CHAPTER 15

Configuring and Managing Zones

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. This chapter defines various zoning concepts and provides details on zone set and management features in the switch.

This chapter contains the following topics:

Zoning Features

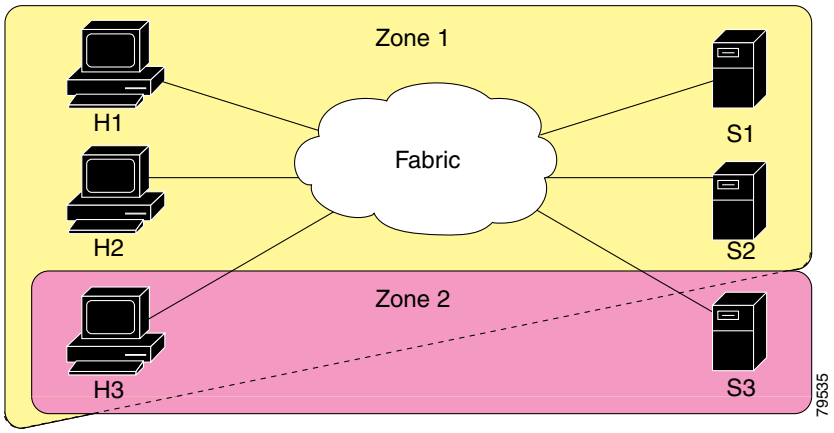
Zoning has the following features:

- A zone consists of multiple zone members.
  - Members in a zone can access each other; members in different zones cannot access each other.
  - 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.
  - Zones can vary in size.
  - Devices can belong to more than one zone.
  - A zone set consists of one or more zones.
  - 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.
  - A zone can be a member of more than one zone set.
  - 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 the option 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.
  - Zone membership criteria is based on WWNs or FC IDs.
  - Port world wide name (pWWN)—Specifies the pWWN of an N port attached to the switch as a member of the zone.
  - Fabric pWWN—Specifies the WWN of the fabric port (switch port's WWN). This membership is also referred to as port-based zoning.
  - FC ID—Specifies the FC ID of an N port attached to the switch as a member of the zone.
  - Interface and switch WWN (sWWN)—Specifies the interface of a switch identified by the sWWN. This membership is also referred to as interface-based zoning.
  - Interface and domain ID—Specifies the interface of a switch identified by the domain ID.
  - Domain ID and port number—Specifies the domain ID of an MDS domain and additionally specifies a port belonging to a non-Cisco switch.
  - IP address—Specifies the IP address (and optionally the subnet mask) of an attached device.
- 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.

Zoning Example

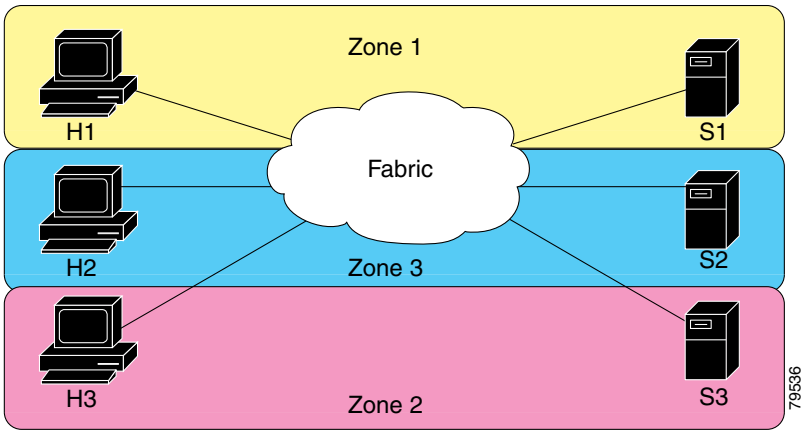
Figure 15-1 illustrates a zone set with two zones, Zone 1 and Zone 2, in a fabric. Zone 1 provides access from all three hosts (H1, H2, H3) to the data residing on storage systems S1 and S2. Zone 2 restricts the data on S3 to access only by H3. Note that H3 resides in both zones.

Figure 15-1 Fabric with Two Zones



Of course, there are other ways to partition this fabric into zones. Figure 15-2 illustrates another possibility. Assume that there is a need to isolate storage system S2 for the purpose of testing new software. To achieve this, Zone 3 is configured, which contains only host H2 and storage S2. You can restrict access to just H2 and S2 in zone 3, and to H1 and S1 in Zone 1.

Figure 15-2 Fabric with Three Zones



Configuring a Zone

A zone can be configured using one of the following types 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).
- 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.

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.

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

Creating Zones

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, perform the following steps.

Step 1 From the Fabric Manager, choose **Zone > Edit Full Database on Switch**. You see the Select VSAN dialog box. Choose the VSAN and click **OK**.

You can also right-click a VSAN folder in the **Logical** tab and choose **Edit Local Zone Database** from the pop-up menu. You see the Edit VSANxxx Local Full Zones window.

Step 2 Right-click the zone for that VSAN and choose **Insert** to add a zone.

Check the **Set Zone as Read Only** check box to specify that the zone be a ready-only zone. (For more information on read-only zones see the "Read-Only Zoning" section on page 15-17.)

Creating Additional Zones

To create additional zones, follow these steps:

Step 1 With the Edit Full Database on Switch dialog 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.

Cloning Zones

Another method of adding zones is to clone existing zones.

To clone a zone from the Edit Full Database on Switch window, follow these steps:

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

Step 2 Enter the name of the cloned zone. By default, the dialog displays the selected zone as ClonedZone1.

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

Adding Zone Members

Once you have created a zone, you can add members to the zone. You can add members using the following port identification types:

- pWWN—The world wide name of the port configured on the end device (in hex format).
- Fabric port WWN—The world wide name of the physical port on the switch (in hex format).
- FC alias—The alias name in alphabetic characters (for example, Payroll).
- LUN—The logical unit number of a disk in a disk device.

For more information about port identification types, refer to the *Cisco 9000 Family Configuration Guide*.

To add members to a zone, follow these steps:

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

You see the Add Members to Zone dialog.

Step 2 Check the check box to the left of the NxPort WWN field.

Step 3 Choose one of the ports in the VSAN 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 can have multiple IDs depending on the operating system. You can select from 6 different operating systems.

Displaying Port Membership Information

To display port membership information for members assigned to zones, follow these steps.

Step 1 From the Fabric Manager, choose **Zone > Edit Full Database on Switch**. You see the Select VSAN dialog box. Choose the VSAN and click **OK**.

You can also right-click a VSAN folder in the Logical tab and choose **Edit Local Zone Database** from the pop-up menu. You see the Edit VSANxxx Local Full Zones window for the VSAN you selected.

Step 2 Click the **Members** tab.

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. For more information, see the"Changing the Default Zone Policy" section on page 15-15.

Viewing Zone Statistics

To monitor zone statistics from the Zone Server, choose **VSANxxx > Domain Manager** from the Fabric Manager menu tree. You see the zone information in the Information pane. Click on the **Statistics** tab to see the statistics information for the switches in the zone.

Deleting Zones and Members

To delete zones or members, follow these steps.

Step 1 From the Fabric Manager, choose **Zone > Edit Full Database on Switch**. You see the Select VSAN dialog box. Choose the VSAN and click **OK**.

You can also right-click a VSAN folder in the **Logical** tab and choose **Edit Local Zone Database** from the pop-up menu. You see the Edit VSANxxx Local Full Zones window for the VSAN you selected.

Step 2 Choose the zone or member you want to delete.

Step 3 Right-click the object and choose **Delete** from the pop-up menu. The selected object is deleted from the zone database.

Configuring Aliases

You can assign an alias name and configure an alias member using either the FC ID, fabric port WWN (fWWN), or pWWN values.

Creating Zones with Aliases

To create a zone with aliases, perform these steps:

Step 1 Choose **Zone > Edit Local Full Zone Database**. You see the Select VSAN dialog box

Step 2 Choose the VSAN on which you want to create the zone, and click **OK**. You see zone information for that VSAN.

Step 3 Click the **Aliases** tab above the right pane.

Step 4 Right-click in left window pane and choose **Insert**. You see the Create Alias dialog box.

Step 5 Enter the Alias name and choose the pWWN. You can add/associate multiple pWWNs, fWWNs to same alias name. The pWWNs do not have to be attached to the fabric you are currently managing.

Step 6 Click **OK** to create the alias.

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

Step 8 Name the zone as desired.

Step 9 Click the **Aliases** tab above the right window pane.

Step 10 Click and drag the desired alias members you created in Steps 5 and 6 above, from the right window pane to the Zone folder you just created in the left window pane.

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 the Fabric Manager, choose **Zone > Edit Full Database on Switch**. You see the Select VSAN dialog box. Choose the VSAN and click **OK**.

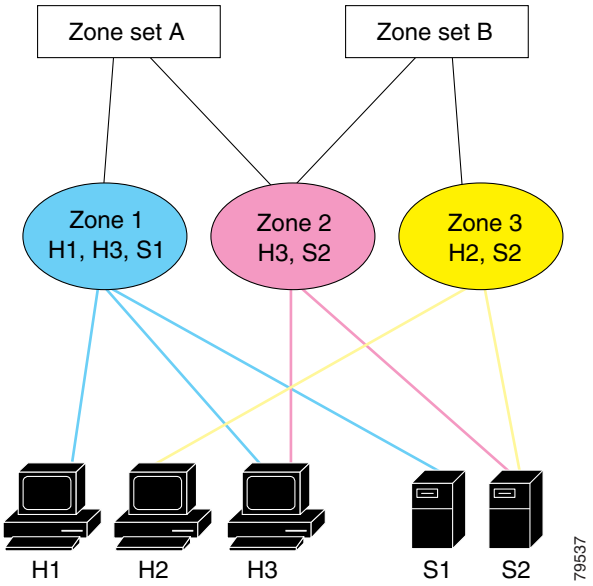
You can also right-click a VSAN folder in the **Logical** tab and choose **Edit Local Zone Database** from the pop-up menu. You see the Edit VSANxxx Local Full Zones window for the VSAN you selected.

Step 2 Click the **Aliases** tab to see the aliases for that zone.

Zone Sets

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).

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

Active and Full Zone Set Considerations

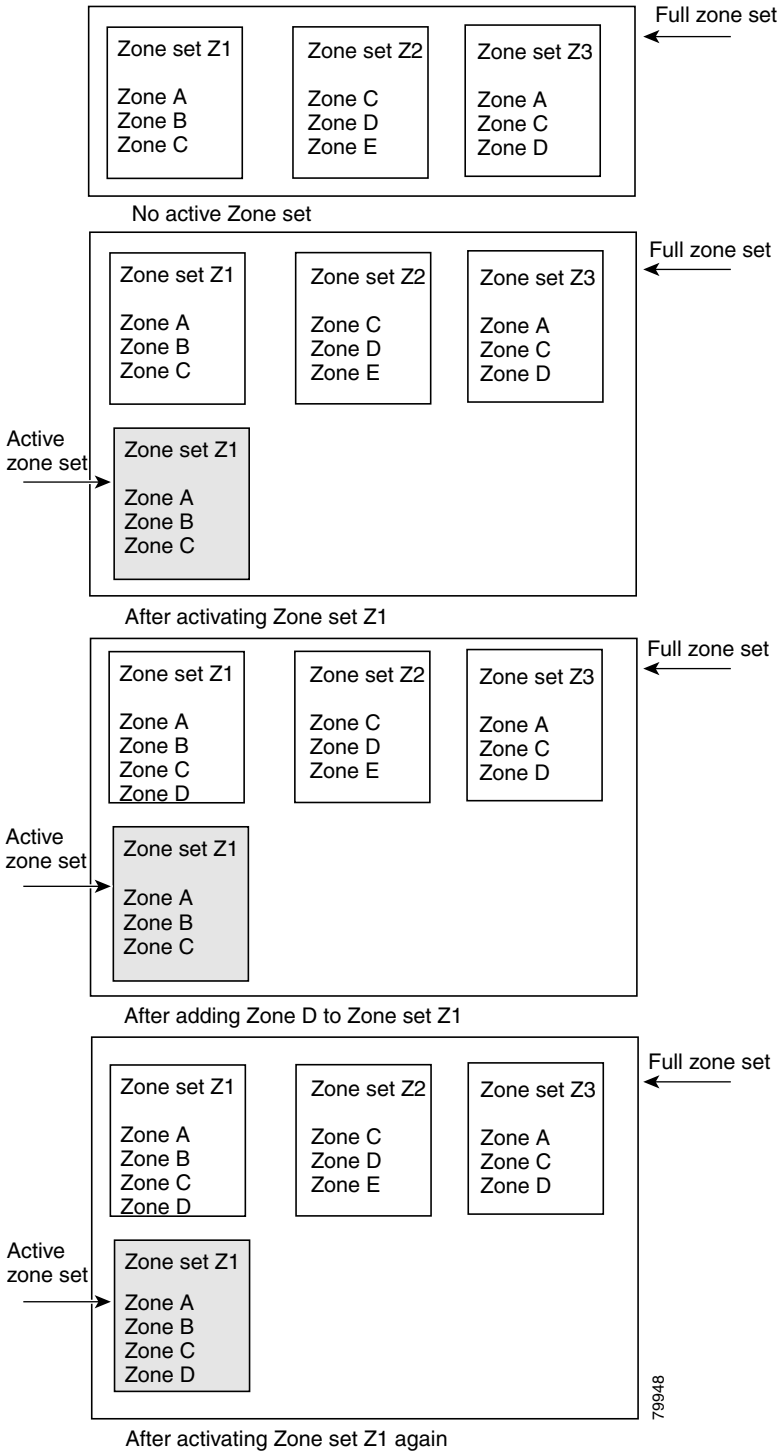
Before configuring a zone set, consider the following guidelines:

- 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. The changes do not take effect until the zone set is activated.
- 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.

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

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

Figure 15-4 Active and Full Zone Sets



Distributing Zone Sets

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 distribution takes effect while sending merge requests to the adjacent switch or while activating a zone set.

Copying Zone Sets

The active zone set is not a part of the full zone set. You can not make changes to an existing zone set and activate it, if the full zone set is lost or is not propagated. You can make a copy of an active zone set and then edit it without altering the existing active zone set. You can copy an active-zone set to a location in bootflash, volatile, slot0, to a remote location (using FTP, SCP, SFTP, or TFTP), or to the full zone set.

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.

Creating Zone Sets

To create zone sets, perform the following steps.

Step 1 From the Fabric Manager, choose **Zone > Edit Full Database on Switch**. You see the Select VSAN dialog box. Choose the VSAN and click **OK**.

You can also right-click a VSAN folder in the **Logical** tab and choose **Edit Local Zone Database** from the pop-up menu. You see the Edit VSANxxx Local Full Zones window.

Step 2 Right-click the zone set for that VSAN and choose **Insert** to add a zone set.

You can activate the zone set by clicking **Activate**. 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).

Creating Additional Zone Sets

To create additional zone sets, follow these steps:

Step 1 To create a zone set, right-click the ZoneSets folder in the Edit Full Database on Switch dialog box, and choose **Insert**.

Step 2 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 Zone Sets

Another method of adding zone sets is to clone existing zone sets.

To clone a zone set from the Edit Full Database on Switch window, follow these steps:

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

Step 2 Enter the name of the cloned zone set. By default, the dialog displays the selected zone as ClonedZoneset1.

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

Adding Zones to a Zone Set

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

Alternatively, follow these steps:

Step 1 Click the ZoneSets 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 Server Select 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 or Enforcing Zone Sets

Once zones and zone sets have been created and populated with members, you must activate or enforce 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 Full Database on Switch 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 activate a zone set, follow these steps:

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

Step 2 Click **Deactivate**. The zone set is removed from the Active Zone Set folder.

Importing Active Zone Sets

You can import active zone sets (do a Merge Fail Recovery) if the cause of an ISL failure is a zone merge fail. To import an active zone set, follow these steps:

Step 1 From the Fabric Manager, choose **Zone > Merge Fail Recovery**. You see the Zone Merge Failure Recovery dialog box.

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

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

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

Step 5 Choose 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 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 the Fabric Manager, choose **Zone > Merge Fail Recovery**. You see the Zone Merge Failure Recovery dialog box.

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

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

Step 4 Choose the VSAN to which to export the Zoneset information from the drop-down list.

Step 5 Choose 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 without exporting the active zone set.

Deleting Zone Sets or Members

To delete zone sets or members, follow these steps.

Step 1 From the Fabric Manager, choose **Zone > Edit Full Database on Switch**. You see the Select VSAN dialog box. Choose the VSAN and click **OK**.

You can also right-click a VSAN folder in the **Logical** tab and choose **Edit Local Zone Database** from the pop-up menu. You see the Edit VSANxxx Local Full Zones window for the VSAN you selected.

Step 2 Choose the zone set or member you want to delete.

Step 3 Right-click the object and choose **Delete** from the pop-up menu. The selected object is deleted from the zone database.

Clearing the Zone Database

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

Recovering a Full Zone Database

You can recover a database by copying the active zone database or the full zone database. To recover a zone database, follow these steps:

Step 1 From the Fabric Manager, choose **Zone > Recover Full Zone Database**. You see the Recover Full Zone Database dialog box.

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

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

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

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

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

Performing Zone Merge Analysis

To perform a zone merge analysis, follow these steps:

Step 1 From the Fabric Manager, choose **Zone > Merge Analysis**. You see the Zone Merge Analysis window.

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

Step 3 Choose 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 field.

Step 5 Click **Analyze** to analyze the zone merge. Click **Clear** to clear the analysis data from the Zone Merge Analysis window. If you click **Analyze** without clicking **Clear**, the new zone merge analysis data displays below the old data.

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.

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.

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

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

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. 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.

Setting Default Zone Policy

Each VSAN contains a default zone, which by default, contains all connected devices assigned to the VSAN.

You can change the default zone policy for any VSAN by choosing **VSANxxx > Default Zone** from the Fabric Manager menu tree and clicking the **Policies** tab. However, we recommend that you establish connectivity among devices by assigning them to a nondefault 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. The tooltip for each zone indicates the activation time or modification time.

Changing the Default Zone Policy

Each member in the fabric can belong to any zone. If a member does not belong to any zone, it is part of the default zone. If no zone has been activated in the fabric, all members belong to the default zone. Even though a member can belong to multiple zones, a member in the default zone cannot be part of any other zone.

Traffic can be permitted and denied to members in the default zone. This information is not distributed to all switches. Permission and denial must be set for each switch in the fabric.

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 menu tree, and click the **Policies** tab. The zone information displays in the Information pane.

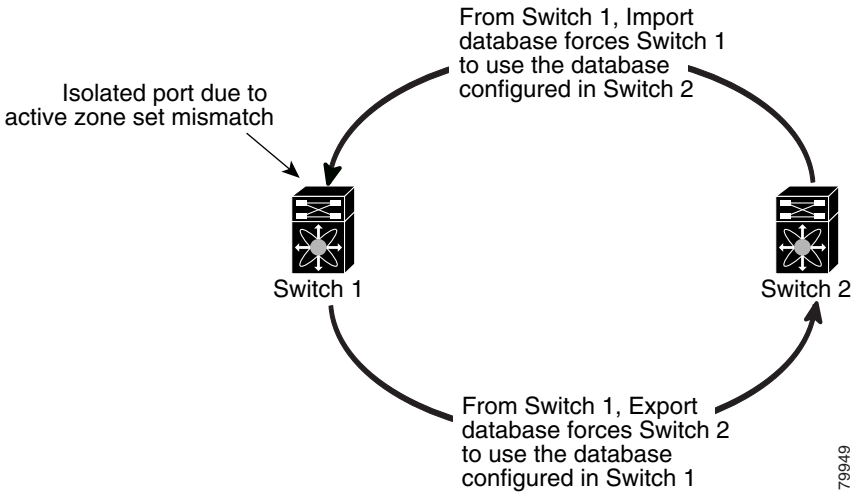
Step 2 Click the DefaultZoneBehavior field and choose either **permit** or **deny** from the pull-down menu.

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. (See Figure 15-5.) 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 "Importing Active Zone Sets" section on page 15-12.
- Export the current database to the neighboring switch. See "Exporting Active Zone Sets" section on page 15-12.
- 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 from one switch and exporting from another switch can lead to isolation again.

LUN Zoning

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

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

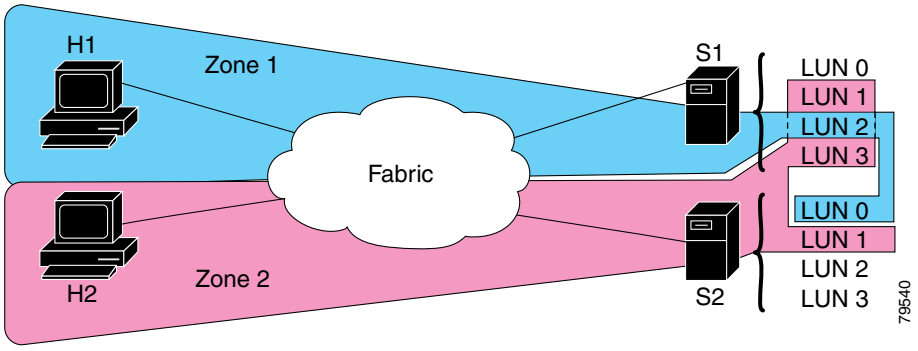
A storage device can have multiple LUNs behind it. If the device port is part of a zone, a member of the zone can access any LUN in the device. With LUN zoning, you can restrict access to specific LUNs associated with a device.

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

- Host H1 can access LUN 2 in S1 and LUN 0 in S2. It cannot access any other LUN 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 LUN in S1 or S2.

Unzoned LUNs automatically become members of the default zone.

Figure 15-6 LUN Zoning Access



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.

Caution 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.

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 in the preceding section.

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 lose data.

Read-Only Zoning

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.

Default Settings

Table 15-1 lists the default settings for zone parameters.

Table 15-1 Default Zone Parameters

Parameters	Default
Default zone policy	Denied to all members.
Full zone set distribute	The full zone set(s) is not distributed.
Read-only zones	Read-write attributes for all zones.

Migrating a Non-MDS Database

You use the Zone Migration Wizard to migrate a non-MDS database.

Step 1 From the Fabric Manager, choose **Zone > Migrate Non-MDS Database**. You see the Zone Migration Wizard.

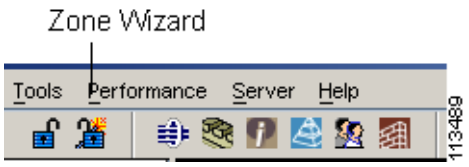
Step 2 Follow the prompts in the wizard to migrate the database.

Using the Zone Wizard

Use the Zone Wizard to configure zones, read-only zones, and IVR zones.

Step 1 From the Fabric Manager, click the **Zone Wizard** icon in the Fabric Manager Zone toolbar (see Figure 15-7).

Figure 15-7 Zone Wizard Icon



You see the Zone Wizard.

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