Send comments to nx5000-docfeedback@cisco.com

CHAPTER 7

Using Cisco Fabric Services

Cisco Nexus 5000 Series switches provide Cisco Fabric Services (CFS) capability, which simplifies provisioning by automatically distributing configuration information to all switches in the network.

Switch features can use the CFS infrastructure to distribute feature data or configuration data required by the feature.

This chapter contains the following sections:

Information About CFS

Some features in the Cisco Nexus 5000 Series switch require configuration synchronization with other switches in the network to function correctly. Synchronization through manual configuration at each switch in the network can be a tedious and error-prone process.

Cisco Fabric Services (CFS) provides a common infrastructure for automatic configuration synchronization in the network. It provides the transport function and a set of common services to the features. CFS has the ability to discover CFS capable switches in the network and discovering feature capabilities in all CFS capable switches.

Cisco Nexus 5000 Series switches support CFS message distribution over Fibre Channel, IPv4 or IPv6 networks. If the switch is provisioned with Fibre Channel ports, CFS over Fibre Channel is enabled by default. CFS over IP must be explicitly enabled.

CFS provides the following features:

- Peer-to-peer protocol with no client-server relationship at the CFS layer.
- CFS message distribution over Fibre Channel, IPv4 or IPv6 networks.
- Three modes of distribution.

Send comments to nx5000-docfeedback@cisco.com

  - Coordinated distributions: Only one distribution is allowed in the network at any given time.
  - Uncoordinated distributions: Multiple parallel distributions are allowed in the network except when a coordinated distribution is in progress.
  - Unrestricted uncoordinated distributions: Multiple parallel distributions are allowed in the network in the presence of an existing coordinated distribution. Unrestricted uncoordinated distributions are allowed to run in parallel with all other types of distributions.

The following features are supported for CFS distribution over IP:

- One scope of distribution over an IP network:
  - Physical scope: The distribution spans the entire IP network.

The following features are supported for CFS distribution over Fibre Channel SANs:

- Three scopes of distribution over SAN fabrics.
  - Logical scope: The distribution occurs within the scope of a VSAN.
  - Physical scope: The distribution spans the entire physical topology.
  - Over a selected set of VSANs: Some features require configuration distribution over some specific VSANs. These features can specify to CFS the set of VSANs over which to restrict the distribution.
- Supports a merge protocol that facilitates the merge of feature configuration during a fabric merge event (when two independent SAN fabrics merge).

CFS Distribution

The CFS distribution functionality is independent of the lower layer transport. Cisco Nexus 5000 Series switches support CFS distribution over IP and CFS distribution over Fibre Channel. Features that use CFS are unaware of the lower layer transport.

Additional details are provided in the following sections:

CFS Distribution Modes

CFS supports three distribution modes to accommodate different feature requirements. Only one mode is allowed at any given time. CFS distribution modes are described in the following sections:

Send comments to nx5000-docfeedback@cisco.com

Uncoordinated Distribution

Uncoordinated distributions are used to distribute information that is not expected to conflict with that from a peer. Parallel uncoordinated distributions are allowed for a feature.

Coordinated Distribution

Coordinated distributions allow only one feature distribution at a given time. CFS uses locks to enforce this. A coordinated distribution is not allowed to start if locks are taken for the feature anywhere in the network. A coordinated distribution consists of three stages:

1. A network lock is acquired.
2. The configuration is distributed and committed.
3. The network lock is released.

Coordinated distribution has two variants:

- CFS driven —The stages are executed by CFS in response to an feature request without intervention from the feature.
- Feature driven—The stages are under the complete control of the feature.

  Coordinated distributions are used to distribute information that can be manipulated and distributed from multiple switches, for example, the port security configuration.

Unrestricted Uncoordinated Distributions

Unrestricted uncoordinated distributions allow multiple parallel distributions in the network in the presence of an existing coordinated distribution. Unrestricted uncoordinated distributions are allowed to run in parallel with all other types of distributions.

Enabling/Disabling CFS Distribution on a Switch

If the switch is provisioned with Fibre Channel ports, CFS over Fibre Channel is enabled by default. CFS over IP must be explicitly enabled.

You can globally disable CFS on a switch to isolate the features using CFS from network-wide distributions while maintaining physical connectivity. When CFS is globally disabled on a switch, CFS operations are restricted to the switch.

To globally disable or enable CFS distribution on a switch using Fabric Manager, perform this task:

Step 1 Choose any CFS feature. For example, expand **Switches > Events** and then choose **CallHome** in the Physical Attributes pane.

The Information pane shows that feature, with a CFS tab.

Step 2 Click the **CFS** tab to display the CFS state for each switch in the network for that feature.

Step 3 Click a value in the **Global State** column. The value changes to a drop-down menu.

Step 4 From the drop-down menu, choose **disable** or **enable.**

Step 5 Repeat steps 3 and 4 for all switches that you want to disable or enable CFS.

Step 6 Set the Config Action column to **commit.**

Send comments to nx5000-docfeedback@cisco.com

Step 7 Click the **Apply Changes** icon to commit the configuration changes for that feature and distribute the changes through CFS.

To globally disable or enable CFS distribution on a switch using Device Manager, perform this task:

Step 1 Choose **Admin > CFS (Cisco Fabric Services)**.

You see the CFS dialog box with the CFS status for all features on that switch.

Step 2 Uncheck or check the **Globally Enabled** check box to disable or enable CFS distribution on this switch.

Step 3 Click **Apply** to disable CFS on this switch.

CFS Distribution over IP

CFS distribution over IP supports the following features:

- Physical distribution over an entirely IP network.
- Physical distribution over a hybrid Fibre Channel and IP network with the distribution reaching all switches that are reachable over either Fibre Channel or IP.

Note The switch attempts to distribute information over Fibre Channel first and then over the IP network if the first attempt over Fibre Channel fails. CFS does not send duplicate messages if distribution over both IP and Fibre Channel is enabled.

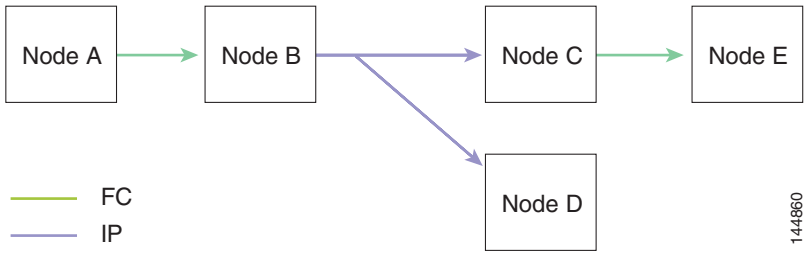
- Distribution over IP version 4 (IPv4) or IP version 6 (IPv6).

Note CFS cannot distribute over both IPv4 and IPv6 from the same switch.

- Keepalive mechanism to detect network topology changes using a configurable multicast address.
- Compatibility with Cisco MDS 9000 Family switches running release 2.x or later.

Figure 7-1 shows a network with both Fibre Channel and IP connections. Node A forwards an event to node B over Fibre Channel. Node B forwards the event node C and node D using unicast IP. Node C forwards the event to node E using Fibre Channel.

Figure 7-1 Network Example 1 with Fibre Channel and IP Connections



Send comments to nx5000-docfeedback@cisco.com

Figure 7-2 is the same as Figure 7-1 except that node C and node D are connected using Fibre Channel. All processes is the same in this example because node B has node C and node D the distribution list for IP. Node C does not forward to node D because node D is already in the distribution list from node B.

Figure 7-2 Network Example 2 with Fibre Channel and IP Connections

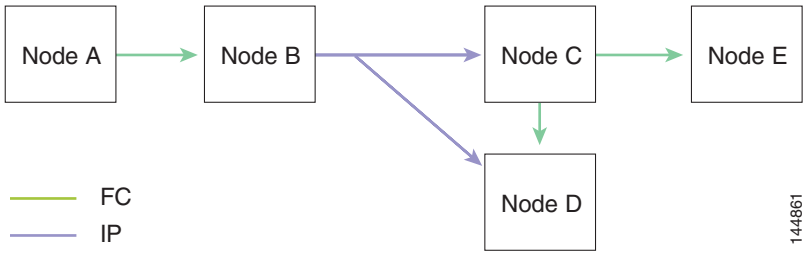
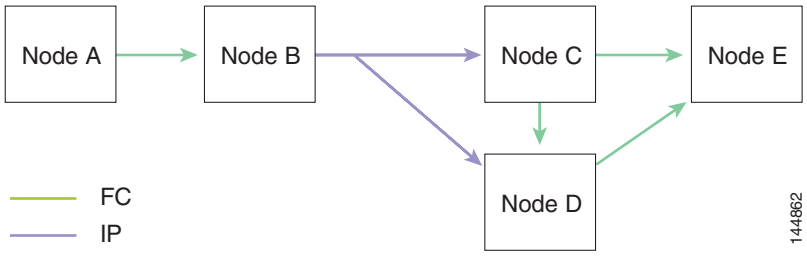


Figure 7-3 is the same as Figure 7-2 except that node D and node E are connected using IP. Both node C and node D forward the event to E because the node E is not in the distribution list from node B.

Figure 7-3 Network Example 3 with Fibre Channel and IP Connections



CFS Distribution over Fibre Channel

For FCS distribution over Fibre Channel, the CFS protocol layer resides on top of the FC2 layer. CFS uses the FC2 transport services to send information to other switches. CFS uses a proprietary SW_ILS (0x77434653) protocol for all CFS packets. CFS packets are sent to or from the switch domain controller addresses.

CFS Distribution Scopes

Different applications on the Cisco Nexus 5000 Series switches need to distribute the configuration at various levels. The following levels are available when using CFS distribution over Fibre Channel:

- VSAN level (logical scope)

  Applications that operate within the scope of a VSAN have the configuration distribution restricted to the VSAN. An example application is port security where the configuration database is applicable only within a VSAN.

Note Logical scope is not supported for FCS distribution over IP.

Send comments to nx5000-docfeedback@cisco.com

- Physical topology level (physical scope)

  Some applications (such as NTP) need to distribute the configuration to the entire physical topology.

- Between two selected switches

  Some applications operate only between selected switches in the network.

CFS Merge Support

CFS Merge is supported for CFS distribution over Fibre Channel.

An application keeps the configuration synchronized in a SAN fabric through CFS. Two such fabrics might merge as a result of an ISL coming up between them. These two fabrics could have two different sets of configuration information that need to be reconciled in the event of a merge. CFS provides notification each time an application peer comes online. If a fabric with M application peers merges with another fabric with N application peers, and if an application triggers a merge action on every notification, a link-up event results in M*N merges in the fabric.

CFS supports a protocol that reduces the number of merges required to one by handling the complexity of the merge at the CFS layer. This protocol runs per application per scope. The protocol involves selecting one switch in a fabric as the merge manager for that fabric. The other switches do not have a role in the merge process.

During a merge, the merge manager in the two fabrics exchange their configuration databases with each other. The application on one of them merges the information, decides if the merge is successful, and informs all switches in the combined fabric of the status of the merge.

In case of a successful merge, the merged database is distributed to all switches in the combined fabric and the entire new fabric remains in a consistent state. You can recover from a merge failure by starting a distribution from any of the switches in the new fabric. This distribution restores all peers in the fabric to the same configuration database.

CFS Support for Applications

The following topics describe the CFS capabilities that support applications:

CFS Application Requirements

All switches in the network must be CFS capable. Switches that are not CFS capable do not receive distributions and result in part of the network not receiving the intended distribution.

Send comments to nx5000-docfeedback@cisco.com

CFS has the following requirements:

- Implicit CFS usage—The first time you issue a CFS task for a CFS-enabled application, the configuration modification process begins and the application locks the network.
- Pending database—The pending database is a temporary buffer to hold uncommitted information. The uncommitted changes are not applied immediately to ensure that the database is synchronized with the database in the other switches in the network. When you commit the changes, the pending database overwrites the configuration database (also known as the active database or the effective database).
- CFS distribution enabled or disabled on a per-application basis—The default (enable or disable) for CFS distribution state differs between applications. If CFS distribution is disabled for an application, then that application does not distribute any configuration nor does it accept a distribution from other switches in the network.
- Explicit CFS commit—Most applications require an explicit commit operation to copy the changes in the temporary buffer to the application database, to distribute the new database to the network, and to release the network lock. The changes in the temporary buffer are not applied if you do not perform the commit operation.

Enabling CFS for an Application

All CFS-based applications provide an option to enable or disable the distribution capabilities.

Applications have the distribution enabled by default.

The application configuration is not distributed by CFS unless distribution is explicitly enabled for that application.

To enable CFS for a feature using Fabric Manager, perform this task:

Step 1 Choose a feature on which to enable CFS.

For example, expand **Switches > Events** and then choose **CallHome** in the Physical Attributes pane. The Information pane shows that feature with a CFS tab. Click the **CFS** tab to display the CFS state for each switch in the network for that feature.

Step 2 Decide on which switches to enable CFS. Set the Feature Admin column to either **enable** to enable CFS or **disable** to disable CFS.

Note Enable CFS for all switches in the network or VSAN for the feature that uses CFS.

Step 3 Right-click the row you changed to see the pop-up menu. Choose **Apply Changes** to apply the CFS configuration change. The CFS tab updates as the CFS changes take effect.

Fabric Manager retrieves the status of the CFS change and updates the Last Result column.

Send comments to nx5000-docfeedback@cisco.com

To enable CFS for a feature using Device Manager, perform this task:

Step 1 Choose **Admin > CFS (Cisco Fabric Services)**.

You see the CFS dialog box with the CFS status for all features on that switch.

Step 2 Decide which features need CFS. Set the Command column to either **enable** to enable CFS or **disable** to disable CFS.

Note Enable or disable CFS for all switches in the network or VSAN for the feature that uses CFS.

Step 3 Click **Pending Differences** to compare the configuration of this feature on this switch to other switches in the network or VSAN that have CFS enabled for this feature. Close the Show Pending Diff dialog box.

Step 4 Click **Apply** to apply the CFS configuration change.

Device Manager retrieves the status of the CFS change and updates the Last Command and Result columns.

Locking the Network

When you configure (first time configuration) a feature (or application) that uses the CFS infrastructure, that feature starts a CFS session and locks the network. When a network is locked, the switch software allows configuration changes to this feature only from the switch holding the lock. If you make configuration changes to the feature from another switch, the switch issues a message to inform the user about the locked status. The configuration changes are held in a pending database by that application.

If you start a CFS session that requires a network lock but forget to end the session, an administrator can clear the session. If you lock a network at any time, your user name is remembered across restarts and switchovers. If another user (on the same machine) tries to perform configuration tasks, that user's attempts are rejected.

Committing Changes

A commit operation saves the pending database for all application peers and releases the lock for all switches.

In general, the commit function does not start a session, only a lock function starts a session. However, an empty commit is allowed if configuration changes are not previously made. In this case, a commit operation results in a session that acquires locks and distributes the current database.

When you commit configuration changes to a feature using the CFS infrastructure, you receive a notification about one of the following responses:

- One or more external switches report a successful status—The application applies the changes locally and releases the network lock.
- None of the external switches report a successful state—The application considers this state a failure and does not apply the changes to any switch in the network. The network lock is not released.

You can commit changes for a specified feature by for that feature.

Send comments to nx5000-docfeedback@cisco.com

To commit changes using Fabric Manager for CFS-enabled features, perform this task:

Step 1 Choose the feature you want to enable CFS for.

For example, expand **Switches** expand **Events**, and then choose **CallHome** from the Physical Attributes pane.

The Information pane shows that feature with a CFS tab.

Step 2 Click the **CFS** tab to display the CFS state for each switch in the network for that feature.

Step 3 Right-click the value in the Config Action column for any switch and choose an option from the drop-down menu (Copy, Paste, Export to File, Print Table, Detach Table).

Step 4 Click the **Apply Changes** icon to commit the configuration changes for that feature and distribute the changes through CFS.

Fabric Manager retrieves the status of the CFS change and updates the Last Command and Last Result columns for the feature or VSAN.

To commit changes using Device Manager for CFS-enabled features, perform this task:

Step 1 Choose **Admin > CFS (Cisco Fabric Services)**.

You see the CFS dialog box with the CFS status for all features on that switch.

Step 2 For each applicable feature, set the Command column to **commit** to commit the configuration changes for that feature and distribute the changes through CFS, or set it to **abort** to discard the changes for that feature and release the network lock for CFS for that feature.

Step 3 Optionally, provide a **Type** or **VsanID** as the basis for the CFS distribution for CFS features that require this information.

Step 4 Click **Pending Differences** to check the configuration of this feature on this switch as compared to other switches in the network or VSAN that have CFS enabled for this feature.

Step 5 Click **Apply** to apply the CFS configuration change.

Device Manager retrieves the status of the CFS change and updates the Last Command and Result columns.

Caution If you do not commit the changes, they are not saved to the running configuration.

Discarding Changes

If you discard configuration changes, the application flushes the pending database and releases locks in the network. Both the abort and commit functions are only supported from the switch from which the network lock is acquired.

You can discard changes for a specified feature by setting the Command column value to **disable** for that feature then clicking **Apply**.

Send comments to nx5000-docfeedback@cisco.com

Saving the Configuration

Configuration changes that have not been applied yet (still in the pending database) are not shown in the running configuration. The configuration changes in the pending database overwrite the configuration in the effective database when you commit the changes.

Caution If you do not commit the changes, they are not saved to the running configuration.

The CISCO-CFS-MIB contains SNMP configuration information for any CFS-related functions. Refer to the *Cisco Cisco Nexus 5000 Series MIB Quick Reference* for more information on this MIB.

Clearing a Locked Session

You can clear locks held by an application from any switch in the network to recover from situations where locks are acquired and not released. This function requires Admin permissions.

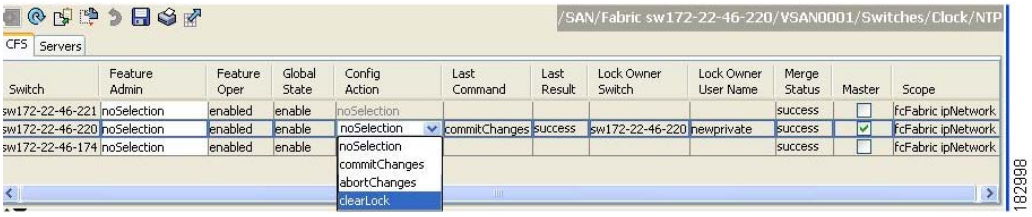
To clear locks using Fabric Manager, perform this task:

Step 1 Click the **CFS** tab.

Step 2 Choose **clearLock** from the Config Action drop-down list for each switch that you want to clear the lock (see Figure 7-4).

Step 3 Click the **Apply Changes** icon to save the change.

Figure 7-4 Clearing Locks



Caution Exercise caution when using this function to clear locks in the network. Any pending configurations in any switch in the network is flushed and lost.

CFS Regions

This section contains the following topics:

Send comments to nx5000-docfeedback@cisco.com

About CFS Regions

A CFS region is a user-defined subset of switches for a given feature or application in its physical distribution scope. When a network spans a vast geography, you may need to localize or restrict the distribution of certain profiles among a set of switches based on their physical proximity. CFS regions allow you to create multiple islands of distribution within the network for a given CFS feature or application. CFS regions are designed to restrict the distribution of a feature's configuration to a specific set or grouping of switches in a network.

Note You can only configure a CFS region based on physical switches. You cannot configure a CFS region in a VSAN.

Example Scenario

The Call Home application triggers alerts to network administrators when a situation arises or something abnormal occurs. When the network covers many geographies, and there are multiple network administrators who are each responsible for a subset of switches in the network, the Call Home application sends alerts to all network administrators regardless of their location. For the Call Home application to send message alerts selectively to network administrators, the physical scope of the application has to be fine tuned or narrowed down, which is achieved by implementing CFS regions.

CFS regions are identified by numbers ranging from 0 through 200. Region 0 is reserved as the default region, and contains every switch in the network. You can configure regions from 1 through 200. The default region maintains backward compatibility.

If the feature is moved, that is, assigned to a new region, its scope is restricted to that region; it ignores all other regions for distribution or merging purposes. The assignment of the region to a feature has precedence in distribution over its initial physical scope.

You can configure a CFS region to distribute configurations for multiple features. However, on a given switch, you can configure only one CFS region at a time to distribute the configuration for a given feature. Once you assign a feature to a CFS region, its configuration cannot be distributed within another CFS region.

Managing CFS Regions Using Fabric Manager

This section describes how to use Fabric Manager for managing CFS regions. Fabric Manager provides a comprehensive view of all the switches, regions, and the features associated with each region in the topology. To complete the following tasks, use the tables under the All Regions and Feature by Region tabs:

- Creating CFS Regions, page 7-12
- Assigning Features to CFS Regions, page 7-12
- Moving a Feature to a Different Region, page 7-13

Send comments to nx5000-docfeedback@cisco.com

- Removing a Feature from a Region, page 7-14

Creating CFS Regions

To create a CFS region using Fabric Manager, perform this task:

Step 1 In the Physical Attributes pane, expand **Switches** and then choose **CFS**.

The information pane displays the Global, IP Multicast, Feature by Region, and All Regions tabs.

Step 2 Click the **All Regions** tab.

The tab displays a list of Switches and RegionIds.

Step 3 Click the **Create Row** button on the toolbar.

Figure 7-5 shows the Create a Region dialog box.

Figure 7-5 Create a Region Dialog Box

Step 4 Choose the switch from the drop-down list and choose a RegionId from the range.

Step 5 Click **Create**.

Upon successful creation of the region, Success is displayed at the bottom of the dialog box.

Assigning Features to CFS Regions

To assign a feature to a region using Fabric Manager, perform this task:

Step 1 In the Physical Attributes pane, expand **Switches** and then choose **CFS**.

The information pane displays the Global, IP Multicast, Feature by Region, and All Regions tabs.

Step 2 Click the **Feature by Region** tab.

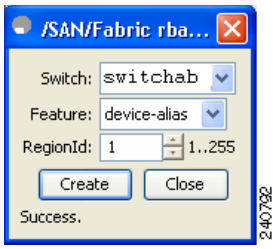
This tab lists all the switches along with their corresponding Feature and RegionId.

Step 3 Click the **Create Row** button on the toolbar.

Figure 7-6 shows the Assign a Feature dialog box.

Send comments to nx5000-docfeedback@cisco.com

Figure 7-6 Assign a Feature Dialog Box



Step 4 Choose a switch from the drop-down box.

The features running on the selected switch are listed in the Feature drop-down box.

Step 5 Choose a feature on that switch to associate a region.

Step 6 Choose the region number from the list to associate a RegionId with the selected feature.

Step 7 Click **Create** to complete assignment of a switch feature to the region.

Upon successful assignment of feature, Success is displayed at the bottom of the dialog box.

When a feature is assigned to a new region using the Feature by Region tab, a new row with the new region is created automatically in the table under the All Regions tab. Alternatively, you can create a region using the All Regions tab.

Note In the Feature by Region tab, when you try to reassign a feature on a switch to another region by clicking **Create Row**, an operation failed message is shown. The error message states that an entry already exists. However, moving a feature to a different region is a different task and it is described in the next section.

Moving a Feature to a Different Region

Before moving a feature to a new region, create the new region in the All Regions tab. That is, a new row has to be added in the All Regions tab with the new Region ID.

To move a feature to a different region using Fabric Manager, perform this task:

Step 1 In the Physical Attributes pane, expand **Switches** and then choose **CFS**.

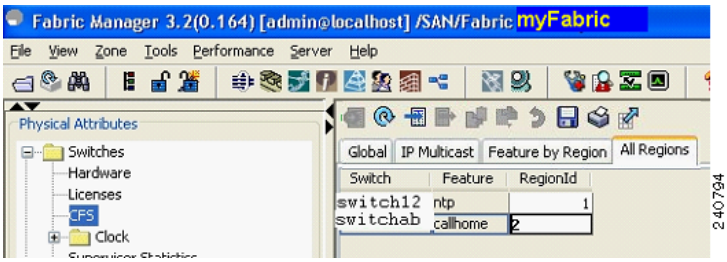
The information pane displays the Global, IP Multicast, Feature by Region, and All Regions tabs.

Step 2 Click the **Feature by Region** tab.

Figure 7-7 shows the Feature by Region tab, which lists all the switches along with their feature and region details.

Send comments to nx5000-docfeedback@cisco.com

Figure 7-7 Feature by Region Tab



Step 3 Double-click the RegionId cell in the required row.

The cursor blinks in the cell prompting a change in the value.

Step 4 Change the RegionId value to the required region.

Step 5 Click the **Apply Changes** button on the tool bar to commit the change.

Removing a Feature from a Region

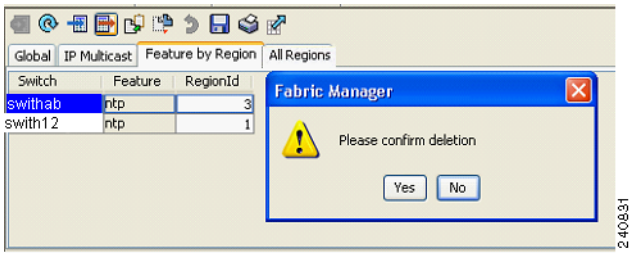
To remove a feature from a region using Fabric Manager, perform this task:

Step 1 Click the **Feature by Region** tab and click the required row.

Step 2 Click the **Delete Row** button on the toolbar.

Figure 7-8 shows a confirmation dialog box.

Figure 7-8 Removing a Feature from a Region



Step 3 Click **Yes** to confirm row deletion from the table in view.

Deleting CFS Regions

To delete an entire region, perform this task:

Step 1 Click the **All Regions** tab and click the required row.

Step 2 Click **Delete Row**.

This action removes all entries pertaining to that switch and region in the table under Feature by Region tab.

Send comments to nx5000-docfeedback@cisco.com

Figure 7-9 shows a confirmation dialog box.

Figure 7-9 Deleting CFS Regions

Step 3 Click **Yes** to confirm deletion of the region.

Note CFS cannot distribute over both IPv4 and IPv6 from the same switch.

Displaying CFS Distribution Information

To display the status of CFS distribution on the switch using Device Manager, perform this task:

Step 1 Choose **Admin > CFS (Cisco Fabric Services)**.

You see the CFS dialog box. This dialog box displays the distribution status of each feature using CFS, which currently registered applications are using CFS, and the result of the last successful merge attempt.

Step 2 Select a row and click **Details** to view more information about the feature.

CFS Example Using Fabric Manager

This procedure is an example of what you see when you use Fabric Manager to configure a feature that uses CFS:

Step 1 Select the CFS-capable feature that you want to configure.

For example, expand a **VSAN** and then choose **Port Security** in the Logical Domains pane.

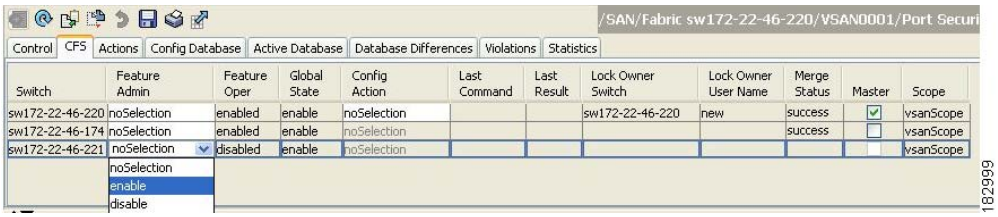
You see the port security configuration for that VSAN in the Information pane.

Step 2 Click the **CFS** tab.

You see the CFS configuration and status for each switch (see Figure 7-10).

Send comments to nx5000-docfeedback@cisco.com

Figure 7-10 CFS Configuration



Step 3 Choose **enable** for each switch from the Feature Admin drop-down list.

Step 4 Repeat step 3 for all switches in the network.

Note A warning displays if you do not enable CFS for all switches in the network for this feature.

Step 5 Check the **Master** check box for the switch to act as the merge master for this feature.

Step 6 Choose **commit Changes** from the Config Action drop-down list for each switch that you enabled for CFS.

Step 7 Click the **Servers** tab in the Information pane.

You see the configuration for this feature based on the master switch (see Figure 7-11).

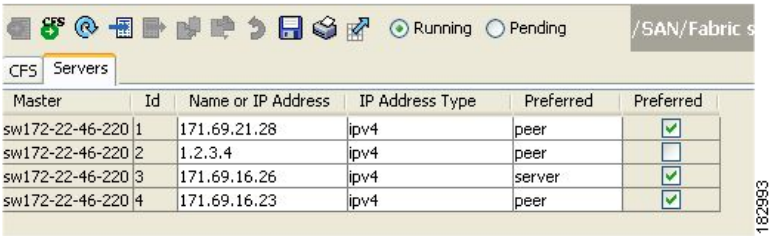
Step 8 Modify the feature configuration. For example, right-click the name in the Master column and choose **Create Row** to create a server for NTP.

a. Enter the ID and the Name or IP Address of the NTP server.

b. Set the **Mode** radio button and optionally check the **Preferred** check box.

c. Click **Create** to add the server.

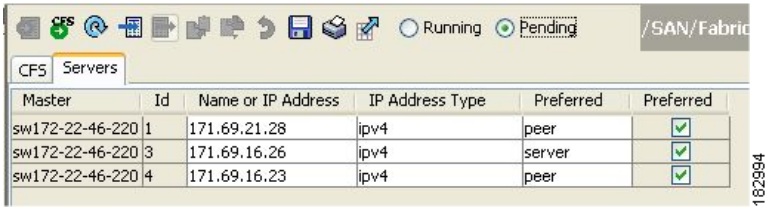
Figure 7-11 Servers Tab



Step 9 Click the **Delete Row** icon to delete a row.

If you make any changes, the status automatically changes to Pending (see Figure 7-12).

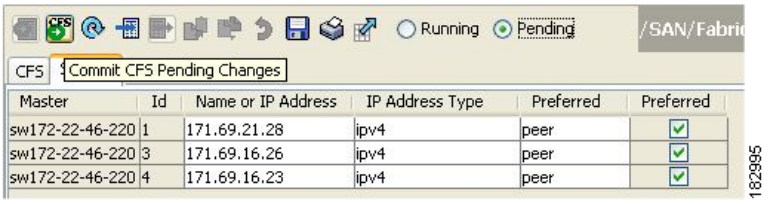
Figure 7-12 Status Change to Pending



Send comments to nx5000-docfeedback@cisco.com

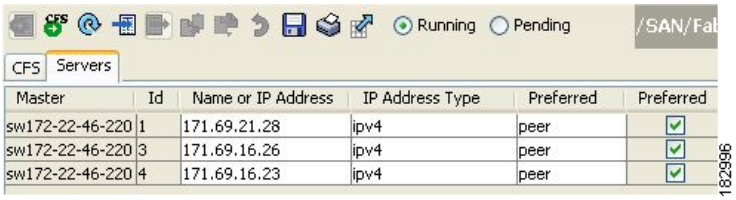
Step 10 Click the **Commit CFS Pending Changes** icon to save the changes (see Figure 7-13).

Figure 7-13 Commit CFS Pending Changes



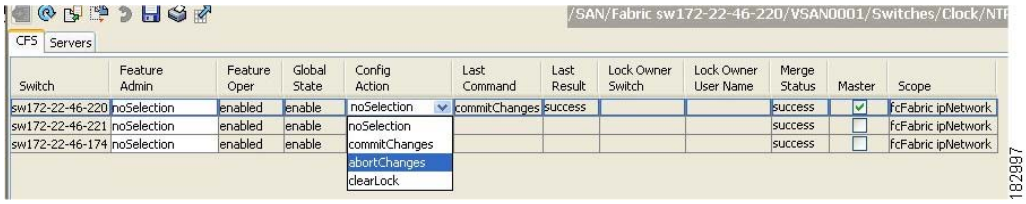
Step 11 The status changes to Running (see Figure 7-14).

Figure 7-14 Status Change to Running



Step 12 Choose **abortChanges** from the Config Action drop-down list for each switch that you enabled for CFS (see Figure 7-15).

Figure 7-15 Commit Configuration Changes



Note Fabric Manager does not change the status to pending if **enable** is selected, because the pending status does not apply until the first actual change is made.

Step 13 Click the **Apply Changes** icon to commit the configuration changes for that feature and distribute the changes through CFS.

Note When using CFS with features such as device alias, you must choose **commit** at the end of each configuration. If the session is locked, you must exit the feature by selecting **abort**.

Send comments to nx5000-docfeedback@cisco.com

To configure the master or seed switch for distribution for each feature using Fabric Manager, perform this task:

Step 1 Choose the feature that needs a merge master for CFS.

For example, expand **Switches > Events**, and then choose **CallHome** from the Physical Attributes pane.

The Information pane shows that feature including a CFS tab.

Step 2 Click the **CFS** tab to display the CFS state for each switch in the network for that feature.

Step 3 Check the **Master column** check box for the switch to act as the merge master for this feature.

Step 4 Click the **Apply Changes** icon to select this switch as master for future CFS distributions.

CFS Example Using Device Manager

This procedure is an example of what you see when you use Device Manager to configure a feature that uses CFS. For specific procedures for features that use CFS, refer to that feature's documentation.

To configure a feature that uses CFS using Device Manager, perform this task:

Step 1 Open the dialog box for any CFS-capable feature.

Device Manager checks to see whether CFS is enabled. It also checks to see if there is a lock on the feature by checking for at least one entry in the Owner table. If CFS is enabled and there is a lock, Device Manager sets the status to pending for that feature. You see a dialog box displaying the lock information.

Step 2 Click **Continue** or **Cancel** when prompted. If you continue, Device Manager remembers the CFS status.

Step 3 Choose **Admin > CFS (Cisco Fabric Services)** to view the user name of the CFS lock holder.

Step 4 Click the locked feature and click **Details**.

Step 5 Click the **Owners** tab and look in the UserName column.

Note Device Manager does not monitor the status of the feature across the network until you click **Refresh**. If a user on another CFS-enabled switch attempts to configure the same feature, they do not see the pending status. However, their configuration changes are rejected by your switch.

Step 6 If CFS is enabled and there is no lock, Device Manager sets the status to running for that feature.

You then see a dialog box for the feature. As soon as you perform a creation, deletion, or modification, Device Manager changes the status to pending and displays the updated information from the pending database.

Step 7 View the CFS table for a feature. Device Manager only changes the status to running when **commit**, **clear,** or **abort** is selected and applied. Device Manager will not change the status to pending if **enable** is selected, because the pending status does not apply until the first actual change is made.

The Last Command and Result fields are blank if the last command is **noOp**.

Send comments to nx5000-docfeedback@cisco.com

Note When using CFS with features like device alias, you must choose **commit** at the end of each configuration. If the session is locked, you must exit the feature by selecting **abort**.

Default Settings

Table 7-1 lists the default settings for CFS configurations.

Table 7-1 Default CFS Parameters

Parameters	Default
CFS distribution on the switch	Enabled.
Database changes	Implicitly enabled with the first configuration change.
Application distribution	Differs based on application.
Commit	Explicit configuration is required.
CFS over IP	Disabled.
IPv4 multicast address	239.255.70.83.
IPv6 multicast address	ff15::efff:4653.

Send comments to nx5000-docfeedback@cisco.com