisco.com)

Displaying RSCN Configuration Distribution Information

The following example shows how to display the registration status for RSCN configuration distribution:

```
switch# show cfs application name rscn

Enabled       : Yes
Timeout      : 5s
Merge Capable : Yes
Scope        : Logical
```



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

The following example shows how 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
```

The following example shows how to display the difference between pending and active configurations:

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

Default Settings

Table 40-1 lists the default settings for RSCN.

Table 40-1 Default RSCN Settings

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