CHAPTER 22

# Advanced Features and Concepts

This chapter describes the advanced Fibre Channel features provided in Cisco Nexus 5000 Series switches. It includes the following sections:



## Fibre Channel Timeout Values

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

- Distributed services TOV (D_S_TOV)—The valid range is from 5,000 to 10,000 milliseconds. The default is 5,000 milliseconds.
- Error detect TOV (E_D_TOV)—The valid range is from 1,000 to 10,000 milliseconds. The default is 2,000 milliseconds. This value is matched with the other end during port initialization.
- Resource allocation TOV (R_A_TOV)—The valid range is from 5,000 to 10,000 milliseconds. The default is 10,000 milliseconds. This value is matched with the other end during port initialization.

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

This section includes the following topics:

# Timer Configuration Across All VSANs

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

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

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

To configure timers in Fabric Manager, perform this task:

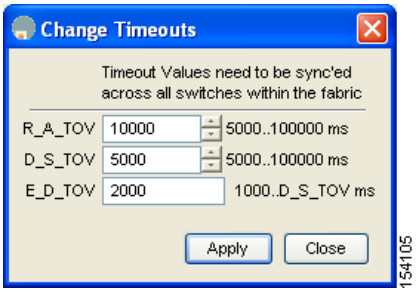
**Step 1** Expand **Switches > FC Services**, and then choose **Timers & Policies** in the Physical Attributes pane.

You see the timers for multiple switches in the Information pane.

**Step 2** Click the **Change Timeouts** button to configure the timeout values.

You see the dialog box as shown in Figure 22-1.

***Figure 22-1 Configure Timers in Fabric Manager***

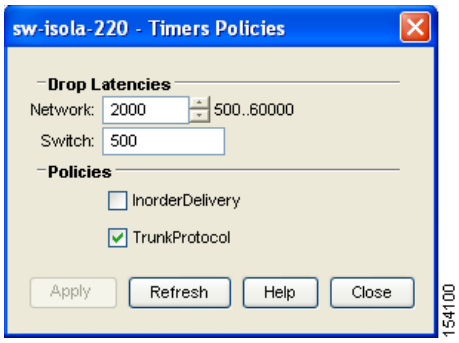



To configure timers in Device Manager, perform this task:

**Step 1** Choose **FC > Advanced > Timers/Policies**.

You see the timers for a single switch in the dialog box as shown in Figure 22-2.

*Figure 22-2 Configure Timers in Device Manager*




# Timer Configuration Per-VSAN

You can also issue the fctimer for a specified VSAN to configure different TOV values for VSANs with special links such as Fibre Channel. You can configure different E_D_TOV, R_A_TOV, and D_S_TOV values for individual VSANs. Active VSANs are suspended and activated when their timer values are changed.

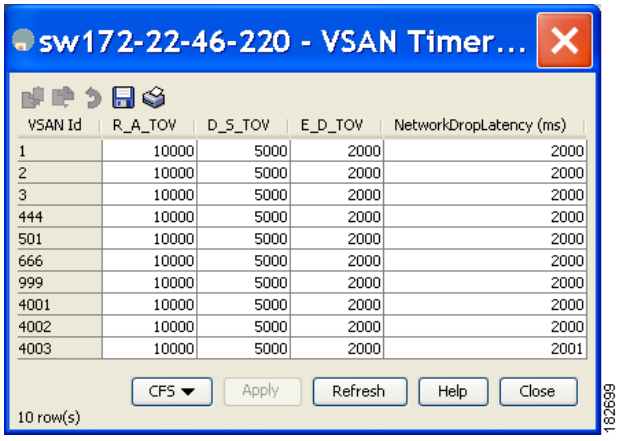
**Note** This configuration must be propagated to all switches in the fabric. Be sure to configure the same value in all switches in the fabric.

To configure per-VSAN Fiber Channel timers using Device Manager, perform this task:

**Step 1** Choose **FC > Advanced > VSAN Timers**.

You see the VSANs Timer dialog box as shown in Figure 22-3.

*Figure 22-3 VSAN Timers in Device Manager*




**Step 2** Fill in the timer values that you want to configure.

**Step 3** Click **Apply** to save these changes.

# About fctimer Distribution

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

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

See Chapter 7, "Using Cisco Fabric Services," for more information on the CFS application.

# Enabling or Disabling fctimer Distribution

To enable and distribute fctimer configuration changes using Device Manager, perform this task:

**Step 1** Choose **FC > Advanced > VSAN Timers**.

You see the VSANs Timer dialog box as shown in Figure 22-3.

**Step 2** Fill in the timer values that you want to configure.

**Step 3** Click **Apply** to save these changes.

**Step 4** Choose **commit** from the CFS drop-down list to distribute these changes or choose **abort** from the CFS drop-down list to discard any unsaved changes.

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

# Database Merge Guidelines

When merging two fabrics, follow these guidelines:

- Be aware of the following merge conditions:
  - The merge protocol is not implemented for distribution of the fctimer values. You must manually merge the fctimer values when a fabric is merged.
  - The per-VSAN fctimer configuration is distributed in the physical fabric.
  - The fctimer configuration is only applied to those switches containing the VSAN with a modified fctimer value.
  - The global fctimer values are not distributed.
- Do not configure global timer values when distribution is enabled.

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

See the "CFS Merge Support" section on page 7-6 for additional information.

# World Wide Names

The world wide name (WWN) in the switch is equivalent to the Ethernet MAC address. As with the MAC address, you must uniquely associate the WWN to a single device. The principal switch selection and the allocation of domain IDs rely on the WWN.

Cisco Nexus 5000 Series switches support three network address authority (NAA) address formats (see Table 22-1).

*Table 22-1 Standardized NAA WWN Formats*

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

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

This section includes the following topics:



## Verifying WWN Information

To display WWN information using Device Manager, choose **FC > Advanced > WWN Manager.** You see the list of allocated WWNs.

## Link Initialization WWN Usage

Exchange Link Protocol (ELP) and Exchange Fabric Protocol (EFP) use WWNs during link initialization. ELPs and EFPs both use the VSAN WWN by default during link initialization. However, the ELP usage changes based on the peer switch's usage:

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

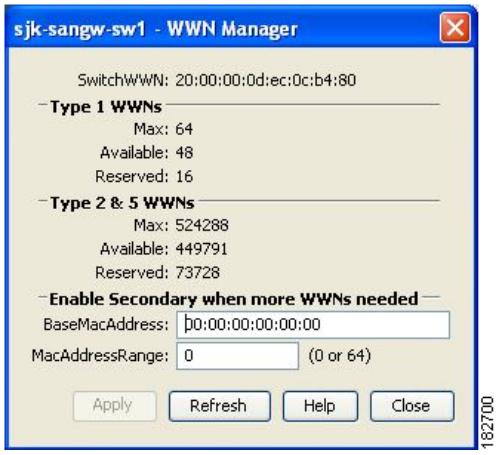
## Configuring a Secondary MAC Address

To allocate secondary MAC addresses using Device Manager, perform this task:

**Step 1** Choose **FC > Advanced > WWN Manager.**

You see the list of allocated WWNs as shown in Figure 22-4.

*Figure 22-4 Allocated World Wide Names in Device Manager*




**Step 2** Fill in the BaseMacAddress and MacAddressRange fields with the appropriate values.

**Step 3** Click **Apply** to save these changes, or click **Close** to discard any unsaved changes.

# FC ID Allocation for HBAs

Fibre Channel standards require a unique FC ID to be allocated to an N port attached to an F port in any switch. To conserve the number of FC IDs used, Cisco Nexus 5000 Series switches use a special allocation scheme.

Some HBAs do not discover targets that have FC IDs with the same domain and area. The switch software maintains a list of tested company IDs that do not exhibit this behavior. These HBAs are allocated with single FC IDs. If the HBA can discover targets within the same domain and area, a full area is allocated.

To allow further scalability for switches with numerous ports, the switch software maintains a list of HBAs that can discover targets within the same domain and area. Each HBA is identified by its company ID (also known as Organizational Unique Identifier, or OUI) used in the pWWN during a fabric log in. A full area is allocated to the N ports with company IDs that are listed and for the others, a single FC ID is allocated. Regardless of the type (whole area or single) of FC ID allocated, the FC ID entries remain persistent.

This section includes the following topics:

## Default Company ID List

All Cisco Nexus 5000 Series switches contain a default list of company IDs that require area allocation. Using the company ID reduces the number of configured persistent FC ID entries. You can configure or modify these entries using the CLI.

**Caution** Persistent entries take precedence over company ID configuration. If the HBA fails to discover a target, verify that the HBA and the target are connected to the same switch and have the same area in their FC IDs, then perform the following procedure:

1. Shut down the port connected to the HBA.
2. Clear the persistent FC ID entry.
3. Get the company ID from the port WWN.
4. Add the company ID to the list that requires area allocation.
5. Bring up the port.

The list of company IDs have the following characteristics:

- A persistent FC ID configuration always takes precedence over the list of company IDs. Even if the company ID is configured to receive an area, the persistent FC ID configuration results in the allocation of a single FC ID.
- New company IDs added to subsequent releases are automatically added to existing company IDs.
- The list of company IDs is saved as part of the running and saved configuration.
- The list of company IDs is used only when the fcinterop FC ID allocation scheme is in auto mode. By default, the interop FC ID allocation is set to auto, unless changed.

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

See the *Cisco Cisco Nexus 5000 Series CLI Configuration Guide* to change the FC ID allocation.

The following example adds a new company ID to the default list.

```
switch(config)# fcid-allocation area company-id 0x003223
```

## Verifying the Company ID Configuration

To view the configured company IDs using Device Manager, choose **FC > Advanced > FcId Area Allocation**. You can implicitly derive the default entries shipped with a specific release by combining the list of Company IDs displayed without any identification with the list of deleted entries.

Some WWN formats do not support company IDs. In these cases, you may need to configure the FC ID persistent entry.

# Switch Interoperability

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

Not all vendors follow the standards in the same way, which results in the need for interoperability modes. This section briefly explains the basic concepts of these modes.

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

This section includes the following topics:



# About Interop Mode

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

- Mode 1— Standards-based interop mode that requires all other vendors in the fabric to be in interop mode.
- Mode 2—Brocade native mode (Core PID 0).
- Mode 3—Brocade native mode (Core PID 1).
- Mode 4—McData native mode.

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

Table 22-2 lists the changes in switch operation when you enable interoperability mode. These changes are specific to Cisco Nexus 5000 Series switches while in interop mode.

***Table 22-2 Changes in Switch Operation When Interoperability Is Enabled***

| Switch Feature | Changes if Interoperability Is Enabled |
|---|---|
| Domain IDs | Some vendors cannot use the full range of 239 domains within a fabric.<br>Domain IDs are restricted to the range 97 to 127, to accommodate McData's nominal restriction to this same range. Domain IDs can either be static or preferred, which operate as follows:<br>• Static: Cisco switches accept only one domain ID; if a switch does not get that domain ID it isolates itself from the fabric.<br>• Preferred: If the switch does not get its requested domain ID, it accepts any assigned domain ID. |
| Timers | All Fibre Channel timers must be the same on all switches as these values are exchanged by E ports when establishing an ISL. The timers are F_S_TOV, D_S_TOV, E_D_TOV, and R_A_TOV. |
| F_S_TOV | Verify that the Fabric Stability Time Out Value timers match exactly. |
| D_S_TOV | Verify that the Distributed Services Time Out Value timers match exactly. |
| E_D_TOV | Verify that the Error Detect Time Out Value timers match exactly. |
| R_A_TOV | Verify that the Resource Allocation Time Out Value timers match exactly. |
| Trunking | Trunking is not supported between two different vendor's switches. This feature may be disabled on a per port or per switch basis. |

*Table 22-2 Changes in Switch Operation When Interoperability Is Enabled (continued)*

| Switch Feature | Changes if Interoperability Is Enabled |
|---|---|
| Default zone | The default zone operation of permit (all nodes can see all other nodes) or deny (all nodes are isolated when not explicitly placed in a zone) may change. |
| Zoning attributes | Zones may be limited to the pWWN and other proprietary zoning methods (physical port number) may be eliminated.<br>**Note** On a Brocade switch, use the **cfgsave** command to save fabric-wide zoning configuration. This command does not have any effect on Cisco Nexus 5000 Series switches if they are part of the same fabric. You must explicitly save the configuration on each Cisco Nexus 5000 Series switch. |
| Zone propagation | Some vendors do not pass the full zone configuration to other switches, only the active zone set gets passed.<br>Verify that the active zone set or zone configuration has correctly propagated to the other switches in the fabric. |
| VSAN | Interop mode only affects the specified VSAN.<br>**Note** Interop modes cannot be enabled on FICON-enabled VSANs. |
| TE ports and SAN port channel s | TE ports and SAN port channels cannot be used to connect Cisco switches to non-Cisco SAN switches. Only E ports can be used to connect to non-Cisco SAN switches. TE ports and SAN port channels can still be used to connect a Cisco switch to other Cisco SAN switches even when in interop mode. |
| FSPF | The routing of frames within the fabric is not changed by the introduction of interop mode. The switch continues to use src-id, dst-id, and ox-id to load balance across multiple ISL links. |
| Domain reconfiguration disruptive | This is a switch-wide impacting event. Brocade and McData require the entire switch to be placed in offline mode and/or rebooted when changing domain IDs. |
| Domain reconfiguration nondisruptive | This event is limited to the affected VSAN. Cisco Nexus 5000 Series switches have the capability to restart only the domain manager process for the affected VSAN and not the entire switch. |
| Name server | Verify that all vendors have the correct values in their respective name server database. |

# Configuring Interop Mode 1

The interop mode1 in Cisco Nexus 5000 Series switches can be enabled disruptively or nondisruptively.

**Note** Brocade's **msplmgmtdeactivate** command must explicitly be run prior to connecting from a Brocade switch to either Cisco Nexus 5000 Series switches or to McData switches. This command uses Brocade proprietary frames to exchange platform information, which Cisco Nexus 5000 Series switches or McData switches do not understand. Rejecting these frames causes the common E ports to become isolated.

To configure interop mode 1 for a VSAN using Fabric Manager, perform this task:

**Step 1** Choose **VSAN*xxx* > VSAN Attributes** from the Logical Domains pane.

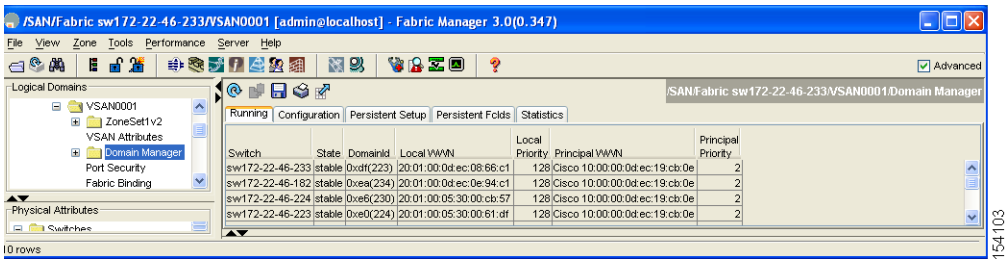
**Step 2** Choose **Interop-1** from the Interop drop-down list.

**Step 3** Click **Apply Changes** to save this interop mode.

**Step 4** Expand **VSAN*xxx***, and then choose **Domain Manager** from the Logical Domains pane.

You see the Domain Manager configuration in the Information pane as shown in Figure 22-5.

***Figure 22-5 Domain Manager Configuration***




**Step 5** Set the Domain ID in the range of 97 (0x61) through 127 (0x7F).

a. Click the **Configuration** tab.

b. Click in the Config Domain ID column under the Configuration tab.

c. Click the **Running** tab and verify that the change has been made.

**Note** The domain ID range limit is to accommodate McData switches.

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

**Step 6** Change the Fibre Channel timers (if they have been changed from the system defaults).

**Note** The Cisco, Brocade, and McData FC error detect (ED_TOV) and resource allocation (RA_TOV) timers default to the same values. They can be changed if needed. The RA_TOV default is 10 seconds, and the ED_TOV default is 2 seconds. Per the FC-SW2 standard, these values must be the same on each switch within the fabric.

a. Expand **Switches > FC Services**, and then choose **Timers and Policies**.

You see the timer settings in the Information pane.

b. Click **Change Timeouts** to modify the time-out values.

c. Click **Apply** to save the new time-out values.

**Step 7** (Optional) Choose **VSAN*xxx* > Domain Manager,** click the **Configuration** tab, and choose **disruptive** or **nonDisruptive** in the Restart drop-down list to restart the domain.

# Verifying Interoperating Status

This section highlights the steps used to verify if the fabric is up and running in interoperability mode.

To verify the interoperability status of the Cisco Cisco Nexus 5000 Series switch using Fabric Manager, perform this task:

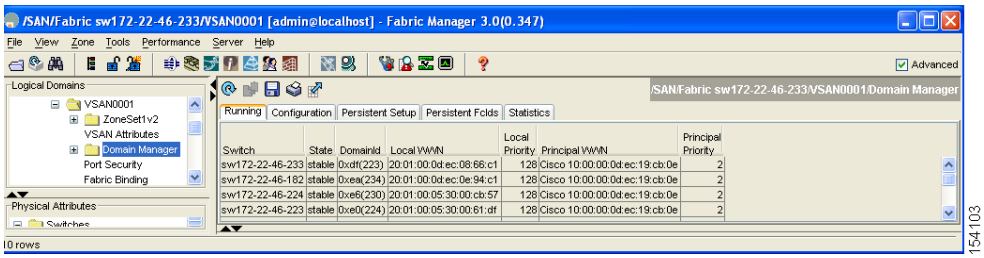
**Step 1** Choose **Switches** in the Physical Attributes pane and check the release number in the Information pane to verify the Cisco SAN-OS release.

**Step 2** In the Physical Attributes pane, expand **Switches** > **Interfaces**, and then choose **FC Physical** to verify the interface modes for each switch.

**Step 3** Expand **Fabric*xx*** in the Logical Domains pane, and then choose **All VSANs** to verify the interop mode for all VSANs.

**Step 4** Expand **Fabric*xx* > All VSANs**, and then choose **Domain Manager** to verify the domain IDs, local, and principal sWWNs for all VSANs (see Figure 22-6).

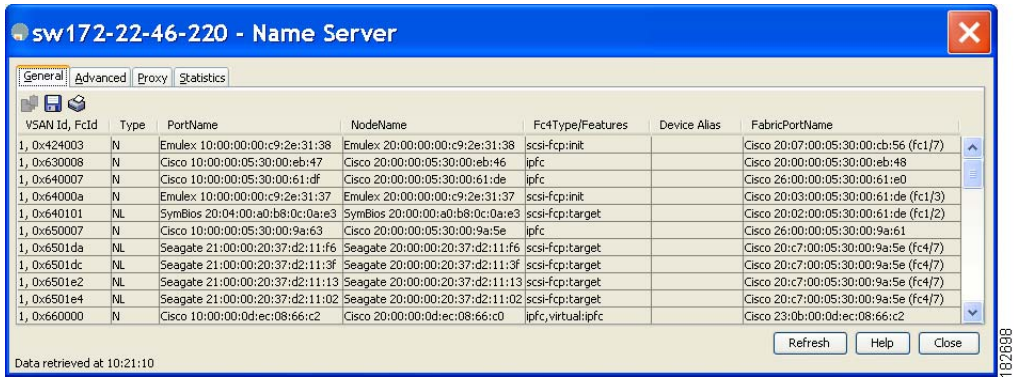
***Figure 22-6 Domain Manager Information***




**Step 5** Using Device Manager, choose **FC > Name Server** to verify the name server information.

You see the Name Server dialog box as shown in Figure 22-7.

***Figure 22-7 Name Server Dialog Box***




**Step 6** Click **Close** to close the dialog box.

**Note** The Cisco switch name server shows both local and remote entries, and does not time out the entries.

# Default Settings

Table 22-3 lists the default settings for the features included in this chapter.

*Table 22-3 Default Settings for Advanced Features*

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