CHAPTER 15

Zone Configuration

Zoning enables you to set up access control between storage devices or user groups. If you have administrator privileges in your fabric, you can create zones to increase network security and to prevent data loss or corruption. Zoning is enforced by examining the source-destination ID field.

As of Cisco MDS SAN-OS Release 2.x, advanced zoning capabilities specified in the FC-GS-4 and FC-SW-3 standards are provided by the Cisco SAN-OS software. You have the option of using the existing basic zoning capabilities or using the advanced, standards-compliant zoning capabilities.

This chapter includes the following sections:

Zoning Features

For Fabric Manager Release 2.0(1b), Fabric Manager has added the following to its zoning capabilities:

- Aliases are treated as groups.
- You can have many different types of aliases.
- You can rename zone sets, zones, and aliases.
- You can backup and restore zone database.
- There are enhanced zoning capabilities.

A zone set consists of one or more zones. A zone can be a member of more than one zone set and consists of multiple zone members. Members in a zone can access each other; members in different zones cannot access each other. Devices can belong to more than one zone.

A zone set can be activated or deactivated as a single entity across all switches in the fabric. Only one zone set can be activated at any time. If zoning is not activated, all devices are members of the default zone. If zoning is activated, any device that is not in an active zone (a zone that is part of an active zone set) is a member of the default zone.

Zoning can be administered from any switch in the fabric. When you activate a zone (from any switch), all switches in the fabric receive the active zone set. Additionally, full zone sets are distributed to all switches in the fabric, if this feature is enabled in the source switch.

If a new switch is added to an existing fabric, zone sets are acquired by the new switch.

Zone changes can be configured nondisruptively. New zones and zone sets can be activated without interrupting traffic on unaffected ports or devices.

Default zone membership includes all ports or WWNs that do not have a specific membership association. Access between default zone members is controlled by the default zone policy.

Zone Implementation

All switches running Cisco MDS SAN-OS automatically support the following basic zone features (no additional configuration is required):

- Zones are contained in a VSAN.
- Only active zone sets are distributed.
- Unzoned devices cannot access each other.
- A zone or zone set with the same name can exist in each VSAN.
- Each VSAN has a full database and an active database.
- Active zone sets cannot be changed, without activating a full zone database.
- Active zone sets are preserved across switch reboots.
- Changes to the full database must be explicitly saved.
- Zone reactivation (a zone set is active and you activate another zone set) does not disrupt existing traffic.

If required, you can additionally configure the following zone features:

- Propagate full zone sets to all switches on a per VSAN basis.
- Change the default policy for unzoned members.
- Interoperate with other vendors by configuring a VSAN in the interop mode. You can also configure one VSAN in the interop mode and another VSAN in the basic mode in the same switch without disrupting each other
- Bring E ports out of isolation.

Zone Configuration

A zone can be configured using one of the following types in Cisco MDS SAN-OS to assign members:

- pWWN—The WWN of the N or NL port in hex format (for example, 10:00:00:23:45:67:89:ab).

Caution You must only configure pWWN-type zoning on an MDS switch running Cisco SAN-OS if there is a Cisco MDS 9020 switch running FabricWare in the same fabric to avoid ISL isolation. It is important to remove all non-pWWN-type zone entries prior to merging fabrics.

- Fabric port WWN—The WWN of the fabric port name in hex format (for example, 10:00:00:23:45:67:89:ab).
- FC ID—The N port ID in 0xhhhhhh format (for example, 0xce00d1).
- FC alias—The alias name is in alphabetic characters (for example, Payroll) and denotes a port ID or WWN. The alias can also include multiple members.
- Domain ID—The domain ID is an integer from 1 to 239. A mandatory port number of a non-Cisco switch is required to complete this membership configuration.
- IP address—The IP address of an attached device in 32 bytes in dotted decimal format along with an optional subnet mask. If a mask is specified, any device within the subnet becomes a member of the specified zone.
- Interface—Interface-based zoning is similar to port-based zoning because the switch interface is used to configure the zone. You can specify a switch interface as a zone member for both local and remote switches. To specify a remote switch, enter the remote switch WWN (sWWN) or the domain ID in the particular VSAN.

A zone can be configured in Cisco FabricWare by assigning members based on the following:

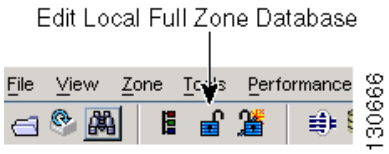
- pWWN—The WWN of the N or NL port in hex format (for example, 10:00:00:23:45:67:89:ab).
- FC alias—The alias name is in alphabetic characters (for example, Payroll) and denotes a port ID or WWN. The alias can also include multiple members.

Using the Zone Configuration Tool

To configure zones, read-only zones, and IVR zones using the Zone configuration tool, follow these steps:

Step 1 From the Fabric Manager toolbar, click the **Zone** icon as shown in Figure 15-1.

Figure 15-1 Zone Icon



Step 2 Select the VSAN where you want to configure zone sets, zones, or add members to a zone.

Step 3 Click **Zoneset** and click the **Create Row** icon to make a new zone set.

Step 4 Click **Zones** and click the **Create Row** icon to make a new zone.

a. Optionally, check **Read Only** check box if you want the zone to permit reads and deny writes.

b. Optionally, check the **Permit QoS traffic with Priority** check box and set the QoS priority from the drop-down menu.

c. Optionally, check the **Restrict Broadcast frames to Zone Members** check box.

Step 5 Click **Aliases** and click the **Create Row** icon to create a new device alias.

Step 6 Click a zone and click the **Create Row** icon to create a new zone member.

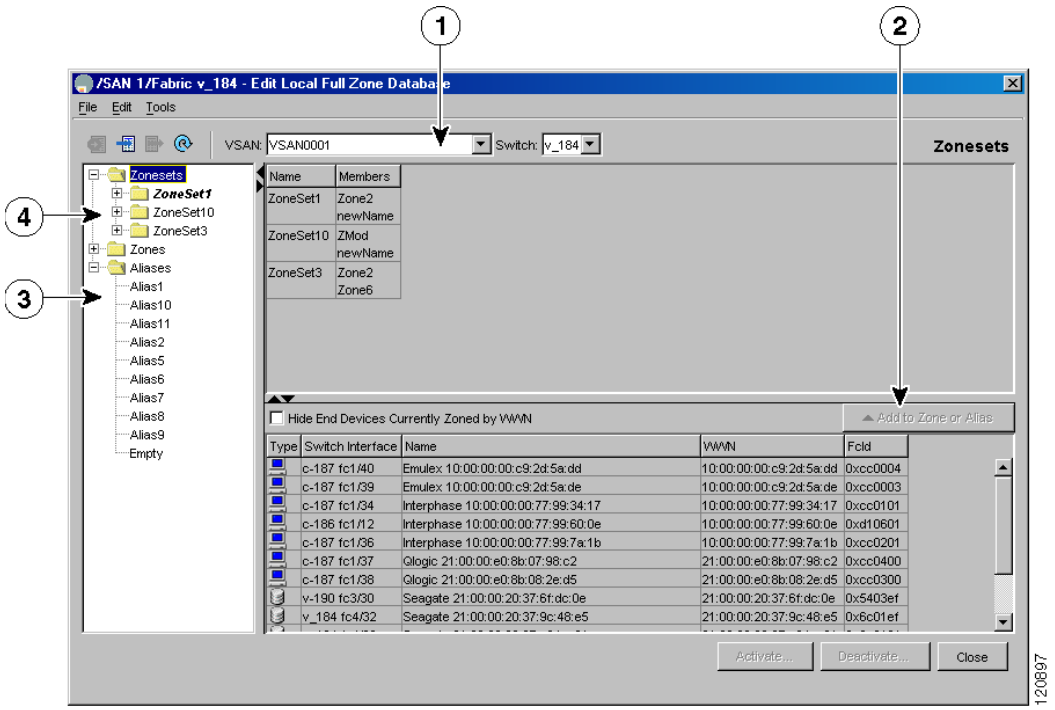
a. Select the zone member type (for example, FC ID, pWWN) at set the appropriate name or ID.

b. Click **Add** to add the zone member to the zone or click **Cancel** to close the dialog box without adding a new zone member.

Edit Full Zone Database Overview

For version 2.0, there are interface changes to the Edit Full Zone Database screen, which is shown in Figure 15-2.

Figure 15-2 Edit Full Zone Database Screen



1	You can display information by VSAN by using the pull-down menu without having to get out of the screen, selecting a VSAN, and re-entering.	**3**	You can add zoning characteristics based on alias in different folders.
2	You can use the **Add to zone or alias** button to move devices up or down by alias or by zone.	**4**	You can triple-click to rename zone sets, zones, or aliases in the tree.

Zone Database Information

If required, you can clear configured information stored in the zone server database.

Note Clearing a zone set only erases the full zone database, not the active zone database.

Configuring a Zone

Note Interface-based zoning only works with Cisco MDS 9000 Family switches. Interface-based zoning does not work if **interop** mode is configured in that VSAN.

Tip If you do not provide an sWWN, the software automatically uses the local sWWN.

Zones are configured within VSANs, but you can configure zones without configuring any VSANs by configuring them within the default VSAN. The Logical tab displays the VSANs configured in the currently discovered fabric. Note that zone information must always be identical for all the switches in the network fabric.

To create zones, follow these steps:

Step 1 From Fabric Manager, choose **Zone > Edit Local Full Zone Database** from the Zone menu or right-click a VSAN folder in the Logical tab and choose **Edit Local Full Zone Database** from the pop-up menu.

If you chose **Zone > Edit Local Full Zone Database**, or the **All VSANs** folder is selected in the Logical Attributes pane, then you see the Select VSAN dialog box. Select the VSAN and click **OK**.

You see the Edit Local Full Zone Database dialog box for the VSAN you selected.

Step 2 Right-click the **Zone** folder in the Edit Local Full Zone Database dialog box for that VSAN and select **Insert** to add a zone.

You can specify that the zone be a read-only zone by checking the **Read Only** check box. (See the "About Read-Only Zones" section on page 15-23.)

Viewing Zone Statistics

To monitor zone statistics from the Zone Server, choose **VSAN**xxx **> Domain Manager** from the Fabric Manager menu tree. The zone information is displayed in the Information pane. Click the **Statistics** tab to see the statistics information for the switches in the zone.

Adding Zone Members

Once you have created a zone, you can add members to the zone. You can add members using multiple port identification types. See the "Zone Configuration" section on page 15-2.

To add a member to a zone, follow these steps:

Step 1 Click the **Zones** folder from the Logical Attributes pane. Right-click the folder for the zone to which you want to add members, and then choose **Insert** from the pop-up menu.

You see the Add Member to Zone dialog box.

Step 2 Click the check box to the left of the port identification type you want to add.

Step 3 Select one of the port identifier options in the dialog box and click **Add** to add it to the zone.

You see the member in the zone server database in the lower frame.

Step 4 Repeat these steps to add other members to the zone.

Note When configuring a zone member, you can specify that a single LUN has multiple IDs depending on the operating system. You can select from six different operating systems.

Displaying Zone Membership Information

To display zone membership information for members assigned to zones, follow these steps:

Step 1 From Fabric Manager, choose **Zone > Edit Local Full Zone Database** from the Zone menu, or right-click a VSAN folder in the Logical tab and choose **Edit Local Full Zone Database** from the pop-up menu.

If you chose **Zone > Edit Local Full Zone Database** , then you see the Select VSAN dialog box . Select the VSAN and click **OK**.

You see the Edit Local Full Zone Database window for the VSAN you selected.

Step 2 Click the **Zones** folder. The right pane lists the members for each zone.

Note The default zone members are explicitly listed only when the default zone policy is configured as permit. When the default zone policy is configured as deny, the members of this zone are not shown. See the "Viewing Zone Statistics" section on page 15-5.

Alias Configuration

You can assign an alias name and configure an alias member using either the FC ID, fabric port WWN (fWWN), pWWN, domain ID and port number, interface ID, IP address, or symbolic node name values.

Tip Cisco MDS SAN-OS Release 1.3(4) or later supports a maximum of 2048 aliases per VSAN.

Tip Cisco FabricWare Release 2.1(2) or later supports a maximum of 2500 aliases.

Creating Zones with Aliases

To create a zone with aliases, follow these steps:

Step 1 Select **Edit Local Full Zone Database.**.. from the Zone menu.

You see the Select VSAN dialog box.

Step 2 Select the VSAN on which you want to create the zone and click **OK**.

You see the zone information for that VSAN.

Step 3 Right-click the **Aliases** folder in the left window pane and select **Insert**.

You see the Create Alias dialog box.

Step 4 Enter the alias name and click **OK** to create the alias.

Step 5 Right-click the newly created alias and select **Insert**.You can add/associate multiple pWWNs and fWWNs to the same alias name. The pWWNs do not have to be attached to the fabric you are currently managing.

Step 6 Click **Add** to add this entity to this alias.

Step 7 Right-click the **Zones** folder in the left pane and select **Insert**.

Step 8 Name the zone as desired and click **OK**.

Step 9 Select the newly created zone from the right pane and select **Insert**. You see the Add Member Dialog box.

Step 10 Select the **Alias** radio button. Type the name of the alias you want to associate with this zone or select the **...** button to see a list of aliases to select from. Click **OK**.

Step 11 Add the zone to a zone set and activate it accordingly.

Viewing Aliases

Aliases are assigned per port.

To view zone aliases, follow these steps:

Step 1 From Fabric Manager, choose **Zone > Edit Local Full Zone Database** from the Zone menu, or right-click a VSAN folder in the Logical tab and choose **Edit Local Full Zone Database** from the pop-up menu.

If you chose **Zone > Edit Local Full Zone Database** , then you see the Select VSAN dialog box . Select the VSAN and click **OK**.

You see the Edit Local Full Zone Database window for the VSAN you selected.

Step 2 Click the **Zones** folder for the zone you are interested in. The aliases for that zone are listed in the right pane.

Converting Zone members to pWWN-based Members

Fabric Manager Release 2.1(2) introduced the ability to convert zone and alias members from switch port or FC ID based memberhip to pWWN-based membership. You can use this feature to convert to pWWN so that your zone configuration does not change if a card or switch is changed in your fabric.

To convert switch port and FC ID members to pWWN members using Fabric Manager, Follow these steps:

Step 1 Select **Edit Local Full Zone Database...** from the Zone menu.

You see the Select VSAN dialog box.

Step 2 Select the VSAN on which you want to convert the zone membership and click **OK**. You see the zone information for that VSAN.

Step 3 Right-click the **any** folder in the left window pane and select **Convert Switch Port/FCID members to pWWN...**. You see the conversion dialog box, listing all members that will be converted.

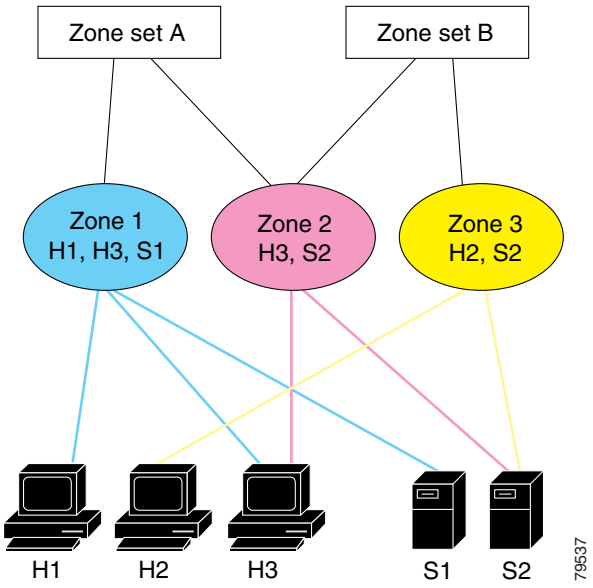
Step 4 Verify the changes and click **Continue Conversion**.

Step 5 Click Yes in the confirmation dialog box to convert that member to pWWN based membership.

Zone Set Creation

In Figure 15-3, two separate sets are created, each with its own membership hierarchy and zone members.

Figure 15-3 Hierarchy of Zone Sets, Zones, and Zone Members



Zones provide a mechanism for specifying access control, while zone sets are a grouping of zones to enforce access control in the fabric. Either zone set A or zone set B can be activated (but not together).

Note You can specify multiple zone members on multiple lines at the switch prompt.

Tip Zone sets are configured with the names of the member zones. If the zone set is in a configured VSAN, you must also specify the VSAN.

Active and Full Zone Set Considerations

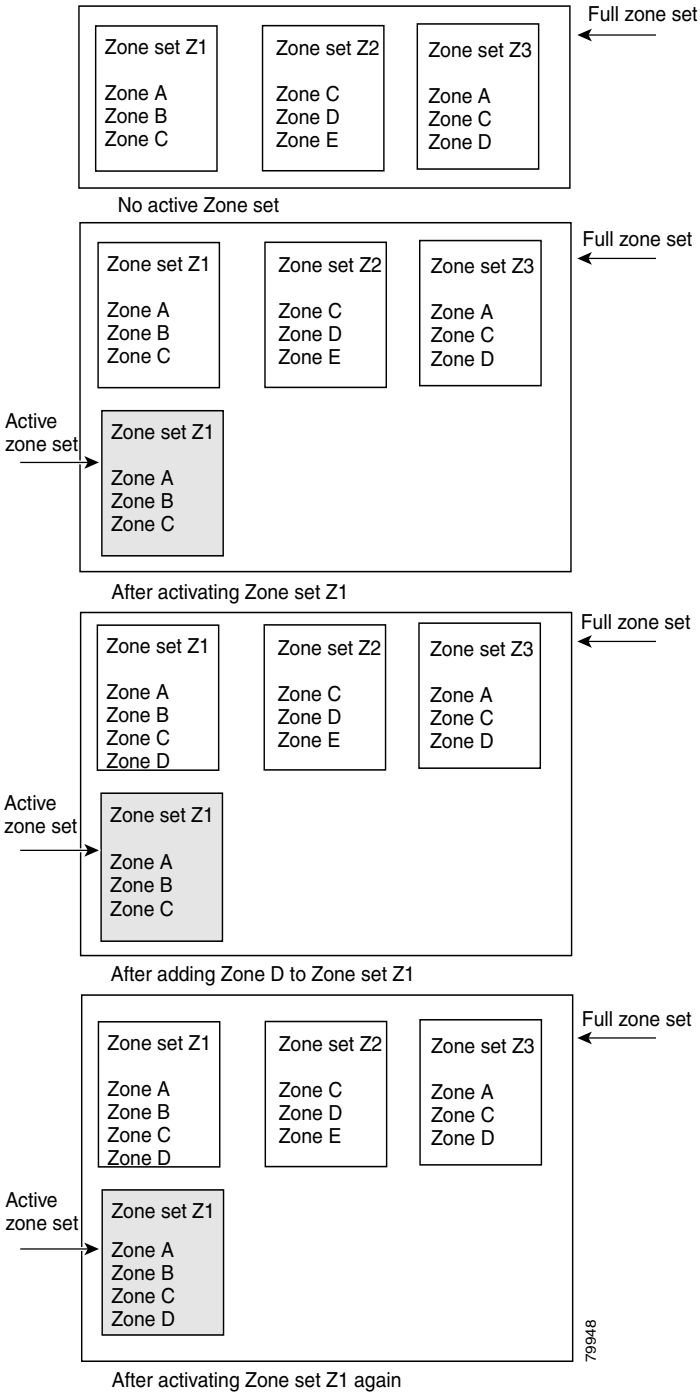
Before configuring a zone set, consider the following guidelines:

- Each VSAN can have multiple zone sets but only one zone set can be active at any given time.
- When you create a zone set, that zone set becomes a part of the full zone set.
- When you activate a zone set, a copy of the zone set from the full zone set is used to enforce zoning, and is called the active zone set. An active zone set cannot be modified. A zone that is part of an active zone set is called an active zone.
- The administrator can modify the full zone set even if a zone set with the same name is active.
- When the activation is done, the active zone set is automatically stored in persistent configuration. This enables the switch to preserve the active zone set information across switch resets.
- All other switches in the fabric receive the active zone set so they can enforce zoning in their respective switches.
- Hard and soft zoning are implemented using the active zone set. Modifications take effect during zone set activation.
- An FC ID or Nx port that is not part of the active zone set belongs to the default zone and the default zone information is not distributed to other switches.

Note If one zone set is active and you activate another zone set, the currently active zone set is automatically deactivated. You do not need to explicitly deactivate the currently active zone set before activating a new zone set.

Figure 15-4 shows a zone being added to an active zone set.

Figure 15-4 Active and Full Zone Sets



Creating Zone Sets

To create zone sets, follow these steps:

Step 1 From Fabric Manager, choose **Zone > Edit Local Full Zone Database** from the Zone menu or right-click a VSAN folder in the Logical tab and choose **Edit Local Full Zone Database** from the pop-up menu.

If you chose **Zone > Edit Local Full Zone Database**, or the **All VSANs** folder is selected, then you see the Select VSAN dialog box. Select the VSAN and click **OK**.

You see the Edit Local Full Zone Database window for the VSAN you selected.

Step 2 Right-click the **Zonese**ts folder in the Edit Local Full Zone Database dialog box for that VSAN and select **Insert** to add a zone set.

You can activate the zone set after creation by clicking the **Activate** button. This button appears when you right-click the newly created zone set. This configuration is distributed to the other switches in the network fabric.

Note When you confirm the activate operation, the current running configuration is saved to the startup configuration. This permanently saves any changes made to the running configuration (not just zoning changes).

Adding Zones to a Zone Set

To add a zone to a zone set from the Edit Local Full Zone Database window, drag and drop the zone to the folder for the zone set.

Alternatively, follow these steps:

Step 1 Click the **Zone sets** folder and then right-click the folder for the zone set to which you want to add a zone and choose **Insert** from the pop-up menu.

You see the Zone dialog box. You can filter the entries in the Zone dialog box by entering the first few letters of the zones you are searching for in the top text box in the Zone dialog box.

Step 2 Select the zone that you want to add to the zone set and click **Add**.

The zone is added to the zone set in the zone database.

Activating Zone Sets

Once zones and zone sets have been created and populated with members, you must activate the zone set. Note that only one zone set can be activated at any time. If zoning is activated, any member that is not assigned to an active zone belongs to the default zone. If zoning is not activated, all members belong to the default zone.

To activate a zone set, follow these steps:

Step 1 Right-click the zone set in the Edit Local Full Database dialog box.

Step 2 Click **Activate**.

You see the zone set in the Active Zone Set folder.

Note If one zone set is active and you activate another zone set, the currently active zone set is automatically deactivated.

Deactivating Zone Sets

To deactivate a zone set, follow these steps:

Step 1 Right-click the zone set in the Edit Full Database dialog box.

Step 2 Click **Deactivate**.

You see the zone set removed from the Active Zone Set folder.

Caution If you deactivate the active zone set in a VSAN that is also configured for IVR, the active IVR zone set (IVZS) is also deactivated and all IVR traffic to and from the switch is stopped. This deactivation can disrupt traffic in more than one VSAN. Before deactivating the active zone set, check the active zone analysis for the VSAN. To reactivate the IVZS, you must reactivate the regular zone set (see the "Configuring IVR Zones and Zone Sets" section on page 16-14).

Caution If the currently active zone set contains IVR zones, activating the zone set from a switch where IVR is not enabled disrupts IVR traffic to and from that VSAN. We strongly recommend that you always activate the zone set from an IVR-enabled switch to avoid disrupting IVR traffic.

Creating Additional Zones and Zone Sets

To create additional zones and zone sets, follow these steps:

Step 1 With the Edit Full Database dialog box open, right-click the **Zones** folder and choose **Insert** from the pop-up menu.

Step 2 Enter the zone name in the dialog box that appears and click **OK** to add the zone.

The zone is automatically added to the zone database.

Step 3 Right-click the **Zonesets** folder in the Edit Full Database dialog box, and choose **Insert**.

Step 4 Enter the zone set name in the dialog box that appears and click **OK** to add the zone set.

The zone set is automatically added to the zone database.

Cloning Zones and Zone Sets

You can make a copy and then edit it without altering the existing active zone set. You can copy an active zone set from the bootflash: directory, volatile: directory, or slot0, to one of the following areas:

- To the full zone set
- To a remote location (using FTP, SCP, SFTP, or TFTP).

The active zone set is not part of the full zone set. You cannot make changes to an existing zone set and activate it, if the full zone set is lost or is not propagated.

To clone a zone or zone set from the Edit Local Full Zone Database window, follow these steps:

Step 1 Select the **Zones** or **Zonesets** folder, right-click the folder for the zone or zone set that you want to clone, and choose **Clone** from the pop-up menu.

Step 2 Enter the name of the cloned zone or zone set.

By default, the dialog box displays the selected zone name by prepending the original zone name with “Cloned" (for example, ClonedZone1) and selects the read-only zone state to match the cloned zone.

Step 3 Click **OK** to add the cloned zone to the zone database.

Caution Copying an active zone set to a full zone set may overwrite a zone with the same name, if it already exists in the full zone set database.

Note Fabric Manager Release 2.0(1b) and earlier, or Fabric Manager Release 2.1(1a) or later includes the zone clone feature.

Deleting Zones, Zone Sets, and Aliases

To delete zones, zone sets, or aliases, follow these steps:

Step 1 From Fabric Manager, choose **Zone > Edit Local Full Zone Database** from the Zone menu, or right-click a VSAN folder in the Logical tab and choose **Edit Local Full Zone Database** from the pop-up menu.

If you chose **Zone > Edit Local Full Zone Database**, then you see the Select VSAN dialog box. Select the VSAN and click **OK**.

You see the Edit Local Full Zone Database window for the VSAN you selected.

Step 2 Select the zone, zone set, or alias you want to delete.

Step 3 Right-click the object and choose **Delete** from the pop-up menu, or click the **Delete** button.

The selected object is deleted from the zone database.

Zone Enforcement

Zoning can be enforced in two ways: soft and hard. Each end device (N port or NL port) discovers other devices in the fabric by querying the name server. When a device logs in to the name server, the name server returns the list of other devices that can be accessed by the querying device. If an Nx port does not know about the FC IDs of other devices outside its zone, it cannot access those devices.

In soft zoning, zoning restrictions are applied only during interaction between the name server and the end device. If an end device somehow knows the FC ID of a device outside its zone, it can access that device.

Hard zoning is enforced by the hardware on each frame sent by an Nx port. As frames enter the switch, source-destination IDs are compared with permitted combinations to allow the frame at wirespeed. Hard zoning is applied to all forms of zoning.

Note Hard zoning enforces zoning restrictions on every frame, and prevents unauthorized access.

Switches in the Cisco MDS 9000 Family support both hard and soft zoning.

The Default Zone

Each member of a fabric (in effect a device attached to an Nx port) can belong to any zone. If a member is not part of any active zone, it is considered to be part of the default zone. Therefore, if no zone set is active in the fabric, all devices are considered to be in the default zone. Even though a member can belong to multiple zones, a member that is part of the default zone cannot be part of any other zone. The switch determines whether a port is a member of the default zone when the attached port comes up.

Note Unlike configured zones, default zone information is not distributed to the other switches in the fabric.

Traffic can either be permitted or denied among members of the default zone. This information is not distributed to all switches; it must be configured in each switch.

Note When the switch is initialized for the first time, no zones are configured and all members are considered to be part of the default zone. Members are not permitted to talk to each other.

Configure the default zone policy on each switch in the fabric. If you change the default zone policy on one switch in a fabric, be sure to change it on all the other switches in the fabric.

Note The default settings for default zone configurations can be changed.

Configuring the Default Zone Policy

The default zone members are explicitly listed when the default policy is configured as **permit** or when a zone set is active. When the default policy is configured as **deny**, the members of this zone are not explicitly enumerated when you deactivate the zone set.

You can change the default zone policy for any VSAN by choosing **VSAN**xxx > **Default Zone** from the Fabric Manager menu tree and clicking the **Policies** tab. It is recommended that you establish connectivity among devices by assigning them to a non-default zone.

The active zone set is shown in italic type. After you have made changes to the active zone set and before you activate the changes, the zone set is shown in boldface italic type.

To permit or deny traffic to members in the default zone from the Zone Server, follow these steps:

Step 1 Choose **VSANxxx > Default Zone** from the Fabric Manager Logical Domains menu tree, and click the **Policies** tab in the Information pane.

You see the zone information in the Information pane.

Step 2 Click the **Default Zone Behavior** field and choose either **permit** or **deny** from the pull-down menu.

Performing Zone Merge Analysis

When two switches in a fabric are merged using a TE or E port, these TE and E ports may become isolated when the active zone set databases are different between the two switches or fabrics. You can perform a zone merge analysis prior to merging the switches to see if the merge will succeed or fail.

To perform a zone merge analysis, follow these steps:

Step 1 From Fabric Manager, choose **Zone > Merge Analysis** from the Zone menu.

You see the Zone Merge Analysis dialog box.

Step 2 Select the first switch to be analyzed from the Check Switch 1 drop-down list.

Step 3 Select the second switch to be analyzed from the And Switch 2 drop-down list.

Step 4 Enter the VSAN ID where the zone set merge failure occurred in the For Active Zoneset Merge Problems in VSAN Id field.

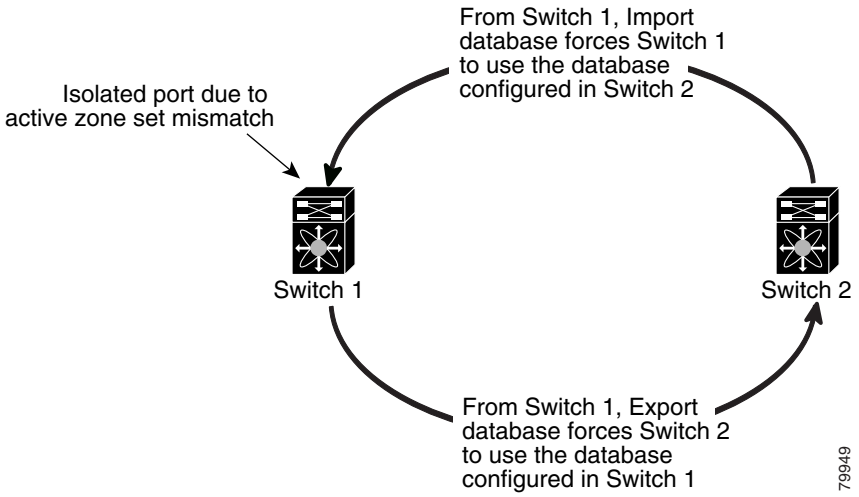
Step 5 Click **Analyze** to analyze the zone merge. Click **Clear** to clear the analysis data from the Zone Merge Analysis dialog box.

Recovering from Link Isolation

When two switches in a fabric are merged using a TE or E port, these TE and E ports may become isolated when the active zone set databases are different between the two switches or fabrics. When a TE port or an E port become isolated, you can recover that port from its isolated state using one of three options:

- Import the neighboring switch's active zone set database and replace the current active zone set (see Figure 15-5).
- Export the current database to the neighboring switch (see Figure 15-5).
- Manually resolve the conflict by editing the full zone set, activating the corrected zone set, and then bringing up the link.

Figure 15-5 Importing and Exporting the Database



Importing Zone Sets

Note Importing from one switch and exporting from another switch can lead to isolation again.

You can import active zone sets (do a Merge Fail Recovery) if the cause of an ISL failure is a zone merge failure.

To import an active zone set, follow these steps:

Step 1 From Fabric Manager, choose **Zone > Merge Fail Recovery** from the Zone menu.

You see the Zone Merge Failure Recovery dialog box.

Step 2 Select the **Import Active Zoneset** radio button.

Step 3 Select the switch from which to import the zone set information from the drop-down list.

Step 4 Select the VSAN from which to import the zone set information from the drop-down list.

Step 5 Select the interface to use for the import process.

Step 6 Click **OK** to import the active zone set, or click **Close** to close the dialog box without importing the active zone set.

Exporting Active Zone Sets

You can export active zone sets (do a Merge Fail Recovery) if the cause of an ISL failure is a zone merge fail.

To export an active zone set, follow these steps:

Step 1 From Fabric Manager, choose **Zone > Merge Fail Recovery** from the Zone menu.

You see the Zone Merge Failure Recovery dialog box.

Step 2 Select the **Export Active Zoneset** radio button.

Step 3 Select the switch to which to export the zone set information from the drop-down list.

Step 4 Select the VSAN to which to export the zone set information from the drop-down list.

Step 5 Select the interface to use for the export process.

Step 6 Click **OK** to export the active zone set, or click **Close** to close the dialog box without exporting the active zone set.

Full Zone Set Propagation

All switches in the Cisco MDS 9000 Family distribute active zone sets when new E port links come up or when a new zone set is activated in a VSAN. The zone set distribution takes effect while sending merge requests to the adjacent switch or while activating a zone set.

To propagate the full zone set from Fabric Manager, follow these steps:

Step 1 Select **VSAN**xxx **> ZoneSet**xx from the Logical Domains pane. You see the zone set configuration in the Information pane.

Step 2 Select the **Policies** tab.

Step 3 Set the propagation column to **fullZoneset** from the drop-down menu.

Step 4 Click **Apply Changes** to propagate the full zone set, or click **Undo Changes** to discard any changes you made.

One-Time Distribution

To propagate a one-time distribution of the full zone set from Fabric Manager, follow these steps:

Step 1 Select **Zone > Edit Local Full Zone Database** from the main menu.

Step 2 Select the appropriate VSAN from the list. You see the Edit Local Full Zone Set configuration tool.

Step 3 Click **Distribute** to distribute the full zone set across the fabric.

Copying a Full Zone Database

You can recover a database by copying the active zone database or the full zone database.

To copy a zone database, follow these steps:

Step 1 From Fabric Manager, choose **Zone > Copy Full Zone Database** from the Zone menu.

You see the Recover Full Zone Database dialog box.

Step 2 Select the **Copy Active** or the **Copy Full** radio button, depending on which type of database you want to copy.

Step 3 Select the source VSAN from which to copy the information from the drop-down list.

Step 4 If you selected **Copy Full**, select the source switch and the destination VSAN from those drop-down lists.

Step 5 Select the destination switch from the drop-down list.

Step 6 Click **Copy** to copy the database, or click **Close** to close the dialog box without copying.

Migrating a Non-MDS Database

To use the Zone Migration Wizard to migrate a non-MDS database, follow these steps:

Step 1 From Fabric Manager, choose **Zone > Migrate Non-MDS Database** from the Zone menu.

You see the Zone Migration Wizard.

Step 2 Follow the prompts in the wizard to migrate the database.

Note All alphanumeric characters or one of the following symbols ($, -, ^, _) are supported.

Zone-Based Traffic Priority

As of Cisco MDS SAN-OS 2.0, the zoning feature provides an additional segregation mechanism to prioritize select zones in a fabric and set up access control between devices. Using this feature, you can configure the Quality of Service (QoS) priority as a zone attribute. You can assign the QoS traffic priority attribute to be **high**, **medium**, or **low**. By default, zones with no specified priority are implicitly assigned a **low** priority.

To use this feature, you need to obtain the ENTERPRISE_PKG license and you must enable QoS in the switch.

This feature allows SAN administrators to configure QoS in terms of a familiar data flow identification paradigm. You can configure this attribute on a zone-wide basis, rather than between zone members.

Configuring Zone QoS and Broadcast Attributes

QoS attribute-specific configuration changes take effect when you activate the zone set of the associated zone.

Note If a member is part of two zones with two different QoS attributes, the higher QoS value is implemented. This situation does not arise in the VSAN-based QoS as the first matching entry is implemented.

As of Cisco MDS SAN-OS Release 2.0(1b), you can configure broadcast frames in the basic zoning mode. By default, broadcast zoning is disabled. When enabled, broadcast frames are sent to all Nx Ports. Broadcast zoning can only be implemented in Cisco MDS 9000 Family switches running Cisco MDS SAN-OS Release 2.0(1b) or later.

Tip If any NL port attached to an FL port shares a broadcast zone with the source of the broadcast frame, then the frames are broadcast to all devices in the loop.

Caution If Broadcast zoning is implemented in a switch, you cannot configure the interop mode in that VSAN.

To configure the zone QoS or broadcast attributes in Fabric Manager, follow these steps:

Step 1 Choose **VSANx**xx > ***<zone set name>*** from the Fabric Manager Logical Domains menu tree, and click the **Policies** tab in the Information pane.

You see the Zone policy information in the Information pane.

Step 2 Check the **QoS** check box to enable QoS on the default zone.

Step 3 Click **QoS Priority** and choose **low**, **medium**, or **high** from the pull-down menu.

Step 4 Check the **Broadcast** check box to enable broadcast frames on the default zone.

Step 5 Click the **Apply Changes** icon to save these changes or click the **Undo Changes** icon to discard these changes.

About LUN Zoning

Logical unit number (LUN) zoning is a feature specific to switches in the Cisco MDS 9000 Family.

Caution LUN zoning can only be implemented in Cisco MDS 9000 Family switches. If LUN zoning is implemented in a switch, you cannot configure the interop mode in that switch.

Note LUN zoning can be implemented in Cisco MDS 9000 Family switches running Cisco MDS SAN-OS Release 1.2(x) or earlier.

A storage device can have multiple LUNs behind it. If the device port is part of a zone, a member of the zone can access any LUN in the device. With LUN zoning, you can restrict access to specific LUNs associated with a device.

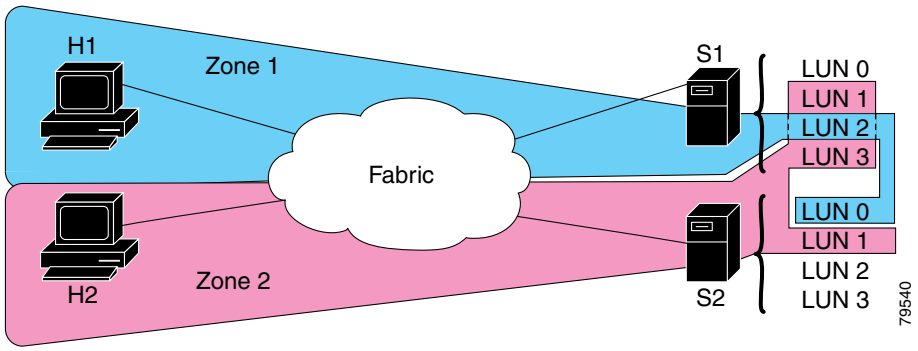
Note When LUN 0 is not included within a zone, then, as per standards requirements, control traffic to LUN 0 (for example, REPORT_LUNS, INQUIRY) is supported, but data traffic to LUN 0 (for example, READ, WRITE) is denied.

- Host H1 can access LUN 2 in S1 and LUN 0 in S2. It cannot access any other LUNs in S1 or S2.
- Host H2 can access LUNs 1 and 3 in S1 and only LUN 1 in S2. It cannot access any other LUNs in S1 or S2.

Note Unzoned LUNs automatically become members of the default zone.

Figure 15-6 shows a LUN-based zone example.

Figure 15-6 LUN Zoning Access



Configuring a LUN-Based Zone

To create LUN-based zones, follow these steps:

Step 1 From Fabric Manager, choose **Zone > Edit Local Full Zone Database** from the Zone menu, or right-click a VSAN folder in the Logical tab and choose **Edit Local Full Zone Database** from the pop-up menu.

If you chose **Zone > Edit Local Full Zone Database**, then you see the Select VSAN dialog box. Select the VSAN and click **OK**.

You see the Edit Local Full Zone Database window for the VSAN you selected.

Step 2 Right-click the **Zones** folder in the Edit Local Full Zone Database dialog for that VSAN and select **Insert** to add a zone.

You can specify that the zone be a read-only zone by checking the Read Only check box. (For more information on read-only zones, see the "About Read-Only Zones" section on page 15-23.)

Step 3 Select either **WWN** or **FCID** radio button for the Zone By options to create a LUN-based zone.

Step 4 Check the **LUN** check box and add the LUNs for this zone in the text box.

Step 5 Click **Add** to add this LUN-based zone or **Close** to close the dialog box without adding the LUN-based zone.

Assigning LUNs to Storage Subsystems

LUN masking and mapping restricts server access to specific LUNs. If LUN masking is enabled on a storage subsystem and if you want to perform additional LUN zoning in a Cisco MDS 9000 Family switch, obtain the LUN number for each Host Bus Adapter (HBA) from the storage subsystem and then configure the LUN-based zone procedure provided earlier.

Note Refer to the relevant user manuals to obtain the LUN number for each HBA.

Caution If you make any errors when configuring this scenario, you are prone to loose data.

About Read-Only Zones

Note Read-only zoning can be implemented in Cisco MDS 9000 Family switches running Cisco MDS SAN-OS Release 1.2(x) or above.

By default, an initiator has both read and write access to the target's media when they are members of the same Fibre Channel zone. The read-only zone feature allows members to have only read access to the media within a read-only Fibre Channel zone.

You can also configure LUN zones as read-only zones.

Guidelines to Configure Read-Only Zones

Any zone can be identified as a read-only zone. By default all zones have read-write permission unless explicitly configured as a read-only zone.

Follow these guidelines when configuring read-only zones:

- If read-only zones are implemented, the switch prevents write access to user data within the zone.
- If two members belong to a read-only zone and to a read-write zone, read-only zone has priority and write access is denied.
- LUN zoning can only be implemented in Cisco MDS 9000 Family switches. If LUN zoning is implemented in a switch, you cannot configure interop mode in that switch.
- Read-only volumes are not supported by some operating system and file system combinations (for example, Windows NT or Windows 2000 and NTFS file system). Volumes within read-only zones are not available to such hosts. However, if these hosts are already booted when the read-only zones are activated, then read-only volumes are available to those hosts.

The read-only zone feature behaves as designed if FAT16 or FAT32 file system is used with the above-mentioned Windows operating systems.

Configuring Read-Only Zones

To create read-only zones, follow these steps:

Step 1 From Fabric Manager, choose **Zone > Edit Local Full Zone Database** from the Zone menu, or right-click a VSAN folder in the Logical tab and choose **Edit Local Full Zone Database** from the pop-up menu.

If you chose **Zone > Edit Local Full Zone Database**, then you see the Select VSAN dialog box. Select the VSAN and click **OK**.

You see the Edit Local Full Zone Database window for the VSAN you selected.

Step 2 Right-click the **Zones** folder in the Edit Local Full Zone Database dialog box for that VSAN and select **Insert** to add a zone.

Step 3 Check the **Read Only** check box to create a read-only zone.

Backing Up and Restoring Zones

You can back up the zone configuration to a workstation using TFTP. This zone backup file can then be used to restore the zone configuration on a switch. Restoring the zone configuration overwrites any existing zone configuration on a switch.

To backup or restore the full zone configuration using Fabric Manager, follow these steps:

Step 1 From Fabric Manager, choose **Zone > Edit Local Full Zone Database** from the Zone menu, or right-click a VSAN folder in the Logical tab and choose **Edit Local Full Zone Database** from the pop-up menu.

If you chose **Zone > Edit Local Full Zone Database**, then you see the Select VSAN dialog box. Select the VSAN and click **OK**.

You see the Edit Local Full Zone Database window for the VSAN you selected.

Step 2 Choose **File > Backup** to back up the existing zone configuration to a workstation using TFTP.

Step 3 Choose **File > Restore** to restore a saved zone configuration. You can optionally edit this configuration before restoring it to the switch.