CHAPTER 10

Configuring Domain Parameters

The Fibre Channel domain (fcdomain) feature performs principal switch selection, domain ID distribution, FC ID allocation, and fabric reconfiguration functions as described in the FC-SW-2 standards.

This chapter includes the following sections:

Information About Fibre Channel Domains

The Fibre Channel domain (fcdomain) feature performs principal switch selection, domain ID distribution, FC ID allocation, and fabric reconfiguration functions as described in the FC-SW-2 standards. The domains are configured on a per VSAN basis. If you do not configure a domain ID, the local switch uses a random ID.

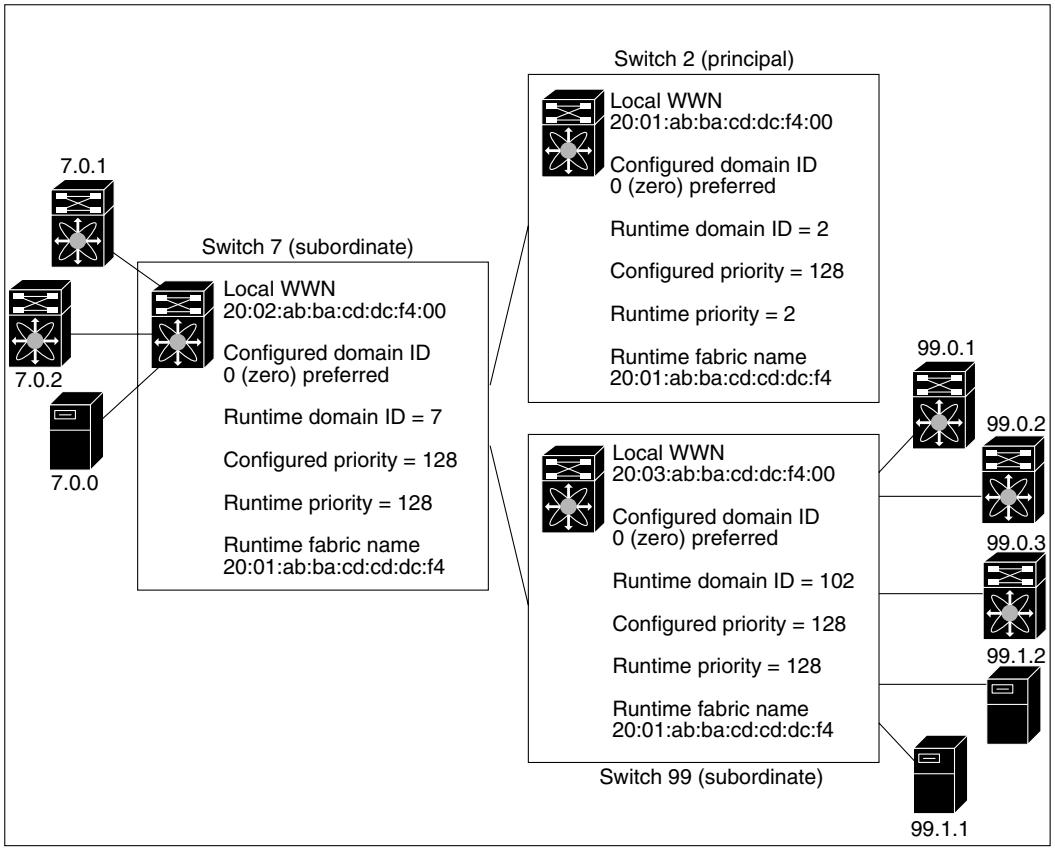
This section describes each fcdomain phase:

- Principal switch selection—This phase guarantees the selection of a unique principal switch across the fabric.
- Domain ID distribution—This phase guarantees each switch in the fabric obtains a unique domain ID.
- FC ID allocation—This phase guarantees a unique FC ID assignment to each device attached to the corresponding switch in the fabric.
- Fabric reconfiguration—This phase guarantees a resynchronization of all switches in the fabric to ensure they simultaneously restart a new principal switch selection phase.

Caution Changes to fcdomain parameters should not be performed on a daily basis. These changes should be made by an administrator or individual who is completely familiar with switch operations.

Figure 10-1 shows a sample fcdomain configuration.

Figure 10-1 Sample fcdomain Configuration



This section includes the following topics:

- Domain Restart, page 10-3
- Domain Manager Fast Restart, page 10-3
- Switch Priority, page 10-4
- fcdomain Initiation, page 10-4
- Incoming RCFs, page 10-4
- Autoreconfiguring Merged Fabrics, page 10-4
- Domain IDs, page 10-4
- Locking the Fabric, page 10-7
- Committing Changes, page 10-7
- Clearing a Fabric Lock, page 10-7

- FC IDs, page 10-8

Domain Restart

Fibre Channel domains can be started disruptively or nondisruptively. If you perform a disruptive restart, reconfigure fabric (RCF) frames are sent to other switches in the fabric and data traffic is disrupted on all the switches in the VSAN (including remotely segmented ISLs). If you perform a nondisruptive restart, build fabric (BF) frames are sent to other switches in the fabric and data traffic is disrupted only on the switch.

If you are attempting to resolve a domain ID conflict, you must manually assign domain IDs. A disruptive restart is required to apply most configuration changes, including manually assigned domain IDs. Nondisruptive domain restarts are acceptable only when changing a preferred domain ID into a static one (and the actual domain ID remains the same).

Note A static domain is specifically configured by the user and may be different from the runtime domain. If the domain IDs are different, the runtime domain ID changes to take on the static domain ID after the next restart, either disruptive or nondisruptive.

Tip If a VSAN is in interop mode, you cannot restart the fcdomain for that VSAN disruptively.

You can apply most of the configurations to their corresponding runtime values. Each of the following sections provide further details on how the fcdomain parameters are applied to the runtime values.

Domain Manager Fast Restart

As of Cisco MDS SAN-OS Release 3.0(2), when a principal link fails, the domain manager must select a new principal link. By default, the domain manager starts a build fabric (BF) phase, followed by a principal switch selection phase. Both of these phases involve all the switches in the VSAN and together take at least 15 seconds to complete. To reduce the time required for the domain manager to select a new principal link, you can enable the domain manager fast restart feature.

When fast restart is enabled and a backup link is available, the domain manager needs only a few milliseconds to select a new principal link to replace the one that failed. Also, the reconfiguration required to select the new principal link only affects the two switches that are directly attached to the failed link, not the entire VSAN. When a backup link is not available, the domain manager reverts to the default behavior and starts a BF phase, followed by a principal switch selection phase. The fast restart feature can be used in any interoperability mode.

Tip We recommend using fast restart on most fabrics, especially those with a large number of logical ports (3200 or more), where a logical port is an instance of a physical port in a VSAN.

Switch Priority

Any new switch can become the principal switch when it joins a stable fabric. During the principal switch selection phase, the switch with the highest priority becomes the principal switch. If two switches have the same configured priority, the switch with the lower WWN becomes the principal switch.

The priority configuration is applied to runtime when the fcdomain is restarted (see the "Domain Restart" section on page 10-3). This configuration is applicable to both disruptive and nondisruptive restarts.

fcdomain Initiation

By default, the fcdomain feature is enabled on each switch. If you disable the fcdomain feature in a switch, that switch can no longer participate with other switches in the fabric. The fcdomain configuration is applied to runtime through a disruptive restart.

Incoming RCFs

You can choose to reject RCF request frames on a per-interface, per-VSAN basis. By default, the RCF reject option is disabled (that is, RCF request frames are not automatically rejected).

The RCF reject option takes immediate effect at runtime through a disruptive restart (see the "Domain Restart" section on page 10-3).

Autoreconfiguring Merged Fabrics

By default, the autoreconfigure option is disabled. When you join two switches belonging to two different stable fabrics that have overlapping domains, the following cases apply:

- If the autoreconfigure option is enabled on both switches, a disruptive reconfiguration phase is started.
- If the autoreconfigure option is disabled on either or both switches, the links between the two switches become isolated.

The autoreconfigure option takes immediate effect at runtime. You do not need to restart the fcdomain. If a domain is currently isolated due to domain overlap, and you later enable the autoreconfigure option on both switches, the fabric continues to be isolated. If you enabled the autoreconfigure option on both switches before connecting the fabric, a disruptive reconfiguration (RCF) will occur. A disruptive reconfiguration may affect data traffic. You can nondisruptively reconfigure the fcdomain by changing the configured domains on the overlapping links and eliminating the domain overlap.

Domain IDs

Domain IDs uniquely identify a switch in a VSAN. A switch may have different domain IDs in different VSANs. The domain ID is part of the overall FC ID.

The configured domain ID can be preferred or static. By default, the configured domain ID is 0 (zero) and the configured type is preferred.

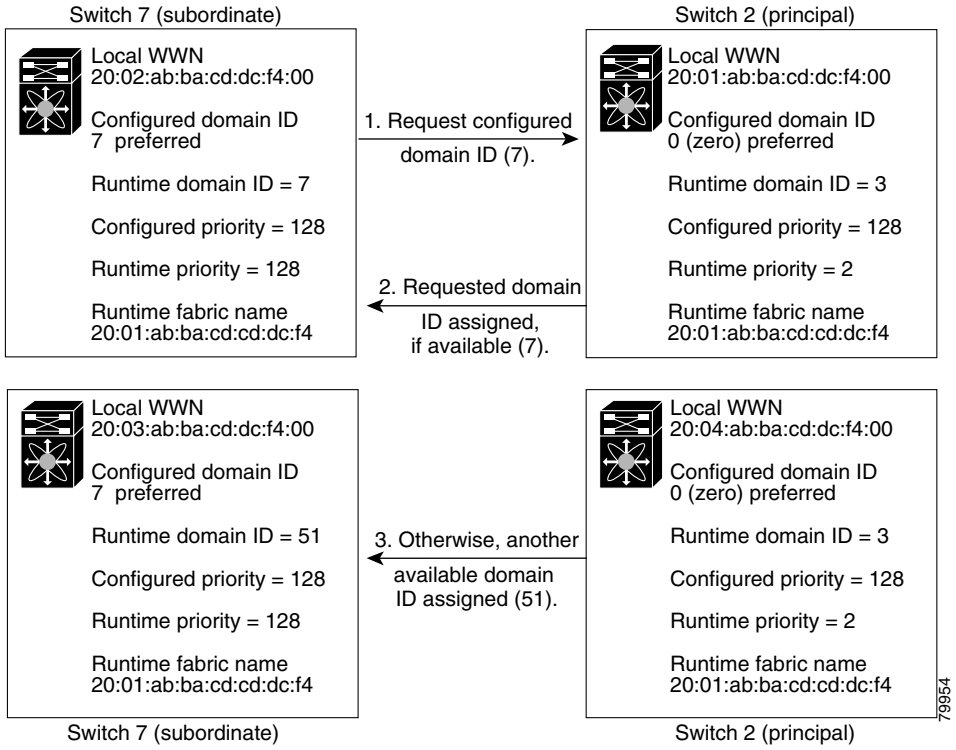
Note The 0 (zero) value can be configured only if you use the preferred option.

If you do not configure a domain ID, the local switch sends a random ID in its request. We recommend that you use static domain IDs.

When a subordinate switch requests a domain, the following process takes place (see Figure 10-2):

1. The local switch sends a configured domain ID request to the principal switch.
2. The principal switch assigns the requested domain ID if available. Otherwise, it assigns another available domain ID.

Figure 10-2 Configuration Process Using the preferred Option



The behavior for a subordinate switch changes based on three factors:

- The allowed domain ID lists.
- The configured domain ID.
- The domain ID that the principal switch has assigned to the requesting switch.

In specific situations, the changes are as follows:

- When the received domain ID is not within the allowed list, the requested domain ID becomes the runtime domain ID and all interfaces on that VSAN are isolated.
- When the assigned and requested domain IDs are the same, the preferred and static options are not relevant, and the assigned domain ID becomes the runtime domain ID.
- When the assigned and requested domain IDs are different, the following cases apply:

- If the configured type is static, the assigned domain ID is discarded, all local interfaces are isolated, and the local switch assigns itself the configured domain ID, which becomes the runtime domain ID.
- If the configured type is preferred, the local switch accepts the domain ID assigned by the principal switch and the assigned domain ID becomes the runtime domain ID.

If you change the configured domain ID, the change is only accepted if the new domain ID is included in all the allowed domain ID lists currently configured in the VSAN. Alternatively, you can also configure zero-preferred domain ID.

Tip When the FICON feature is enabled in a given VSAN, the domain ID for that VSAN remains in the static state. You can change the static ID value but you cannot change it to the preferred option.

Note In an IVR without NAT configuration, if one VSAN in the IVR topology is configured with static domain IDs, then the other VSANs (edge or transit) in the topology should also be configured with static domain IDs.
In an IVR NAT configuration, if one VSAN in the IVR topology is configured with static domain IDs, then the IVR domains that can be exported to that VSAN must also be assigned static domains.

Caution You must restart the **fcdomain** if you want to apply the configured domain changes to the runtime domain.

Note If you have configured an allowed domain ID list, the domain IDs that you add must be in that range for the VSAN. See the "Configuring Allowed Domain ID Lists" section on page 10-14.

Specifying Static or Preferred Domain IDs

When you assign a static domain ID type, you are requesting a particular domain ID. If the switch does not get the requested address, it will isolate itself from the fabric. When you specify a preferred domain ID, you are also requesting a particular domain ID; however, if the requested domain ID is unavailable, then the switch will accept another domain ID.

While the static option can be applied at runtime after a disruptive or nondisruptive restart, the preferred option is applied at runtime only after a disruptive restart (see the "Domain Restart" section on page 10-3).

Allowed Domain ID Lists

By default, the valid range for an assigned domain ID list is from 1 to 239. You can specify a list of ranges to be in the allowed domain ID list and separate each range with a comma. The principal switch assigns domain IDs that are available in the locally configured allowed domain list.

Use allowed domain ID lists to design your VSANs with non-overlapping domain IDs. This helps you in the future if you need to implement IVR without the NAT feature.

CFS Distribution of Allowed Domain ID Lists

You can enable the distribution of the allowed domain ID lists configuration information to all Cisco MDS switches in the fabric using the Cisco Fabric Services (CFS) infrastructure. This feature allows you to synchronize the configuration across the fabric from the console of a single MDS switch. Since the same configuration is distributed to the entire VSAN, you avoid possible misconfiguration and the likelihood that two switches in the same VSAN have configured incompatible allowed domains.

Use CFS to distribute the allowed domain ID list to ensure consistency in the allowed domain ID lists on all switches in the VSAN.

Note We recommend configuring the allow domain ID list and committing it on the principle switch.

For more information about CFS, see Chapter 2, "Using the CFS Infrastructure."

Contiguous Domain ID Assignments

By default, the contiguous domain assignment is disabled. When a subordinate switch requests the principal switch for two or more domains and the domains are not contiguous, the following cases apply:

- If the contiguous domain assignment is enabled in the principal switch, the principal switch locates contiguous domains and assigns them to the subordinate switches. If contiguous domains are not available, the NX-OS software rejects this request.
- If the contiguous domain assignment is disabled in the principal switch, the principal switch assigns the available domains to the subordinate switch.

Locking the Fabric

The first action that modifies the existing configuration creates the pending configuration and locks the feature in the fabric. Once you lock the fabric, the following conditions apply:

- No other user can make any configuration changes to this feature.
- A pending configuration is created by copying the active configuration. Modifications from this point on are made to the pending configuration and remain there until you commit the changes to the active configuration (and other switches in the fabric) or discard them.

Committing Changes

To apply the pending domain configuration changes to other MDS switches in the VSAN, you must commit the changes. The pending configuration changes are distributed and, on a successful commit, the configuration changes are applied to the active configuration in the MDS switches throughout the VSAN and the fabric lock is released.

Clearing a Fabric Lock

If you have performed a domain configuration task and have not released 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 pending changes are discarded and the fabric lock is released.

The pending changes are only available in the volatile directory and are discarded if the switch is restarted.

FC IDs

When an N or NL port logs into a Cisco MDS 9000 Family switch, it is assigned an FC ID. By default, the persistent FC ID feature is enabled. If this feature is disabled, the following consequences apply:

- An N or NL port logs into a Cisco MDS 9000 Family switch. The WWN of the requesting N or NL port and the assigned FC ID are retained and stored in a volatile cache. The contents of this volatile cache are not saved across reboots.
- The switch is designed to preserve the binding FC ID to the WWN on a best-effort basis. For example, if one N port disconnects from the switch and its FC ID is requested by another device, this request is granted and the WWN with the initial FC ID association is released.
- The volatile cache stores up to 4000 entries of WWN to FC ID binding. If this cache is full, a new (more recent) entry overwrites the oldest entry in the cache. In this case, the corresponding WWN to FC ID association for the oldest entry is lost.
- The switch connection behavior differs between N ports and NL ports:
  - N ports receive the same FC IDs if disconnected and reconnected to any port within the same switch (as long as it belongs to the same VSAN).
  - NL ports receive the same FC IDs only if connected back to the same port on the switch to which they were originally connected.

Persistent FC IDs

When persistent FC IDs are enabled, the following consequences apply:

- The currently *in use* FC IDs in the fcdomain are saved across reboots.
- The fcdomain automatically populates the database with dynamic entries that the switch has learned about after a device (host or disk) is plugged into a port interface.

Persistent FC ID Configuration

When the persistent FC ID feature is enabled, you can enter the persistent FC ID submode and add static or dynamic entries in the FC ID database. By default, all added entries are static. Persistent FC IDs are configured on a per-VSAN basis. Follow these requirements to manually configure a persistent FC ID:

- Ensure that the persistent FC ID feature is enabled in the required VSAN.
- Ensure that the required VSAN is an active VSAN—persistent FC IDs can only be configured on active VSANs.
- Verify that the domain part of the FC ID is the same as the runtime domain ID in the required VSAN. If the software detects a domain mismatch, the command is rejected.
- Verify that the port field of the FC ID is 0 (zero) when configuring an area.

Note FICON uses a different scheme for allocating FC IDs based in the front panel port number. This scheme takes precedence over FC ID persistence in FICON VSANs.

About Unique Area FC IDs for HBAs

Note Read this section only if the HBA port and the storage port are connected to the same switch.

Some HBA ports require a different area ID than storage ports when they are both connected to the same switch. For example, if the storage port FC ID is 0x6f7704, the area for this port is 77. In this case, the HBA port's area can be anything other than 77. The HBA port's FC ID must be manually configured to be different from the storage port's FC ID.

Switches in the Cisco MDS 9000 Family facilitate this requirement with the FC ID persistence feature. You can use this feature to preassign an FC ID with a different area to either the storage port or the HBA port.

Persistent FC ID Selective Purging

Persistent FC IDs can be purged selectively. Static entries and FC IDs currently in use cannot be deleted. Table 10-1 identifies the FC ID entries that are deleted or retained when persistent FC IDs are purged.

Table 10-1 Purged FC IDs

Persistent FC ID state	Persistent Usage State	Action
Static	In use	Not deleted
Static	Not in use	Not deleted
Dynamic	In use	Not deleted
Dynamic	Not in use	Deleted

Guidelines and Limitations

- When you change the configuration, be sure to save the running configuration. The next time you reboot the switch, the saved configuration is used. If you do not save the configuration, the previously saved startup configuration is used.
- Domain IDs and VSAN values used in all procedures are only provided as examples. Be sure to use IDs and values that apply to your configuration.

Default Settings

Table 10-2 lists the default settings for all fcdomain parameters.

Table 10-2 Default fcdomain Parameters

Parameters	Default
fcdomain feature	Enabled.
Configured domain ID	0 (zero).
Configured domain	Preferred.

Table 10-2 Default fcdomain Parameters (continued)

Parameters	Default
autoreconfigure option	Disabled.
contiguous-allocation option	Disabled.
Priority	128.
Allowed list	1 to 239.
Fabric name	20:01:00:05:30:00:28:df.
rcf-reject	Disabled.
Persistent FC ID	Enabled.
Allowed domain ID list configuration distribution	Disabled.

Configuring Fibre Channel Domains

This section describes the fcdomain feature and includes the following topics:

Configuring Domain Manager Turbo Mode

The Domain Manager turbo mode feature allows you to restart the Domain Manager with optimization. You have the option to select fast-restart or selective-restart mode for restarting the Domain Manager. You can leave the restart mode empty indicating that optimization is disabled.

Detailed Steps

To configure the Domain Manager turbo mode, follow these steps:

Step 1 Expand **Fabric > All VSANs** and then select **Domain Manager** in the Logical Domains pane for the fabric and VSAN for which you want to configure turbo mode.
You see the Running tab configuration of the domain in the Information pane.

Step 2 Click the **Configuration** tab.

Step 3 Set the Optimization drop-down menu to **fast-restart** or **selective-restart** for any switch in the fabric that you want to optimize. You can leave the Optimization field without any selection, indicating that the optimization is disabled.

Step 4 Click the **Apply Changes** icon to initiate this restart.

To configure the Domain Manager turbo mode using Device Manager, follow these steps:

Step 1 Expand **FC > Domain Manager** and then select the **Configuration** tab.

Note The Optimization field is not available in releases prior to NX-OS Release 4.2(1).

Step 2 Set the Optimization drop-down menu to **fast-restart** or **selective-restart** for any switch in the fabric that you want to optimize. You can leave the Optimization field without any selection, indicating that the optimization is disabled.

Step 3 Click **Apply** to initiate this restart.

Restarting a Domain

Detailed Steps

To restart the fabric disruptively or nondisruptively, follow these steps:

Step 1 Expand **Fabric > All VSANs** and then select **Domain Manager** in the Logical Domains pane for the fabric and VSAN that you want to restart.

Step 2 Click the **Configuration** tab.

Step 3 Set the Restart drop-down menu to **disruptive** or **nonDisruptive** for any switch in the fabric that you want to restart the fcdomain.

Step 4 Click the **Apply Changes** icon to initiate this fcdomain restart.

Configuring Switch Priority

Restrictions

- By default, the configured priority is 128. The valid range to set the priority is between 1 and 254. Priority 1 has the highest priority. Value 255 is accepted from other switches, but cannot be locally configured.

Detailed Steps

To configure the priority for the principal switch, follow these steps:

Step 1 Expand **Fabric > All VSANs** and then select **Domain Manager** in the Logical Domains pane for the fabric and VSAN that you want to set the principal switch priority for.

Step 2 Set Priority to a high value for the switch in the fabric that you want to be the principal switch.

Step 3 Click the **Apply Changes** icon to save these changes.

Enabling or Disabling fcdomains

Detailed Steps

To disable or reenable fcdomains in a single VSAN or a range of VSANs, follow these steps:

Step 1 Expand **Fabric > All VSANs** and then select **Domain Manager** in the Logical Domains pane for the fabric and VSAN that you want to disable fcdomain for.

You see the domain's running configuration in the Information pane.

Step 2 Click the **Configuration** tab and uncheck the **Enable** check box for each switch in the fabric that you want to disable fcdomain on.

Step 3 Click the **Apply Changes** icon to save these changes.

Configuring Fabric Names

Detailed Steps

To set the fabric name value for a disabled fcdomain, follow these steps:

Step 1 Expand **Fabric > All VSANs** and then select **Domain Manager** in the Logical Domains pane for the fabric and VSAN that you want to set the fabric name for.

You see the running configuration of the domain in the Information pane.

Step 2 Click the **Configuration** tab and set the fabric name for each switch in the fabric.

Step 3 Click the **Apply Changes** icon to save these changes.

Rejecting Incoming RCFs

Detailed Steps

To reject incoming RCF request frames, follow these steps:

Step 1 Expand **Switches > FC Interfaces** and then select **Physical** in the Physical Attributes pane**.**

You see the Fibre Channel configuration in the Information pane.

Step 2 Click the **Domain Mgr** tab.

Step 3 Check the **RcfReject** check box for each interface that you want to reject RCF request frames on.

Step 4 Click the **Apply Changes** icon to save these changes.

Enabling Autoreconfiguration

Detailed Steps

To enable automatic reconfiguration in a specific VSAN (or range of VSANs), follow these steps:

Step 1 Expand **Fabric > All VSANs** and then select **Domain Manager** in the Logical Domains pane for the fabric and VSAN that you want to enable automatic reconfiguration for.

You see the running configuration of the domain in the Information pane.

Step 2 Select the **Configuration** tab and check the **Auto Reconfigure** check box for each switch in the fabric that you want to automatically reconfigure.

Step 3 Click the **Apply Changes** icon to save these changes.

Configuring Domain IDs

Domain IDs uniquely identify a switch in a VSAN. A switch may have different domain IDs in different VSANs. The domain ID is part of the overall FC ID.

The configured domain ID can be preferred or static. By default, the configured domain ID is 0 (zero) and the configured type is preferred.

This section includes the following topics:

Specifying Static or Preferred Domain IDs

Restrictions

- Within a VSAN all switches should have the same domain ID type (either static or preferred). If a configuration is mixed (some switches with static domain types and others with preferred), then you may experience link isolation.

Detailed Steps

To specify a static or preferred domain ID, follow these steps:

Step 1 Expand **Fabric > All VSANs** and then select **Domain Manager** in the Logical Domains pane for the fabric and VSAN that you want to configure the domain ID for.

You see the running configuration of the domain in the Information pane.

Step 2 Enter a value for the Config DomainID and click **static** or **preferred** from the Config Type drop-down menu to set the domain ID for switches in the fabric.

Step 3 Click the **Apply Changes** icon to save these changes.

Configuring Allowed Domain ID Lists

Prerequisites

An allowed domain ID list must satisfy the following conditions:

- If this switch is a principal switch, all the currently assigned domain IDs must be in the allowed list.
- If this switch is a subordinate switch, the local runtime domain ID must be in the allowed list.

- The locally configured domain ID of the switch must be in the allowed list.
- The intersection of the assigned domain IDs with other already configured domain ID lists must not be empty.

If you configure an allowed list on one switch in the fabric, we recommend that you configure the same list in all other switches in the fabric to ensure consistency or use CFS to distribute the configuration.

Detailed Steps

To configure the allowed domain ID list, follow these steps:

Step 1 Expand **Fabric > All VSANs > Domain Manager** and then select **Allowed** in the Logical Domains pane for the fabric and VSAN for which you want to set the allowed domain ID list.

You see the CFS configuration in the Information pane.

Step 2 Set the Admin drop-down menu to **enable** and set the Global drop-down menu to **enable.**

Step 3 Click **Apply Changes** to enable CFS distribution for the allowed domain ID list.

Step 4 Select the **Allowed DomainIds** tab.

Step 5 Set the list to the allowed domain IDs list for this domain.

Step 6 Select the **CFS** tab and set Config Action to **commit**.

Step 7 Click the **Apply Changes** icon to commit this allowed domain ID list and distribute it throughout the VSAN.

Enabling Allowed Domain ID Distribution

CFS distribution of allowed domain ID lists is disabled by default. You must enable distribution on all switches to which you want to distribute the allowed domain ID lists.

Prerequisites

- All switches in the fabric must be running Cisco SAN-OS Release 3.0(1) or later to distribute the allowed domain ID list using CFS.

Detailed Steps

To enable (or disable) allowed domain ID list configuration distribution, follow these steps:

Step 1 Expand **Fabric > All VSANs > Domain Manager** and then select **Allowed** in the Logical Domains pane for the fabric and VSAN that you want to set the allowed domain ID list for.

You see the CFS configuration in the Information pane.

Step 2 Set the Admin drop-down menu to **enable** and the Global drop-down menu to **enable** to enable CFS distribution for the allowed domain ID list.

Step 3 Click the **Apply Changes** icon to enable CFS distribution for the allowed domain ID list.

Committing Changes

Detailed Steps

To commit pending domain configuration changes and release the lock, follow these steps:

Step 1 Expand **Fabric > All VSANs > Domain Manager** and then select **Allowed** in the Logical Domains pane for the fabric and VSAN that you want to set the allowed domain ID list for.

You see the CFS configuration in the Information pane.

Step 2 Set the Config Action drop-down menu to **commit**.

Step 3 Click the **Apply Changes** icon to commit the allowed domain ID list and distribute it throughout the VSAN.

Discarding Changes

At any time, you can discard the pending changes to the domain configuration and release the fabric lock. If you discard (abort) the pending changes, the configuration remains unaffected and the lock is released.

Detailed Steps

To discard pending domain configuration changes and release the lock, follow these steps:

Step 1 Expand **Fabric > All VSANs > Domain Manager** and then select **Allowed** in the Logical Domains pane for the fabric and VSAN that you want to set the allowed domain ID list for.

You see the CFS configuration in the Information pane.

Step 2 Set the Config Action drop-down menu to **abort**.

Step 3 Click the **Apply Changes** icon to discard any pending changes to the allowed domain ID list.

Enabling Contiguous Domain ID Assignments

Detailed Steps

To enable contiguous domains in a specific VSAN (or a range of VSANs), follow these steps:

Step 1 Expand **Fabric > All VSANs** and then select **Domain Manager** in the Logical Domains pane for the fabric and VSAN that you want to enable contiguous domains for.

You see the running configuration of the domain in the Information pane.

Step 2 Click the **Configuration** tab and check the **Contiguous Allocation** check box for each switch in the fabric that will have contiguous allocation.

Step 3 Click the **Apply Changes** icon to save these changes.

Configuring FC IDs

When an N or NL port logs into a Cisco MDS 9000 Family switch, it is assigned an FC ID.

This section includes the following topics:

Enabling the Persistent FC ID Feature

If you connect to the switch from an AIX or HP-UX host, be sure to enable the persistent FC ID feature in the VSAN that connects these hosts.

A persistent FC ID assigned to an F port can be moved across interfaces and can continue to maintain the same persistent FC ID.

Restrictions

- FC IDs are enabled by default. This change of default behavior from releases prior to Cisco MDS SAN-OS Release 2.0(1b) prevents FC IDs from being changed after a reboot. You can disable this option for each VSAN.
- Persistent FC IDs with loop-attached devices (FL ports) need to remain connected to the same port in which they were configured.
- Due to differences in Arbitrated Loop Physical Address (ALPA) support on devices, FC ID persistency for loop-attached devices is not guaranteed.

Detailed Steps

To enable the persistent FC ID feature, follow these steps:

Step 1 Expand **Fabric > All VSANs** and then select **Domain Manager** in the Logical Domains pane for the fabric and VSAN that you want to enable the Persistent FC ID feature for.

You see the running configuration of the domain in the Information pane.

Step 2 Select the **Persistent Setup** tab and check the **enable** check box for each switch in the fabric that will have persistent FC ID enabled.

Step 3 Click the **Apply Changes** icon to save these changes.

Configuring Persistent FC IDs

Detailed Steps

To configure persistent FC IDs, follow these steps:

Step 1 Expand **Fabric > All VSANs** and then select **Domain Manager** in the Logical Domains pane for the fabric and VSAN that you want to configure the Persistent FC ID list for.

You see the running configuration of the domain in the Information pane.

Step 2 Click the **Persistent FcIds** tab and click **Create Row**.

Step 3 Select the switch, WWN, and FC ID that you want to make persistent.

Step 4 Set the Mask radio button to **single** or **area**.

Step 5 Set the Assignment radio button to **static** or **dynamic**.

Step 6 Click the **Apply Changes** icon to save these changes.

Configuring Unique Area FC IDs for an HBA

Detailed Steps

To configure a different area ID for the HBA port, follow these steps:

Step 1 Expand **End Device** in the Physical Attributes pane and select the **FLOGI** tab in the Information pane to obtain the port WWN (Port Name field) of the HBA.

Note Both FC IDs in this setup have the same area 00 assignment.

Step 2 Expand **Switches > FC Interfaces** and then select **Physical** from the Physical Attributes pane.

Step 3 Set the Status Admin drop-down menu to **down** for the interface that the HBA is connected to.

This shuts down the HBA interface in the MDS switch.

Step 4 Expand **Fabric > All VSANs** and then select **Domain Manager.**

Step 5 Click the **Persistent Setup** tab in the Information pane to verify that the FC ID feature is enabled.

If this feature is disabled, continue with this procedure to enable the persistent FC ID.

If this feature is already enabled, skip to Step 7.

Step 6 Check the **Enable** check box to enable the persistent FC ID feature in the Cisco MDS switch.

Step 7 Select the **Persistent FcIds** tab and assign a new FC ID with a different area allocation in the FcId field. In this example, we replace 00 with ee.

Step 8 Click **Apply Changes** to save this new FC ID.

Step 9 Compare the FC ID values to verify the FC ID of the HBA.

Note Both FC IDs now have different area assignments.

Step 10 Expand **Switches > FC Interfaces** and then select **Physical** from the Physical Attributes pane. Set the Status Admin drop-down menu to **up** for the interface that the HBA is connected to. This enables the HBA interface in the MDS switch.

Purging Persistent FC IDs

Detailed Steps

To purge persistent FC IDs, follow these steps:

Step 1 Expand **Fabric > All VSANs > Domain Manager** in the Logical Domains pane for the fabric that you want to purge the Persistent FC IDs for. You see the running configuration of the domain in the Information pane.

Step 2 Click the **Persistent Setup** tab.

Step 3 Check the **Purge** check box for the switch that you want to purge persistent FC IDs on.

Step 4 Click the **Apply Changes** icon to save these changes.

Clearing a Fabric Lock

To release a fabric lock, follow these steps:

Step 1 Expand **Fabric > All VSANs > Domain Manager** and then select **AllowedId** in the Logical Domains pane for the fabric and VSAN for which you want the allowed domain ID list.

You see the CFS configuration in the Information pane.

Step 2 Set the Config Action drop-down menu to **clear**.

Step 3 Click the **Apply Changes** icon to clear the fabric lock.

Verifying FC Domain Configuration

To display the domain ID configuration information, perform the following tasks:

- Displaying Pending Changes, page 10-19
- Displaying Session Status, page 10-20

Displaying Pending Changes

To display the pending configuration changes, follow these steps:

Step 1 Expand **Fabric > All VSANs > Domain Manager > Allowed** in the Logical Domains pane for the fabric and VSAN that you want to set the allowed domain ID list for.

You see the CFS configuration in the Information pane.

Step 2 Set the Config View As drop-down menu to **pending**.

Step 3 Click the **Apply Changes** icon to clear the fabric lock.

Step 4 Click the **AllowedDomainIds** tab.

You see the pending configuration for the allowed domain IDs list.

Displaying Session Status

To display the status of the distribution session, follow these steps:

Step 1 Expand **Fabric > All VSANs > Domain Manager** and then select **Allowed** in the Logical Domains pane for the fabric and VSAN for which you want to set the allowed domain ID list.

Step 2 View the CFS configuration and session status in the Information pane.

Monitoring FC Domain

This section covers the following topic:

- Displaying fcdomain Statistics, page 10-20

Displaying fcdomain Statistics

DCNM-SAN collects statistics for fcdomain and displays them in the Information pane.

To display fcdomain statistics, follow these steps:

Step 1 Expand **Fabric > All VSANs** and then select **Domain Manager** in the Logical Domains pane for the fabric that you want to display statistics for.

You see the running configuration of the domain in the Information pane.

Step 2 Click the **Statistics** tab. You see the FC ID statistics in the Information pane.

Field Descriptions for FC Domain

This section describes the field descriptions for FC Domain.

IVR Domains

Filed	Description
Domain Id	The FC domain ID that will be used to represent the VSAN.

Feature History for Domain Parameters

Table 10-3 lists the release history for this feature. Only features that were introduced or modified in Release 3.x or a later release appear in the table.

Table 10-3 Feature History for Domain Parameters

Feature Name	Releases	Feature Information
Domain Manager Turbo Mode	4.2(1)	Added procedure to configure Domain Manager turbo mode.
CFS support for allowed domain ID lists	3.0(1)	Allows the allowed domain ID lists to be distributed in the fabric using the CFS infrastructure.