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.

Advanced zoning capabilities specified in the FC-GS-4 and FC-SW-3 standards are provided. You can use either the existing basic zoning capabilities or the advanced, standards-compliant zoning capabilities.

This chapter includes the following sections:

- About Zoning, page 30-1
- Using the Quick Config Wizard, page 30-7
- Zone Configuration, page 30-10
- Zone Sets, page 30-15
- Zone Set Distribution, page 30-26
- Zone Set Duplication, page 30-29
- Advanced Zone Attributes, page 30-36
- Displaying Zone Information, page 30-42
- Enhanced Zoning, page 30-43
- Compacting the Zone Database for Downgrading, page 30-47
- Default Settings, page 30-48

---

**Note**

Table 26-1 on page 26-4 lists the differences between zones and VSANs.

---

About Zoning

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.
About Zoning

- Only one zone set can be activated at any time.
- A zone can be a member of more than one zone set.
- A zone switch can have a maximum of 500 zone sets.
- 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.
- Zone membership criteria is based mainly 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.
  
  IPv4 address—Specifies the IPv4 address (and optionally the subnet mask) of an attached device.
  
  IPv6 address—The IPv6 address of an attached device in 128 bits in colon(:)-separated hexadecimal format.
- 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.
- You can configure up to 8000 zones per VSAN and a maximum of 8000 zones for all VSANs on the switch.

Zoning Example

Figure 30-1 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 30-1  Fabric with Two Zones

Of course, there are other ways to partition this fabric into zones. Figure 30-2 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 30-2  Fabric with Three Zones

Zone Implementation

All switches in the Cisco MDS 9000 Family automatically support the following basic zone features (no additional configuration is required):

- Zones are contained in a VSAN.
- Hard zoning cannot be disabled.
- Name server queries are soft-zoned.
- 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 Member Configuration Guidelines**

All members of a zone can communicate with each other. For a zone with N members, N*(N-1) access permissions need to be enabled. The best practice is to avoid configuring large number of targets and or large numbers of initiators in a single zone. Such configuration wastes switch resources by provisioning and managing many communicating pairs (initiator-to-initiator or target-to-target) which will never actually communicate with each other. For this reason, single initiator with a single target is the most efficient approach to zoning.

The following guidelines must be considered when creating zone members:
- Configuring only one initiator and one target for a zone provides most efficient use of the switch resources.
- Configuring the same initiator to multiple targets is accepted.
- Configuring multiple initiators to multiple targets is not recommended.

**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. However, the modification will be enforced only upon reactivation.
- 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 30-3* shows a zone being added to an activated zone set.
Figure 30-3   Active and Full Zone Sets

Zone set Z1
Zone A
Zone B
Zone C

Zone set Z2
Zone C
Zone D
Zone E

Zone set Z3
Zone A
Zone C
Zone D

No active Zone set

Zone set Z1
Zone A
Zone B
Zone C

Zone set Z2
Zone C
Zone D
Zone E

Zone set Z3
Zone A
Zone C
Zone D

After activating Zone set Z1

Zone set Z1
Zone A
Zone B
Zone C

Zone set Z2
Zone C
Zone D
Zone E

Zone set Z3
Zone A
Zone C
Zone D

After adding Zone D to Zone set Z1

Zone set Z1
Zone A
Zone B
Zone C

Zone set Z2
Zone C
Zone D
Zone E

Zone set Z3
Zone A
Zone C
Zone D

After activating Zone set Z1 again

Zone set Z1
Zone A
Zone B
Zone C

Zone set Z2
Zone C
Zone D
Zone E

Zone set Z3
Zone A
Zone C
Zone D

Full zone set

Active zone set

Full zone set

No active Zone set
Using the Quick Config Wizard

**Note**  
The Quick Config Wizard supports only switch interface zone members.

As of Cisco SAN-OS Release 3.1(1) and NX-OS Release 4.1(2), you can use the Quick Config Wizard on the Cisco MDS 9124 Switch to add or remove zone members per VSAN. You can use the Quick Config Wizard to perform interface-based zoning and to assign zone members for multiple VSANs using Device Manager.

**Note**  
The Quick Config Wizard is supported on the Cisco MDS 9124 Fabric Switch, the Cisco MDS 9134 Fabric Switch, the Cisco Fabric Switch for HP c-Class BladeSystem, and the Cisco Fabric Switch for IBM BladeCenter.

**Caution**  
The Quick Config Wizard can only be used on stand-alone switches that do not have any existing zoning defined on the switch.

To add or remove ports from a zone and to zone only the devices within a specific VSAN using Device Manager on the Cisco MDS 9124 Switch, follow these steps:

**Step 1**  
Choose **FC > Quick Config** or click the **Zone** icon in the toolbar.

You see the Quick Config Wizard (see Figure 30-5) with all controls disabled and the Discrepancies dialog box (see Figure 30-4), which shows all unsupported configurations.

**Note**  
You will see the Discrepancies dialog box only if there are any discrepancies.
Step 2  Click **OK** to continue.

You see the Quick Config Wizard dialog box shown in Figure 30-5.

⚠️ **Caution**

If there are discrepancies and you click **OK**, the affected VSANs in the zone databases are cleared. This may become disruptive if the switch is in use.
Step 3  Check the check box in the Ports Zoned To column for the port you want to add or remove from a zone. The check box for the matching port is similarly set. The selected port pair is added or removed from the zone, creating a two-device zone.

The VSAN drop-down menu provides a filter that enables you to zone only those devices within a selected VSAN.

Step 4  Right-click any of the column names to show or hide a column.

Step 5  Click Next to verify the changes.

You see the Confirm Changes dialog box shown in Figure 30-6.
Step 6 If you want to see the CLI commands, right-click in the dialog box and click CLI Commands from the pop-up menu.

Step 7 Click Finish to save the configuration changes.

Zone Configuration

This section describes how to configure zones and includes the following topics:

- About the Edit Local Full Zone Database Tool, page 30-11
- Configuring a Zone Using the Zone Configuration Tool, page 30-12
- Adding Zone Members, page 30-14
About the Edit Local Full Zone Database Tool

The Edit Local Full Zone Database tool allows you to zone across multiple switches and all zoning features are available through the Edit Local Full Zone Database dialog box (see Figure 30-7).

**Figure 30-7 Edit Local Full Zone Database Dialog Box**

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

---

**Note**

The Device Alias radio button is visible only if device alias is in enhanced mode. For more information, see “Creating a Device Alias” section on page 31-6.

---

**Tip**

Expand **Switches** from the Physical Attributes pane to retrieve the sWWN. If you do not provide a sWWN, the software automatically uses the local sWWN.
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.

Configuring a Zone Using the Zone Configuration Tool

To create a zone and move it into a zone set using Fabric Manager, follow these steps:

**Step 1**
Click the Zone icon in the toolbar (See Figure 30-8).

**Figure 30-8 Zone Icon**

You see the Select VSAN dialog box.

**Step 2**
Select the VSAN where you want to create a zone and click OK.
You see the Edit Local Full Zone Database dialog box shown in Figure 30-9.

**Figure 30-9 Edit Local Full Zone Database Dialog Box**

If you want to view zone membership information, right-click in the All Zone Membership(s) column, and then click Show Details for the current row or all rows from the pop-up menu.

**Step 3**
Click Zones in the left pane and click the Insert icon to create a zone.
You see the Create Zone dialog box shown in Figure 30-10.

**Figure 30-10  Create Zone Dialog Box**

Step 4 Enter a zone name.

Step 5 Check one of the following check boxes:

a. **Read Only**—The zone permits read and denies write.

b. **Permit QoS traffic with Priority**—You set the priority from the drop-down menu.

c. **Restrict Broadcast Frames to Zone Members**

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

If you want to move this zone into an existing zone set, skip to Step 8.

Step 7 Click **Zoneset** in the left pane and click the **Insert** icon to create a zone set.

You see the Zoneset Name dialog box shown in Figure 30-11.

**Figure 30-11  Zoneset Name Dialog Box**

Step 8 Enter a zone set name and click **OK**.

**Note** One of these symbols ($, -, ^, _) or all alphanumeric characters are supported. In interop mode 2 and 3, this symbol (_) or all alphanumeric characters are supported.

Step 9 Select the zone set where you want to add a zone and click the **Insert** icon or you can drag and drop Zone3 over Zoneset1.

You see the Select Zone dialog box shown in Figure 30-12.
Adding Zone Members

Once you create a zone, you can add members to the zone. You can add members using multiple port identification types.

To add a member to a zone using Fabric Manager, follow these steps:

**Step 1** Choose Zone > Edit Local Full Zone Database.

You see the Select VSAN dialog box.

**Step 2** Select a VSAN and click OK.

You see the Edit Local Full Zone Database dialog box for the selected VSAN.
Step 3  Select the members you want to add from the Fabric pane (see Figure 30-13) and click Add to Zone or click the zone where you want to add members and click the Insert icon.

You see the Add Member to Zone dialog box shown in Figure 30-14.

Figure 30-14   Add Member to Zone Dialog Box

Note The Device Alias radio button is visible only if device alias is in enhanced mode. For more information, see “Creating a Device Alias” section on page 31-6.

Step 4  Click the browse button and select a port name or check the LUN check box and click the browse button to configure LUNs.

Step 5  Click Add to add the member 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.

Zone Sets

This section describes zone sets and includes the following topics:

- About Zone Set Creation, page 30-16
- Activating a Zone Set, page 30-17
- Displaying Zone Membership Information, page 30-20
- About the Default Zone, page 30-20
- Configuring the Default Zone, page 30-21
• About FC Alias Creation, page 30-21
• Creating FC Aliases, page 30-22
• Adding Members to Aliases, page 30-22
• Converting Zone Members to pWWN-based Members, page 30-24
• Zone Enforcement, page 30-26

About Zone Set Creation

In Figure 30-15, two separate sets are created, each with its own membership hierarchy and zone members.

Figure 30-15  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).

Tip

Zone sets are configured with the names of the member zones and the VSAN (if the zone set is in a configured VSAN).
Activating a Zone Set

Changes to a zone set do not take effect in a full zone set until you activate it.
To activate an existing zone set using Fabric Manager, follow these steps:

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

**Step 2** Select a VSAN and click OK.
You see the Edit Local Full Zone Database dialog box for the selected VSAN.

**Step 3** Click Activate to activate the zone set.
You see the pre-activation check dialog box shown in Figure 30-16.

**Step 4** Click Yes to review the differences.
You see the Local vs. Active Differences dialog box shown in Figure 30-17.

**Step 5** Click Close to close the dialog box.
You see the Save Configuration dialog box shown in Figure 30-18.
Zone Sets

Step 6  Check the **Save Running to Startup Configuration** check box to save all changes to the startup configuration.

Step 7  Click **Continue Activation** to activate the zone set, or click **Cancel** to close the dialog box and discard any unsaved changes.

You see the Zone Log dialog box, which shows if the zone set activation was successful (see Figure 30-19).

**Deactivating a Zoneset**

To deactivate an existing zone set, follow these steps:

Step 1  Right-click the zone set you want to deactivate and then click **Deactivate** from the pop-up menu.

You see the Deactivate Zoneset dialog box as shown in Figure 30-20.
Step 2  Enter deactivate in the text box and then click **OK**.
You see the Input dialog box as shown in **Figure 30-21**.

**Figure 30-21  Input Dialog Box**

```
Input

Do you really want to deactivate Zoneset3?
(This will isolate all VSAN members)
Please Type 'DEACTIVATE' to confirm.

OK  Cancel
```

Step 3  Enter deactivate in the text box and then click **OK** to deactivate the zone set.

**Note**
To enable this option, you need to modify the server.properties file. See **Fabric Manager Server Properties File, page 3-4** to know more about modifying server.properties file.
Displaying Zone Membership Information

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

---

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

**Step 2** Select a VSAN and click OK.
You see the Edit Local Full Zone Database dialog box for the selected VSAN.

**Step 3** Click Zones in the left pane. 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 “Displaying Zone Information” section on page 30-42.

---

About 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.

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 view the active zone set.

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

To permit or deny traffic to members in the default zone using Fabric Manager, follow these steps:

**Step 1** Expand a and then select in the Fabric Manager Logical Domains pane.

**Step 2** Click the tab in the Information pane. You see the zone policies information in the Information pane (see Figure 30-22).

Figure 30-22  Default Zone Policies

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

**Step 3** In the Default Zone Behaviour field, choose either or from the drop-down menu.

About FC Alias Creation

You can assign an alias name and configure an alias member using the following values:

- **pWWN**—The WWN of the N or NL port is in hex format (for example, 10:00:00:23:45:67:89:ab).
- **fWWN**—The WWN of the fabric port name is in hex format (for example, 10:00:00:23:45:67:89:ab).
- **FC ID**—The N port ID is in 0xhhhhhh format (for example, 0xce00d1).
- **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.
- **IPv4 address**—The IPv4 address of an attached device is in 32 bits 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.
- **IPv6 address**—The IPv6 address of an attached device is in 128 bits in colon- (:) separated) hexadecimal format.
- **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.

Tip

The Cisco NX-OS software supports a maximum of 2048 aliases per VSAN.
Creating FC Aliases

To create an FC alias using Fabric Manager, follow these steps:

Step 1: Choose > . You see the Select VSAN dialog box.

Step 2: Select a VSAN and click . You see the Edit Local Full Zone Database dialog box for the selected VSAN.

Step 3: Click in the lower left pane (see Figure 30-23). The right pane lists the existing aliases.

Step 4: Click the icon to create an alias. You see the Create Alias dialog box shown in Figure 30-24.

Step 5: Set the Alias Name and the pWWN.

Step 6: Click to create the alias.

Adding Members to Aliases

To add a member to an alias using Fabric Manager, follow these steps:
**Step 1** Choose > .
You see the Select VSAN dialog box.

**Step 2** Select a VSAN and click .
You see the Edit Local Full Zone Database dialog box for the selected VSAN as shown in Figure 30-25.

*Figure 30-25  Edit Local Full Zone Database Dialog Box*

**Step 3** Select the member(s) you want to add from the Fabric pane (see Figure 30-25) and click or click the alias where you want to add members and click the icon.
You see the Add Member to Alias dialog box shown in Figure 30-26.
Zone Sets

Figure 30-26 Add Member to Alias Dialog Box

![Add Member to Alias Dialog Box]

**Note** The Device Alias radio button is visible only if device alias is in enhanced mode. For more information, see “Creating a Device Alias” section on page 31-6.

**Step 4** Click the browse button and select a port name or check the check box and click the browse button to configure LUNs.

**Step 5** Click to add the member to the alias.

---

**Converting Zone Members to pWWN-based Members**

You can convert zone and alias members from switch port or FC ID based membership 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** Choose > . You see the Select VSAN dialog box.

**Step 2** Select a VSAN and click. You see the Edit Local Full Zone Database dialog box for the selected VSAN.

**Step 3** Click the zone you want to convert.

**Step 4** Choose Tools Convert Switch Port/FCID members to By pWWN

**Step 5** Continue Conversion
Step 6

Yes

Note

Tip
copy

Caution

Caution

Note

Note enhanced
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.

### Zone Set Distribution

<table>
<thead>
<tr>
<th>One-Time Distribution</th>
<th>Full Zone Set Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 
- 
- 

### Enabling Full Zone Set Distribution
Enabling a One-Time Distribution

Step 1

Step 2

Step 3

Note - interop 1

interop 2

interop 3
About Recovering from Link Isolation

- Import the neighboring switch’s active zone set database and replace the current active zone set (see Figure 30-28).

Export the current database to the neighboring switch.

Manually resolve the conflict by editing the full zone set, activating the corrected zone set, and then bringing up the link.

To import or export the zone set information from or to an adjacent switch using Fabric Manager, follow these steps:

Choose > .

You see the Zone Merge Failure Recovery dialog box shown in Figure 30-29.
Zone Merge Failure Recovery Dialog Box

Zone Set Duplication

Caution
Copying Zone Sets

Step 1

Caution

About Backing Up and Restoring Zones
Backing Up Zones

Step 1

Step 2

Step 3
Chapter 30      Configuring and Managing Zones

Zone Set Duplication

Step 4

a. 

b. 

c. 

d. 

e. 

Step 5

Restoring Zones

Step 1

Step 2
Step 3

Step 4

a.

b.

c.
Renaming Zones, Zone Sets, and Aliases

Step 1

Step 2

Step 3

Step 4  > Rename
Cloning Zones, Zone Sets, FC Aliases, and Zone Attribute Groups

Step 1  Zone   Edit Local Full Zone Database
Step 2          OK.
Step 3    Edit   Clone

Migrating a Non-MDS Database

Step 1  Zone   Migrate Non-MDS Database
Advanced Zone Attributes

About Zone-Based Traffic Priority

To use this feature, you need to obtain the ENTERPRISE_PKG license see Chapter 10, “Obtaining and Installing Licenses” and you must enable QoS in the switch (see the “About Data Traffic” section on page 64-4).

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.

If zone-based QoS is implemented in a switch, you cannot configure the interop mode in that VSAN.
To configure the zone priority using Fabric Manager, follow these steps:

1. Expand a and then select a zone set in the Logical Domains pane.
2. Click the tab in the Information pane.
3. You see the Zone policy information in the Information pane (see Figure 30-37).

Use the check boxes and drop-down menus to configure QoS on the default zone.
4. Click to save the changes.

## Configuring Default Zone QoS Priority Attributes

**Note**

**Step 1**

**Step 2**

**Step 3**
Configuring the Default Zone Policy

Step 1

Step 2

Step 3

About Broadcast Zoning

Note
### Broadcasting Requirements

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Tip

- [Tip Text]

#### Caution

- [Caution Text]

### Configuring Broadcast Zoning

1. **Step 1**
2. **Step 2**
3. **Step 3**
4. **Step 4**
About LUN Zoning

Caution

Note

Note

LUN Zoning Access

Configuring a LUN-Based Zone

Step 1

Step 2
Step 3

Figure 30-42 Add Member to Zone Dialog Box

Assigning LUNs to Storage Subsystems

Note

Caution

About Read-Only Zones

- 
- 
-
Displaying Zone Information

Configuring Read-Only Zones

Step 1

Step 2

Step 3

Note

Displaying Zone Information

Step 1
### Enhanced Zoning

- 
- 
- 
- 
- 
- 
- 

**About Enhanced Zoning**

<table>
<thead>
<tr>
<th>Basic Zoning</th>
<th>Enhanced Zoning</th>
<th>Enhanced Zoning Advantages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Enhanced Zoning

Advantages of Enhanced Zoning (continued)

Changing from Basic Zoning to Enhanced Zoning

Step 1

Step 2

Tip

Changing from Enhanced Zoning to Basic Zoning

Step 1
## Enhanced Zoning

### Caution

1. In the enhanced zoning mode, the active zone set does not have a name in interop mode 1. The zone set names are only present for full zone sets.

### Analyzing a Zone Merge

#### Step 1

<table>
<thead>
<tr>
<th>Local Database</th>
<th>Adjacent Database</th>
<th>Merge Status</th>
<th>Results of the Merge</th>
</tr>
</thead>
<tbody>
<tr>
<td>different zones, aliases, and attributes groups.</td>
<td>1 <strong>but</strong> different zones, aliases, and attributes groups.</td>
<td>Successful.</td>
<td>The union of the local and adjacent databases.</td>
</tr>
<tr>
<td>The databases contains a zone, zone alias, or zone attribute group object with same name 1 but different members.</td>
<td>Failed.</td>
<td>ISLs are isolated.</td>
<td></td>
</tr>
<tr>
<td>Empty.</td>
<td>Contains data.</td>
<td>Successful.</td>
<td>The adjacent database information populates the local database.</td>
</tr>
<tr>
<td>Contains data.</td>
<td>Empty.</td>
<td>Successful.</td>
<td>The local database information populates the adjacent database.</td>
</tr>
</tbody>
</table>

1. **Caution**

   - 1. 
   - 2. 
   - 3. 
     - a. 
     - b. 

**Analyzing a Zone Merge**

---

**Step 1**
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 to analyze the zone merge.

Step 6 Click to clear the analysis data in the Zone Merge Analysis dialog box.

Configuring Zone Merge Control Policies

To configure merge control policies, refer to the .

Compacting the Zone Database for Downgrading
## Default Settings

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>