CHAPTER 12

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 and includes the following sections:

Table 8-1 on page 8-4 lists the differences between zones and VSANs.

Note For a comprehensive summary of zone implementation, refer to the "Zone Implementation" section on page 12-16.

Zoning Features

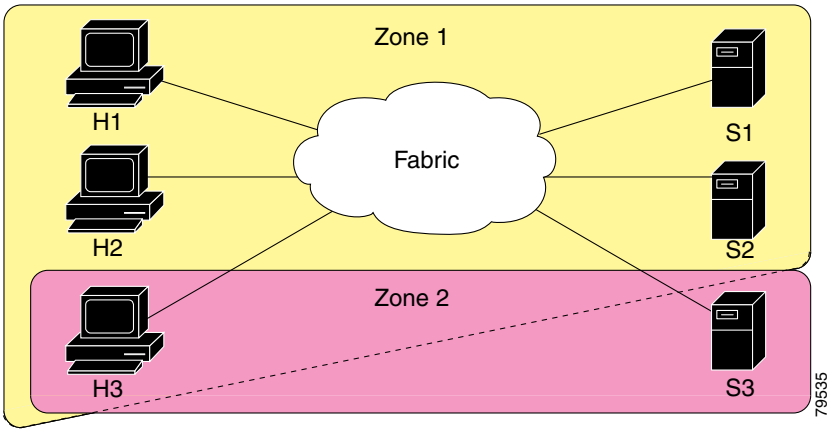
Zoning has the following features:

- 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 (**zoneset distribute full vsan** command) 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 configured 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.
- 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

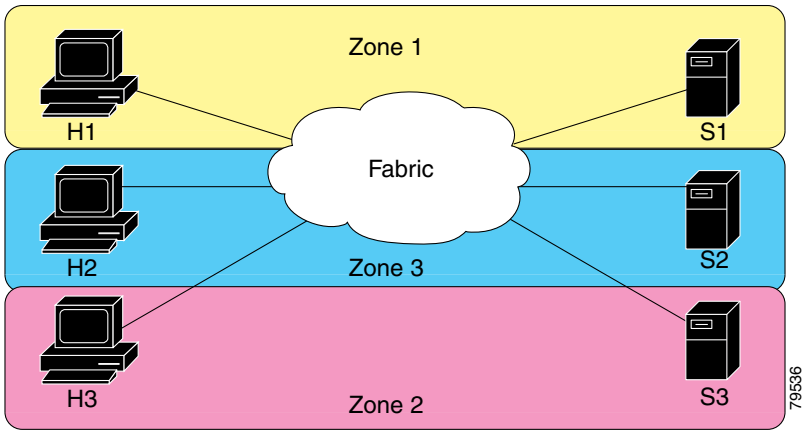
Figure 12-1 illustrates a zone set with two zones, zone 1 and zone 2, in a fabric. Zone 1 provides access from all three hosts (H1, H2, H3) to the data residing on storage systems S1 and S2. Zone 2 restricts the data on S3 to access only by H3. Note that H3 resides in both zones.

Figure 12-1 Fabric with Two Zones



Of course, there are other ways to partition this fabric into zones. Figure 12-2 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 12-2 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.

To configure a zone and assign a zone name, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zone name Zone1 vsan 3` `switch(config-zone)#`	Configures a zone called Zone 1 for the VSAN called vsan3.

Step 3	`switch(config-zone)# member <type> <value>`
	`pWWN example:`
	`sswitch(config-zone)# member pwwn 10:00:00:23:45:67:89:ab`
	`Fabric pWWN example:`
	`switch(config-zone)# member fwwn 10:01:10:01:10:ab:cd:ef`
	`FC ID example:`
	`switch(config-zone)# member fcid 0xce00d1`
	`FC alias example:`
	`switch(config-zone)# member fcalias Payroll`
		Configures a member for the specified zone (Zone1) based on the type (pWWN, fabric pWWN, FC ID, 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.

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.

To create an alias using the **fcalias** command, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# fcalias name AliasSample vsan 3` `switch-config-fcalias#`	Configures an alias name (AliasSample).
Step 3	`switch-config-fcalias# member fcid 0x222222` `switch-config-fcalias#`	Configures alias members based on the specified FC ID type and value (0x222222).
	`switch-config-fcalias# member pwwn 10:00:00:23:45:67:89:ab` `switch-config-fcalias#`	Configures alias members based on the specified port WWN type and value (pWWN 10:00:00:23:45:67:89:ab).
	`switch-config-fcalias# member fwwn 10:01:10:01:10:ab:cd:ef` `switch-config-fcalias#`	Configures alias members based on the specified fWWN type and value (fWWN 10:01:10:01:10:ab:cd:ef).

Note Multiple members can be specified on multiple lines.

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.

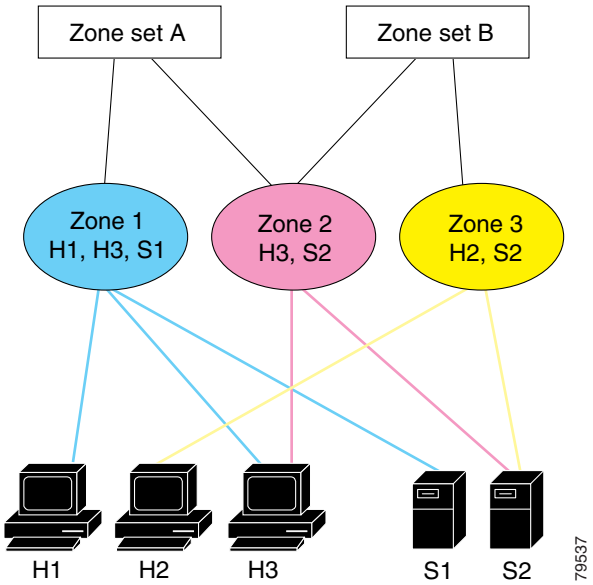
Note Hard zoning enforces zoning restrictions on every frame, and it prevents unauthorized access at all times.

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

Zone Sets

In Figure 12-3, two separate sets are created, each with its own membership hierarchy and zone members.

Figure 12-3 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 both at once).

To create a zone set to include several zones, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zoneset name Zoneset1 vsan 3` `switch-config-zoneset#`	Configures a zone set called Zoneset1. **Note** To activate a zone set, you must first create the zone and a zone set.
Step 3	`switch-config-zoneset# member Zone1` `switch-config-zoneset#`	Adds Zone1 as a member of the specified zone set (Zoneset1). **Note** 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.
Step 5	`switch-config-zoneset-zone# member fcid 0x111112` `switch-config-zoneset-zone#`	Adds a new member (FC ID 0x111112) to the newly created zone (InlineZone1). **Tip** Execute this step only if you need to add a member to a zone from a zone set prompt. **Note** Multiple members can be specified on multiple lines.

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

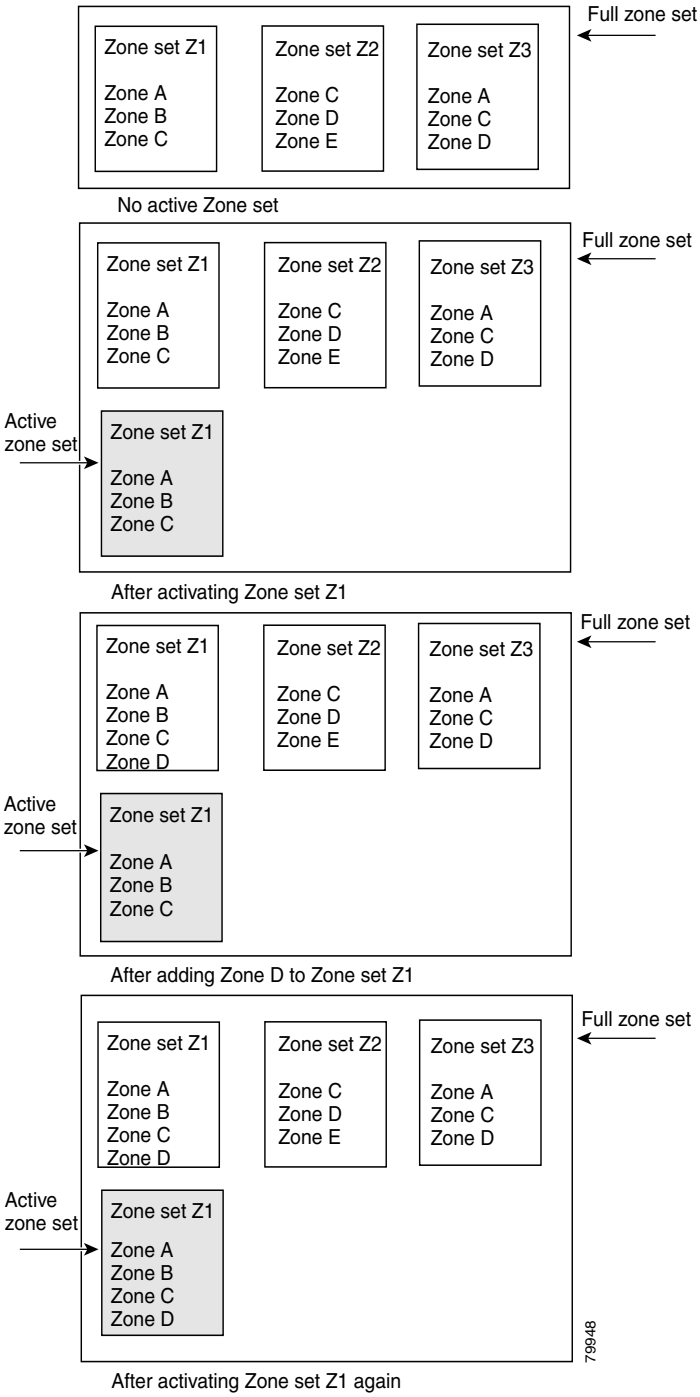
Before configuring a zone set, consider the following guidelines:

- 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. You can activate a zone set using the **zoneset activate name** command.
- 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 with the **zoneset activate name** command.

- 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. You do not have to issue the **copy running-config startup-config** command to store the active zone set. However, you need to issue the **copy running-config startup-config** command to explicitly store full zone sets. It is not available 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 12-4 shows a zone being added to an activated zone set.

Figure 12-4 Active and Full Zone Sets



To activate a zone set, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.

	Command	Purpose
Step 2	`switch(config)# zoneset activate name Zoneset1 vsan 3` `switch(config)#`	Activates the specified zone set.
	`switch(config)# no zoneset activate name Zoneset1 vsan 3` `switch(config)#`	Deactivates the specified zone set

Note 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.

A 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 a 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 be permitted or denied to members of the default zone. This information is not distributed to all switches; it must be performed for 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. The default zone members are explicitly listed only when the default policy is configured as **permit**. When the default policy is configured as **deny**, the members of this zone are not explicitly enumerated when you issue the **show zoneset active** command.

To permit or deny traffic in the default zone, follow these steps:

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

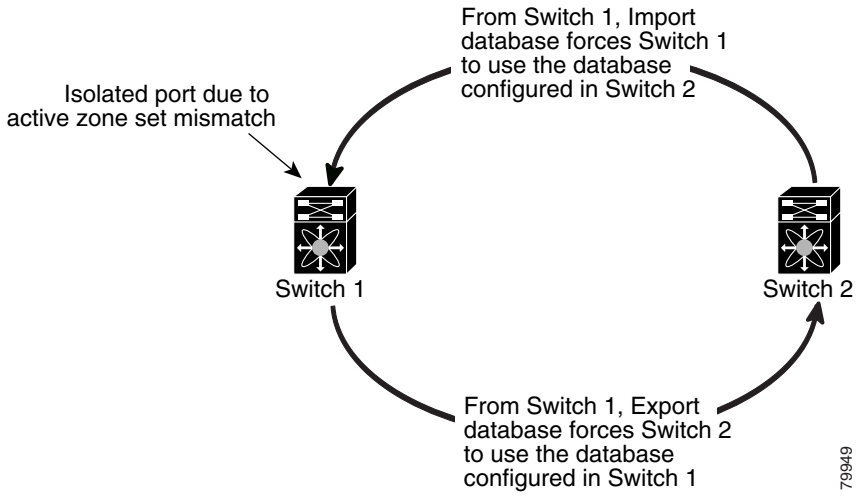
Note The default settings for default zone configurations can be changed.

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 zoneset 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 zoneset database and replace the current active zoneset (see Figure 12-5).
- Export the current database to the neighboring switch (see Figure 12-5).
- Manually resolve the conflict by editing the full zone set, bringing up the link, and then activating the corrected zone set.

Figure 12-5 Importing and Exporting the Database



Tip The **import** and **export** commands should be issued from a single switch. Importing from one switch and exporting from another switch can lead to isolation again.

To import the zone database from an adjacent switch, follow these steps:

	Command	Purpose
Step 1	`switch# zone merge interface fc1/3 import vsan2`	Imports the zone database from the adjacent switch connected through the VSAN 2 interface.
	`switch# zone merge interface fc2/8 export vsan5`	Exports the zone database from the adjacent switch connected through the VSAN 5 interface.

Note You can also issue **zone merge interface** commands for a range of VSANs.

Distributing Zone Sets

When a zone set is activated, by default, only the active zone set is sent to other switches in the Fabric. This command enables sending a full zone set along with the active zone set. It takes effect while sending merge request frame to the adjacent switch.

To distribute zone sets, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zoneset distribute full vsan 33`	Enables sending a full zone set along with an active zone set.

Copying Zone Sets

You can copy an active zone set to a full zone set using the **zone copy active-zoneset full-zoneset** command. You can not make changes to an existing zone set and activate it, if the full zone set is lost or is not propagated. This command does not distribute zone sets.

Note Since you can not edit an active zone set, this command is helpful in changing a copy of an existing zone set. You can make a copy and then edit it without altering the existing active zone set.

The **zone copy** command is used to copy active zone sets to the full zone set.

To distribute zone sets, follow this step:

	Command	Purpose
Step 1	`switch# zone copy active-zoneset full-zoneset` `Please enter yes to proceed.(y/n) [n]? y`	Makes a copy of the active zone set in the full zone set.

Clearing Zone Sets

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

To clear the zone server database, follow these steps:

	Command	Purpose
Step 1	`switch# clear zone database vsan2`	Clears all configured information in the zone server for the specified VSAN.

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

Viewing Zone Information

You can view any zone information for any configured interface by using the **show** command. If you request information for a specific object (for example, a specific zone, zone set, VSAN, alias, 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 12-1 to 12-12.

Example 12-1 Displays Zone Information for All VSANs

```
switch(config)# show zone
zone name Zone3 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:9c:48:e5

zone name Zone2 vsan 2
  fwwn 20:41:00:05:30:00:2a:1e
  fwwn 20:42:00:05:30:00:2a:1e
  fwwn 20:43:00:05:30:00:2a:1e

zone name Zone1 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:a6:be:2f
  pwwn 21:00:00:20:37:9c:48:e5
  fcalias Alias1
```

Example 12-2 Displays Zone Information for a Specific VSAN.

```
switch(config)# show zone vsan 1
zone name Zone3 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:9c:48:e5

zone name Zone2 vsan 1
    fwwn 20:4f:00:05:30:00:2a:1e
    fwwn 20:50:00:05:30:00:2a:1e
    fwwn 20:51:00:05:30:00:2a:1e
    fwwn 20:52:00:05:30:00:2a:1e
    fwwn 20:53:00:05:30:00:2a:1e

zone name Zone1 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:a6:be:2f
  pwwn 21:00:00:20:37:9c:48:e5
  fcalias Alias1
```

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

Example 12-3 Display Configured Zone Set Information:

```
switch# show zoneset vsan 1
zoneset name ZoneSet2 vsan 1
  zone name Zone2 vsan 1
    fwwn 20:4e:00:05:30:00:2a:1e
    fwwn 20:4f:00:05:30:00:2a:1e
    fwwn 20:50:00:05:30:00:2a:1e
    fwwn 20:51:00:05:30:00:2a:1e
    fwwn 20:52:00:05:30:00:2a:1e

  zone name Zone1 vsan 1
    pwwn 21:00:00:20:37:6f:db:dd
```

```
    pwwn 21:00:00:20:37:a6:be:2f
    pwwn 21:00:00:20:37:9c:48:e5
    fcalias Alias1

zoneset name ZoneSet1 vsan 1
  zone name Zone1 vsan 1
    pwwn 21:00:00:20:37:6f:db:dd
    pwwn 21:00:00:20:37:a6:be:2f
    pwwn 21:00:00:20:37:9c:48:e5
    fcalias Alias1
```

Example 12-4 Display Configured Zone Set Information for a Range of VSANs:

```
switch# show zoneset vsan 2-3
zoneset name ZoneSet2 vsan 2
  zone name Zone2 vsan 2
    fwwn 20:52:00:05:30:00:2a:1e
    fwwn 20:53:00:05:30:00:2a:1e
    fwwn 20:54:00:05:30:00:2a:1e
    fwwn 20:55:00:05:30:00:2a:1e
    fwwn 20:56:00:05:30:00:2a:1e

  zone name Zone1 vsan 2
    pwwn 21:00:00:20:37:6f:db:dd
    pwwn 21:00:00:20:37:a6:be:2f
    pwwn 21:00:00:20:37:9c:48:e5
    fcalias Alias1

zoneset name ZoneSet3 vsan 3
  zone name Zone1 vsan 1
    pwwn 21:00:00:20:37:6f:db:dd
    pwwn 21:00:00:20:37:a6:be:2f
    pwwn 21:00:00:20:37:9c:48:e5
    fcalias Alias1
```

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

Example 12-5 Displays Members of a Zone

```
switch# show zone name Zone1
zone name Zone1 vsan 1
  pwwn 21:00:00:20:37:6f:db:dd
  pwwn 21:00:00:20:37:a6:be:2f
  pwwn 21:00:00:20:37:9c:48:e5
  fcalias Alias1
```

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

Example 12-6 Displays fcalias Configuration

```
switch# show fcalias vsan 1
fcalias name Alias2 vsan 1

fcalias name Alias1 vsan 1
  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 FC ID.

Example 12-7 Displays Membership Status

```
switch# show zone member pwwn 21:00:00:20:37:9c:48:e5
           VSAN: 1
zone Zone3
zone Zone1
fcalias Alias1
```

Use the **show zone statistics** command to display the number of control frames exchanged with other switches.

Example 12-8 Displays Zone Statistics

```
switch# show zone statistics
Statistics For VSAN: 1
**********************************
Number of Merge Requests Sent: 24
Number of Merge Requests Recvd: 25
Number of Merge Accepts Sent: 25
Number of Merge Accepts Recvd: 25
Number of Merge Rejects Sent: 0
Number of Merge Rejects Recvd: 0
Number of Change Requests Sent: 0
Number of Change Requests Recvd: 0
Number of Change Rejects Sent: 0
Number of Change Rejects Recvd: 0
Number of GS Requests Recvd: 0
Number of GS Requests Rejected: 0
Statistics For VSAN: 2
**********************************
Number of Merge Requests Sent: 4
Number of Merge Requests Recvd: 4
Number of Merge Accepts Sent: 4
Number of Merge Accepts Recvd: 4
Number of Merge Rejects Sent: 0
Number of Merge Rejects Recvd: 0
Number of Change Requests Sent: 0
Number of Change Requests Recvd: 0
Number of Change Rejects Sent: 0
Number of Change Rejects Recvd: 0
Number of GS Requests Recvd: 0
Number of GS Requests Rejected: 0
```

Example 12-9 Displays Active Zonesets

```
switch# show zoneset active
zoneset name ZoneSet1 vsan 1
  zone name zone1 vsan 1
    fcid 0x080808
    fcid 0x090909
    fcid 0x0a0a0a
  zone name zone2 vsan 1
  * fcid 0xef0000 [pwwn 21:00:00:20:37:6f:db:dd]
  * fcid 0xef0100 [pwwn 21:00:00:20:37:a6:be:2f]
```

Example 12-10 Displays Brief Descriptions of Zone Sets

```
switch# show zoneset brief
zoneset name ZoneSet1 vsan 1
  zone zone1
  zone zone2
```

Example 12-11 Displays Active Zones

```
switch# show zone active
zone name zone1 vsan 1
  fcid 0x080808
  fcid 0x090909
  fcid 0x0a0a0a

zone name zone2 vsan 1
* fcid 0xef0000 [pwwn 21:00:00:20:37:6f:db:dd]
* fcid 0xef0100 [pwwn 21:00:00:20:37:a6:be:2f]
```

Example 12-12 Displays Zone Status

```
switch# show zone status
VSAN: 1 default-zone: deny distribute: full Interop: Off
Full Zoning Database :
    Zonesets:1  Zones:11  Aliases:0
Active Zoning Database :
    Name: zoneset-1  Zonesets:1  Zones:11  Aliases:0
Status: Activation completed at Thu Feb 13 10:22:34 2003

VSAN: 2 default-zone: deny distribute: full Interop: Off
Full Zoning Database :
    Zonesets:1  Zones:10  Aliases:0
Active Zoning Database :
    Name: zoneset-2  Zonesets:1  Zones:10  Aliases:0
Status: Activation completed at Thu Feb 13 10:23:12 2003

VSAN: 3 default-zone: deny distribute: full Interop: Off
Full Zoning Database :
    Zonesets:1  Zones:10  Aliases:0
Active Zoning Database :
    Name: zoneset-3  Zonesets:1  Zones:10  Aliases:0
Status: Activation completed at Thu Feb 13 10:23:50 2003
```

Default Settings

Table 12-1 lists the default settings for zone parameters.

Table 12-1 Default Zone Parameters

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

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 changed (more secure).
- 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 zonesets 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

You can additionally configure the following zone features if required:

- Propagate full zone sets to all switches on a per VSAN basis using the **zoneset distribute full-database vsan** command.
- Change the default policy for unzoned members using the **zone default permit vsan** command.
- Inter-operate with other vendors by configuring a VSAN in the interop mode using the **vsan 1 interop** command.
  - 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 using the **export** or **import** commands