



## CHAPTER 19

# 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 19-1](#)
- [Name Server Proxy, page 19-2](#)
- [FDMI, page 19-4](#)
- [Displaying FDMI, page 19-4](#)
- [RSCN, page 19-5](#)
- [Default Settings, page 19-8](#)

## Information About Fabric Login

In a Fibre Channel fabric, each host or disk requires an FC ID. 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. See the [“Default Company ID List” section on page 22-7](#) and the [“Switch Interoperability” section on page 22-7](#).

To verify that a storage device is in the fabric login (FLOGI) table using Fabric Manager, perform this task:

- 
- Step 1** In the Physical Attributes pane, expand **Switches > Interfaces**, and then choose **FC Physical**.  
You see the interface configuration in the Information pane.
- Step 2** Click the **FLOGI** tab.  
You see all end devices that are logged into the fabric as shown in [Figure 19-1](#).

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

**Figure 19-1 FLOGI Physical Interfaces**

Switch	Interface, VSAN Id	FcId	PortName	NodeName	Version	CoS	Class 2 RxDataSize	Class 2 SeqDeliv	Class 3 RxDataSize	Class 3 SeqDeliv
sw172-22-46-224	Fc1/6, 4001	ea0197	Seagate 22:00:00:20:37:73:de:d6	Seagate 20:00:00:20:37:73:de:d6	32/3		0	false	2112	true
sw172-22-46-224	Fc1/6, 4001	ea019b	Seagate 22:00:00:20:37:46:56:52	Seagate 20:00:00:20:37:46:56:52	32/3		0	false	2112	true
sw172-22-46-224	Fc1/6, 4001	ea019f	Seagate 22:00:00:20:37:4b:35:1a	Seagate 20:00:00:20:37:4b:35:1a	32/3		0	false	2112	true
sw172-22-46-224	Fc1/6, 4001	ea01a3	Seagate 22:00:00:20:37:5b:b1:8e	Seagate 20:00:00:20:37:5b:b1:8e	32/3		0	false	2112	true
sw172-22-46-224	Fc1/6, 4001	ea01a7	Seagate 22:00:00:20:37:5b:81:1b	Seagate 20:00:00:20:37:5b:81:1b	32/3		0	false	2112	true

## 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 19-2](#)
- [Registering Name Server Proxies, page 19-2](#)
- [About Rejecting Duplicate pWWNs, page 19-3](#)
- [Rejecting Duplicate pWWNs, page 19-3](#)
- [About Name Server Database Entries, page 19-3](#)
- [Viewing Name Server Database Entries, page 19-3](#)

## 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.

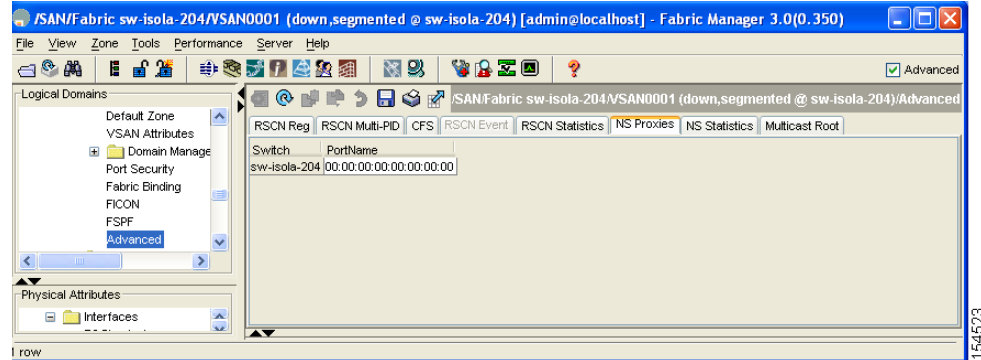
## Registering Name Server Proxies

To register the name server proxy using Fabric Manager, perform this task:

- 
- Step 1** Expand a fabric, expand a VSAN, and then choose **Advanced**.  
You see the VSAN advanced configuration in the Information pane.
- Step 2** Click the **NS Proxies** tab.  
You see the existing name server proxy for the selected VSAN as shown in [Figure 19-2](#).

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

**Figure 19-2** Name Server Proxies



- Step 3** Double-click the PortName field and enter a new value to register a new name server proxy.
- Step 4** Click **Apply Changes** to save these changes, or click **Undo Changes** to cancel any unsaved changes.

## About Rejecting Duplicate pWWNs

You can prevent malicious or accidental log in using another device's pWWN. These pWWNs are allowed to log in to the fabric and replace the first device in the name server database.

## Rejecting Duplicate pWWNs

To reject duplicate pWWNs, see the *Cisco Cisco Nexus 5000 Series CLI Configuration Guide*.

## 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.

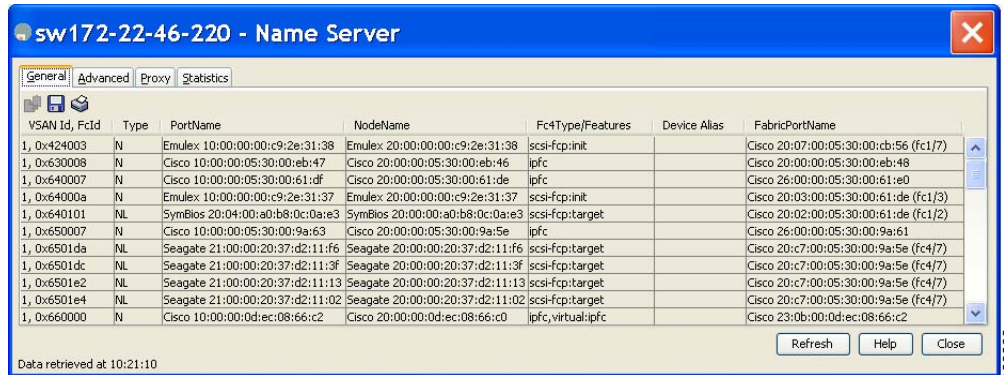
## Viewing Name Server Database Entries

To view the name server database using Device Manager, perform this task:

- Step 1** Click **FC > Name Server**.
- You see the Name Server dialog box as shown in [Figure 19-3](#).

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

Figure 19-3 Name Server Dialog Box



The General tab is the default tab; you see the name server database.

**Step 2** Click the **Statistics** tab.

You see the name server statistics.

**Step 3** Click **Close** to close the dialog box.

## 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

To display the FDMI database information using Device Manager, perform this task:

**Step 1** Click **FC > Advanced > FDMI**

You see the FDMI dialog box.

**Step 2** Click the **HBA** tab, the **Versions** tab or the **Targets** tab.

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

## 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 19-5](#)
- [Displaying RSCN Information, page 19-5](#)
- [About the multi-pid Option, page 19-6](#)
- [Configuring the multi-pid Option, page 19-6](#)
- [Configuring the multi-pid Option, page 19-6](#)
- [Configuring the multi-pid Option, page 19-6](#)
- [Clearing RSCN Statistics, page 19-7](#)
- [RSCN Timer Configuration Distribution Using CFS, page 19-7](#)
- [Configuring the RSCN Timer with CFS, page 19-8](#)

## 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

To display RSCN information using Fabric Manager, perform this task:

- Step 1** Expand a fabric, expand a VSAN, and then choose **Advanced**.  
You see the VSAN advanced configuration in the Information pane.
- Step 2** Click the **RSCN Reg** tab or the **RSCN Statistics** tab (see [Figure 19-4](#)).  
You see the RSCN Statistics pane as shown in [Figure 19-4](#).

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

Figure 19-4 RSCN Statistics

Switch	SCR Rx	SCR R/T	RSCN Rx	RSCN Tx	RSCN R/T	SW-RSCN Rx	SW-RSCN Tx	SW-RSCN R/T
sw-isola-204	0	0	0	0	0	0	0	0

1 row

## 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.

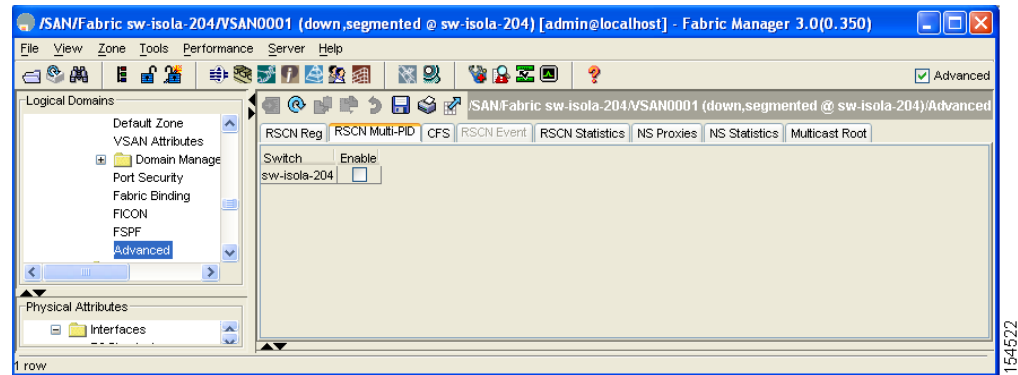
## Configuring the multi-pid Option

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

- Step 1** Expand a fabric, expand a VSAN, and then choose **Advanced**.  
You see the VSAN advanced configuration in the Information pane.
- Step 2** Click the **RSCN Multi-PID** tab.  
You see the RSCN Multi-PID pane as shown in [Figure 19-5](#).

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

**Figure 19-5 RSCN Multi-PID**



**Step 3** Check the **Enable** check box.

**Step 4** Click **Apply Changes** to save these changes, or click **Undo Changes** to cancel any unsaved changes.

## 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.

To clear the RSCN statistics for the specified VSAN, see the *Cisco Cisco Nexus 5000 Series CLI Configuration Guide*.

## 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.

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

**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.

Compatibility across various software releases during an upgrade or downgrade is supported by **conf-check** provided by CFS. You are required to disable RSCN timer distribution support before you downgrade. By default, the RSCN timer distribution capability is disabled.

## Configuring the RSCN Timer with CFS

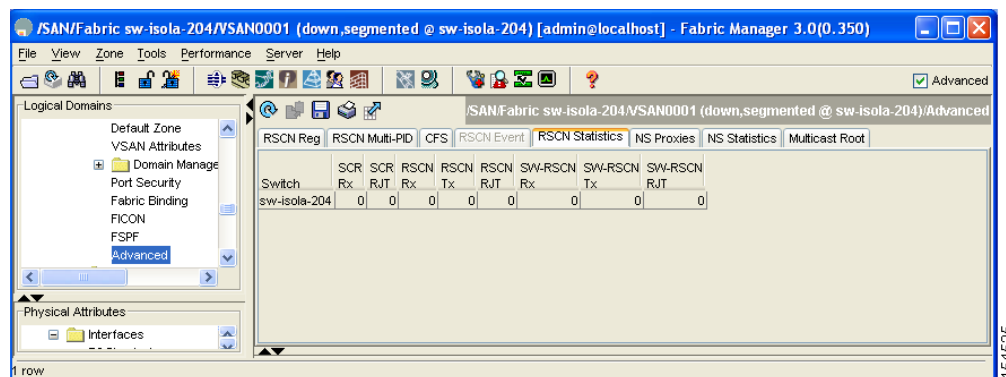
To configure the RSCN timer with CFS using Fabric Manager, perform this task:

**Step 1** Expand a fabric, expand a VSAN, and then choose **Advanced** in the Logical Domains pane.

**Step 2** Click the **RSCN Event** tab.

You see the VSAN advanced configuration in the Information pane as shown in [Figure 19-6](#).

**Figure 19-6 VSAN Advanced Configuration**



**Step 3** Double-click the **TimeOut** value to change the value (in milliseconds) for the selected VSAN.

**Step 4** Click **Apply Changes** to save these changes, or click **Undo Changes** to cancel any unsaved changes.

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

## Default Settings

[Table 19-1](#) lists the default settings for RSCN.

**Table 19-1 Default RSCN Settings**

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



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

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