CHAPTER 7

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 includes the following sections:

Zoning Features

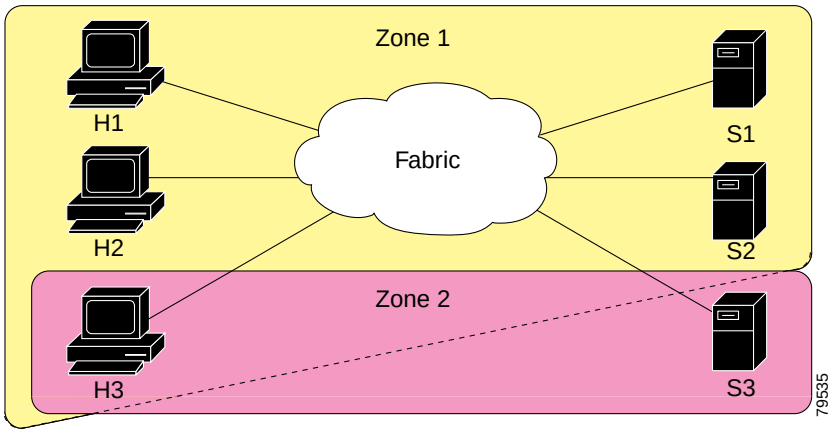
Zoning has the following features:

- 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 set (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 on Port world wide name (pWWN). The pWWN of an N port is attached to the switch as a member of the zone.
- 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

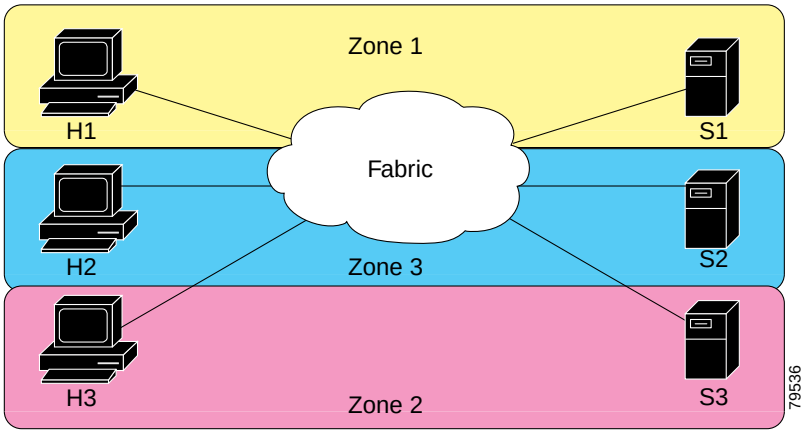
Figure 7-1 illustrates a zone set with two zones, zone 1 and zone 2, in a fabric. Zone 1 provides access from all three hosts (H1, H2, H3) to the data residing on storage systems S1 and S2. Zone 2 restricts the data on S3 to access only by H3. Note that H3 resides in both zones.

Figure 7-1 Fabric with Two Zones



Of course, there are other ways to partition this fabric into zones. Figure 7-2 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 7-2 Fabric with Three Zones



Zone Implementation

The Cisco MDS 9020 Fabric Switch automatically supports the following basic zone features (no additional configuration is required):

- Name server queries are soft-zoned.
- Only active zone sets are distributed.
- Unzoned devices cannot access each other.
- 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.
- Change the default policy for unzoned members.
- Bring E ports out of isolation.

Zone Configuration

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).
- FC alias—The alias name is in alphabetic characters (for example, Payroll) and denotes a WWN. The alias can also include multiple WWN members.

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 Inter-Switch Link (ISL) isolation. It is important to remove all non-pWWN-type zone entries prior to merging fabrics.

Configuring a Zone

To configure a zone and assign a zone name, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zone name Zone1` `switch(config-zone)#`	Creates a zone called Zone 1.

Step 3	`switch(config-zone)# member <type> <value>`
	`pWWN example:`
	`sswitch(config-zone)# member pwwn 10:00:00:23:45:67:89:ab`
	`FC alias example:`
	`switch(config-zone)# member fcalias Payroll`
		Configures a member for the specified zone (Zone1) based on the type (pWWN or FC alias) and value specified.

Tip	Use a relevant display command (for example, **show interface** or **show flogi database**) to obtain the required value in hex format.	

Alias Configuration

You can assign an alias name and configure an alias member using pWWN values.

Tip The Cisco MDS 9020 Fabric Switch supports a maximum of 2500 aliases.

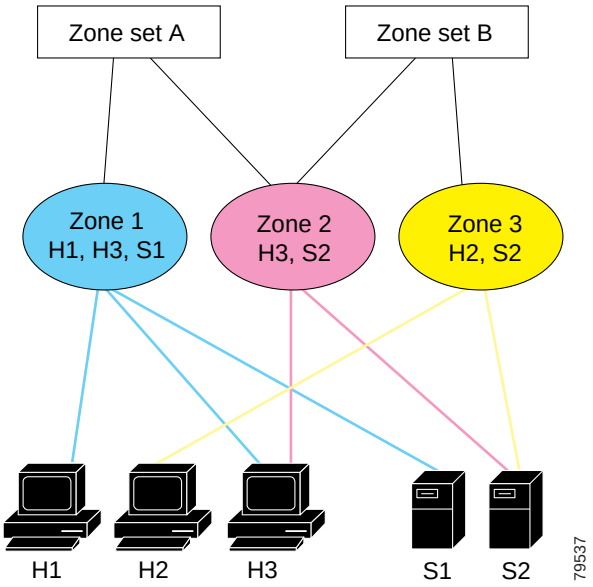
To create an alias using the **fcalias** command, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# fcalias name AliasSample` `switch-config-fcalias#`	Configures an alias name (AliasSample).
Step 3	`switch-config-fcalias# member pwwn 10:00:00:23:45:67:89:ab`	Configures alias members based on the specified port WWN type and value (pWWN 10:00:00:23:45:67:89:ab).

Zone Set Creation

In Figure 7-3, two separate sets are created, each with its own membership hierarchy and zone members.

Figure 7-3 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).

To create a zone set to include several zones, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zoneset name Zoneset1` `switch-config-zoneset#`	Configures a zone set called Zoneset1. **Tip** A zone set must have member zones before you can activate the zone set.
Step 3	`switch-config-zoneset# member Zone1`	Adds Zone1 as a member of the specified zone set (Zoneset1). **Tip** If the specified zone name was not previously configured, this command will return the `Zone not present` error message.
Step 4	`switch-config-zoneset# zone name InlineZone1` `switch-config-zoneset-zone#`	Adds a zone (InlineZone1) to the specified zone set (Zoneset1). **Tip** Execute this step only if you need to create a zone from a zone set prompt.

Active and Full Zone Set Considerations

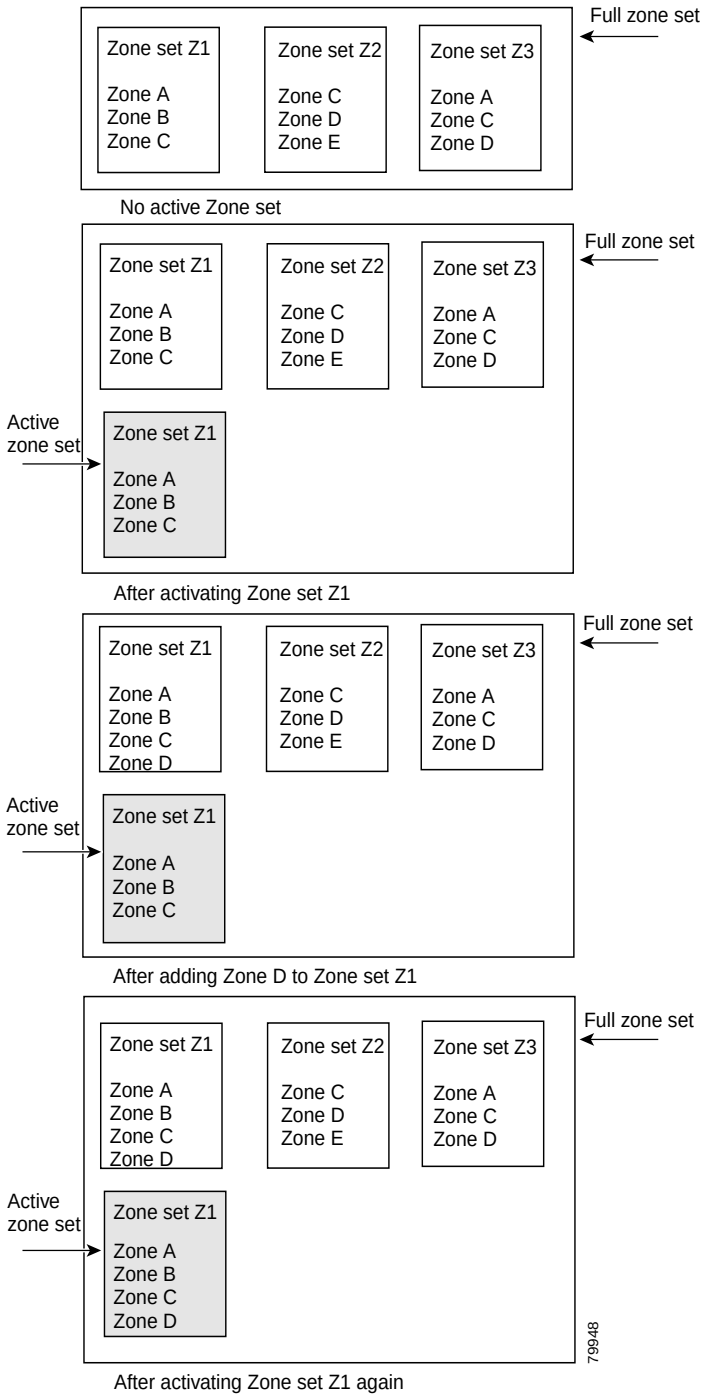
Before configuring a zone set, consider the following guidelines:

- 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.
- Soft zoning is implemented using the active zone set. Modifications take effect during zone set activation.

Note You must explicitly deactivate the currently active zone set before activating a new zone set.

Figure 7-4 shows a zone being added to an activated zone set.

Figure 7-4 Active and Full Zone Sets



Activating a Zone Set

You can activate a zone set using the **zoneset activate name** command. The changes to a full zone set do not take effect until the zone set is activated with the **zoneset activate name** command.

Tip You do not have to enter the **copy running-config startup-config** command to store the active zone set. However, you need to enter the **copy running-config startup-config** command to explicitly store full zone sets. It is not available across switch resets.

To activate a zone set, perform this task:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# zoneset activate name Zoneset1`	Activates the specified zone set.
	`switch(config)# no zoneset activate name Zoneset1`	Deactivates the specified zone set.

Zone Enforcement

Zoning is enforced in the form of soft zones. 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 of its zone, it cannot access those devices. 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.

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 or not 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.

To permit or deny traffic in the default zone, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zone default-zone permit`	Permits traffic flow to default zone members.
	`switch(config)# no zone default-zone permit`	Denies traffic flow to default zone members and reverts to factory default.

Full Zone Set Propagation

The Cisco MDS 9020 Fabric Switch distributes active zone sets when new E port links come up or when a new zone set is activated. The zone set distribution takes effect while sending merge requests to the adjacent switch or while activating a zone set.

The **zoneset distribute full** command in configuration mode distributes the full zone set along with the active zone set.

To propagate full zone sets to all switches, perform this task:

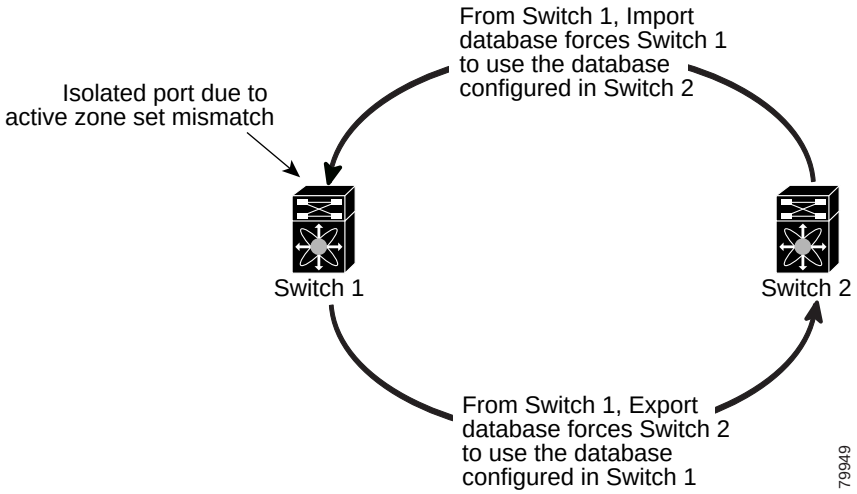
	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zoneset distribute full`	Enables sending a full zone set along with an active zone set.

Recovering from Link Isolation

When two switches in a fabric are merged using an E port, the E ports may become isolated when the active zone sets are different between the two switches or fabrics. When an E port becomes 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 7-5.)
- Export the current database to the neighboring switch. (See Figure 7-5.)
- Manually resolve the conflict by editing the full zone set, activating the corrected zone set, and then bringing up the link.

Figure 7-5 Importing and Exporting the Database



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.

Clearing the Zone Server Database

To clear the zone server database, use the **clear zone database** command:

```
switch# clear zone database
```

This command clears all configured information in the zone server.

Note After entering a **clear zone database** command, you need to explicitly enter the **copy running-config startup-config** to ensure that the running configuration is used when you next start the switch.

Renaming Zone Sets, Zones and, fcaliases

To rename a zone set, zone, or fcalias, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zoneset rename oldname newname`	Renames a zone set in the specified.
	`switch(config)# zone rename oldname newname`	Renames a zone in the specified.
	`switch(config)# fcalias rename oldname newname`	Renames a fcalias in the specified.

Displaying Zone Information

You can view any zone information by using the **show** command. If you request information for a specific object (for example, a specific zone, zone set, fcalias, or even a keyword like **brief** or **active**), only information for the specified object is displayed. If you do not request specific information, all available information is displayed. (See Examples 7-1 to 7-8.)

Example 7-1 Displays Zone Information

```
switch# show zone
zone name Z1
        pwwn 10:00:00:c0:dd:07:00:f8
        fcalias name A1
                  pwwn 10:00:00:c0:dd:07:00:f9
```

Use the **show zoneset** command to view the configured zone sets.

Example 7-2 Displays Configured Zone Set Information

```
switch# show zoneset
zoneset name ZS1
         zone name Z1
               pwwn 10:00:00:c0:dd:07:00:f8
               fcalias name A1
                         pwwn 10:00:00:c0:dd:07:00:f9
```

Use the **show zone name** command to display members of a specific zone.

Example 7-3 Displays Members of a Zone

```
switch# show zone name Zone1
zone name Z1
      pwwn 10:00:00:c0:dd:07:00:f8
      fcalias name A1
               pwwn 10:00:00:c0:dd:07:00:f9
```

Use the **show fcalias** command to display fcalias configuration.

Example 7-4 Displays fcalias Configuration

```
switch# show fcalias
fcalias name Alias2
```

```
fcalias name Alias1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:9c:48:e5
```

Use the **show zone member** command to display all zones to which a member belongs using the pWWN.

Example 7-5 Displays Membership Status

```
switch# show zone member pwwn 10:00:00:c0:dd:07:00:f9
fcalias name A1
          pwwn 10:00:00:c0:dd:07:00:f9
```

Example 7-6 Displays Active Zones

```
switch# show zone active
zone name zone1
  pwwn 10:11:22:33:44:55:66:77
  pwwn 10:11:22:33:44:55:66:88
  pwwn 10:11:22:33:44:55:66:99

zone name zone2
  pwwn 20:11:22:33:44:55:66:00
  pwwn 20:11:22:33:44:55:66:01
  pwwn 20:11:22:33:44:55:66:02
  pwwn 20:11:22:33:44:55:66:03
```

Example 7-7 Displays Active Zone Sets

```
switch# show zoneset active
zoneset name circus
  zone name bozo
    pwwn 10:11:22:33:44:55:66:77
    pwwn 10:11:22:33:44:55:66:88
    pwwn 10:11:22:33:44:55:66:99

  zone name clown
    pwwn 20:11:22:33:44:55:66:00
    pwwn 20:11:22:33:44:55:66:01
    pwwn 20:11:22:33:44:55:66:02
    pwwn 20:11:22:33:44:55:66:03
```

Example 7-8 Displays Zone Status

```
switch# show zone status
Full Zoning Database :
        Zonesets: 1 Zones: 1 Aliases: 1
        Active Zoning Database:
                Name: ZS1 Zonesets: 1 Zones: 1
                Status:
```

Merging the Database

The merge behavior is governed by the merge rules specified in Table 7-1.

Table 7-1 Database Zone Merge Status

Local Database	Adjacent Database	Merge Status	Results of the Merge
The databases contain zone sets with the same name but different zones, aliases, and attributes groups.		Successful.	The union of the local and adjacent databases.
The databases contains a zone, zone alias, or zone attribute group object with same name but different members.		Failed.	ISLs are isolated.
Empty.	Contains data.	Successful.	The adjacent database information populates the local database.
Contains data.	Empty.	Successful.	The local database information populates the adjacent database.

Caution Remove all non-pWWN-type zone entries on all MDS switches running Cisco SAN-OS prior to merging fabrics if there is a Cisco MDS 9020 switch running FabricWare in the adjacent fabric to avoid Inter-Switch Link (ISL) isolation.

Default Zone Policies

To permit or deny traffic in the default zone, perform this task:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zone default-zone permit`	Permits traffic flow to default zone members.
	`switch(config)# no zone default-zone permit`	Denies traffic flow to default zone members and reverts to factory default.

Default Settings

Table 7-2 lists the default settings for basic zone parameters.

Table 7-2 Default Basic Zone Parameters

Parameters	Default
Default zone policy	Denied to all members.
Full zone set distribute	The full zone set(s) is not distributed.