CHAPTER 3

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:

Note Table 2-1 on page 2-4 lists the differences between zones and VSANs.

About Zoning

Zoning has the following features:

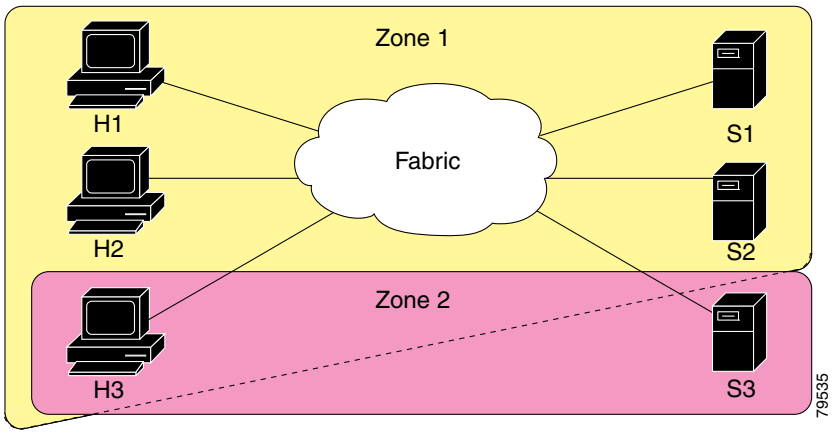
- A zone consists of multiple zone members.
  - Members in a zone can access each other; members in different zones cannot access each other.
  - If zoning is not activated, all devices are members of the default zone.
  - If zoning is activated, any device that is not in an active zone (a zone that is part of an active zone set) is a member of the default zone.

  - Zones can vary in size.
  - Devices can belong to more than one zone.
  - A physical fabric can have a maximum of 16,000 members. This includes all VSANs in the fabric.
- 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.
  - 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

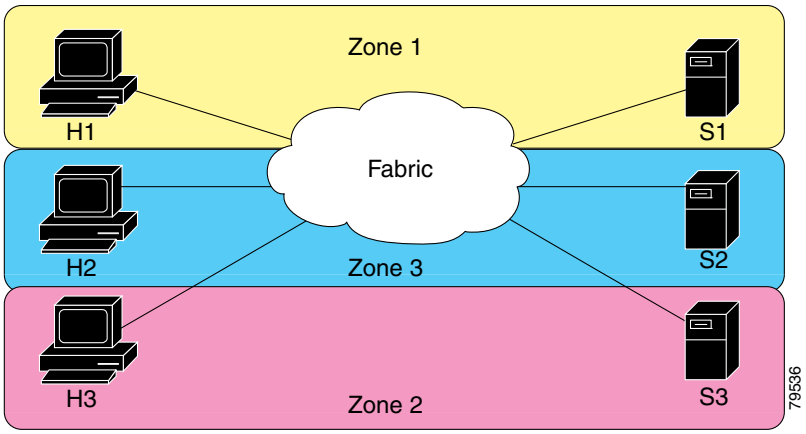
Figure 3-1 illustrates a zone set with two zones, zone 1 and zone 2, in a fabric. Zone 1 provides access from all three hosts (H1, H2, H3) to the data residing on storage systems S1 and S2. Zone 2 restricts the data on S3 to access only by H3. Note that H3 resides in both zones.

Figure 3-1 Fabric with Two Zones



Of course, there are other ways to partition this fabric into zones. Figure 3-2 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 3-2 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 numbers of targets or large numbers of initiators in a single zone. This type of configuration wastes switch resources by provisioning and managing many communicating pairs (initiator-to-initiator or target-to-target) that will never actually communicate with each other. For this reason, a 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 the 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:

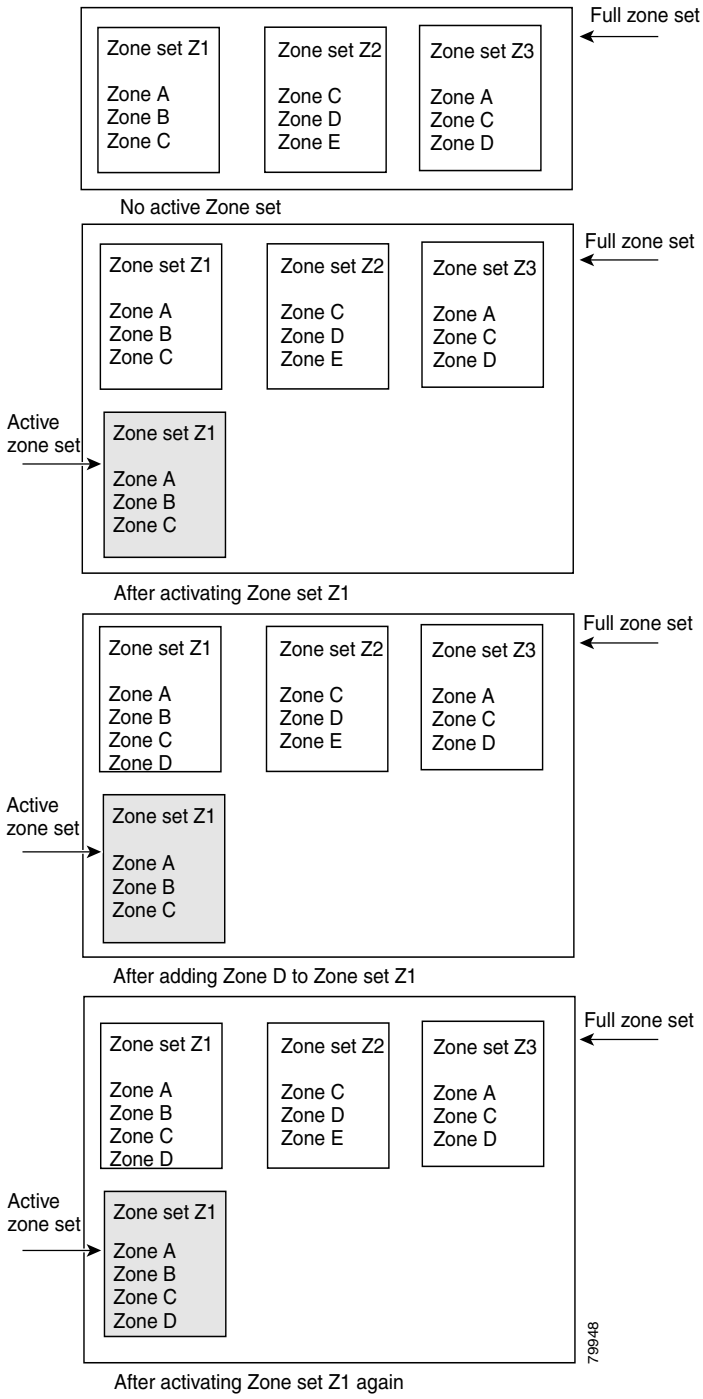
- Each VSAN can have multiple zone sets but only one zone set can be active at any given time.
- When you create a zone set, that zone set becomes a part of the full zone set.
- When you activate a zone set, a copy of the zone set from the full zone set is used to enforce zoning, and is called the active 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 3-3 shows a zone being added to an activated zone set.

Figure 3-3 Active and Full Zone Sets



Zone Configuration

This section describes how to configure zones and includes the following topic(s):

- Configuring a Zone, page 3-7

Configuring a Zone

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 Zone1 for the VSAN called vsan3. **Note** All alphanumeric characters or one of the following symbols ($, -, ^, _) are supported.

Step 3	`switch(config-zone)# member` *type value*
	`pWWN example:`
	`switch(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`
	`Domain ID example:`
	`switch(config-zone)# member domain-id 2 portnumber 23`
	`IPv4 address example:`
	`switch(config-zone)# member ip-address 10.15.0.0 255.255.0.0`
	`IPv6 address example:`
	`switch(config-zone)# member ipv6-address 2001::db8:800:200c:417a/64`
	`Local sWWN interface example:`
	`switch(config-zone)# member interface fc 2/1`
	`Remote sWWN interface example:`
	`switch(config-zone)# member interface fc2/1 swwn 20:00:00:05:30:00:4a:de`
	`Domain ID interface example:`
	`switch(config-zone)# member interface fc2/1 domain-id 25`
		Configures a member for the specified zone (Zone1) based on the type (pWWN, fabric pWWN, FC ID, fcalias, domain ID, IPv4 address, IPv6 address, or interface) and value specified.
		Caution You must only configure pWWN-type zoning on all MDS switches running Cisco SAN-OS if there is a Cisco MDS 9020 switch running FabricWare in the same fabric.

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

Tip Use the **show wwn switch** command 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.

Zone Sets

Zones provide a mechanism for specifying access control, while zone sets are a grouping of zones to enforce access control in the fabric.

This section describes zone sets and includes the following topics:

About Zone Sets

Zones provide a mechanism for specifying access control, while zone sets are a grouping of zones to enforce access control in the fabric.

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

Zone Set Distribution—You can distribute full zone sets using one of two methods: one-time distribution or full zone set distribution.

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

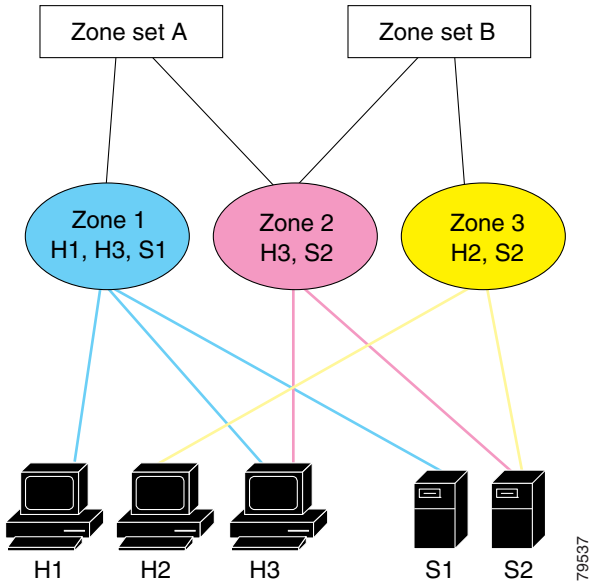
- To the full zone set
- To a remote location (using FTP, SCP, SFTP, or TFTP)

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

About Zone Set Creation

In Figure 3-4, two separate sets are created, each with its own membership hierarchy and zone members.

Figure 3-4 Hierarchy of Zone Sets, Zones, and Zone Members



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 or deactivate an existing zone set, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# zoneset activate name Zoneset1 vsan 3`	Activates the specified zone set.
	`switch(config)# no zoneset activate name Zoneset1 vsan 3`	Deactivates the specified zone set.

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 issue the **show zoneset active** command.

Note The current default zoning policy in both the switches are deny. In MDS9222i the active zoneset is "coco_isola_zoneset". In MDS 9513, there is no active zoneset, but because default zoning policy is deny, the hidden active zoneset is "d__efault__cfg". Thus zone merge is failing. The behavior is even same between two brocade switches.

Configuring the Default Zone Access Permission

To permit or deny traffic to members 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`	Permits traffic flow to default zone members.
	`switch(config)# no zone default-zone permit vsan 1`	Denies (default) traffic flow to default zone members.

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 alias, 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).

	Command	Purpose
Step 3	switch(config-fcalias)# **member** *type value* pWWN example: switch(config-fcalias)# **member pwwn 10:00:00:23:45:67:89:ab** fWWN example: switch(config-fcalias)# **member fwwn 10:01:10:01:10:ab:cd:ef** FC ID example: switch(config-fcalias)# **member fcid 0x222222** Domain ID example: switch(config-fcalias)# **member domain-id 2 portnumber 23** IPv4 address example: switch(config-fcalias)# **member ip-address 10.15.0.0 255.255.0.0** IPv6 address example: switch(config-fcalias)# **member ipv6-address 2001::db8:800:200c:417a/64** Local sWWN interface example: switch(config-fcalias)# **member interface fc 2/1** Remote sWWN interface example: switch(config-fcalias)# **member interface fc2/1 swwn 20:00:00:05:30:00:4a:de** Domain ID interface example: switch(config-fcalias)# **member interface fc2/1 domain-id 25**	Configures a member for the specified fcalias (AliasSample) based on the type (pWWN, fabric pWWN, FC ID, domain ID, IPv4 address, IPv6 address, or interface) and value specified.
Step 4	**Note** Multiple members can be specified on multiple lines.	

Creating Zone Sets and Adding Member Zones

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)# **zone*set* name Zoneset1 vsan 3** switch(config-zoneset)#	Configures a zone set called Zoneset1. **Tip** To activate a zone set, you must first create the zone and a 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.

	Command	Purpose
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 new zone (InlineZone1). **Tip** Execute this step only if you need to add a member to a zone from a zone set prompt.

Tip 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.

Caution If you deactivate the active zone set in a VSAN that is also configured for IVR, the active IVR zone set (IVZS) is also deactivated and all IVR traffic to and from the switch is stopped. This deactivation can disrupt traffic in more than one VSAN. Before deactivating the active zone set, check the active zone analysis for the VSAN (see the "Zone and Zone Set Analysis" section on page 3-46). To reactivate the IVZS, you must reactivate the regular zone set (refer to the *Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide*).

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

Note Set the device alias mode to **enhanced** when using SDV (because the pWWN of a virtual device could change).

For example, SDV is enabled on a switch and a virtual device is defined. SDV assigns a pWWN for the virtual device, and it is zoned based on the pWWN in a zone. If you later disable SDV, this configuration is lost. If you reenable SDV and create the virtual device using the same name, there is no guarantee that it will get the same pWWN again. You will have to rezone the pWWN-based zone. However, if you perform zoning based on the device-alias name, there are no configuration changes required if or when the pWWN changes.

Be sure you understand how device alias modes work before enabling them. Refer to Chapter 5, "Distributing Device Alias Services" for details and requirements about device alias modes.

Zone Enforcement

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

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

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

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

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

Zone Set Distribution

You can distribute full zone sets using one of two methods: one-time distribution at the EXEC mode level or full zone set distributionat the configuration mode level.

Table 3-1 lists the differences between these distribution methods.

Table 3-1 zoneset distribution Command Differences

zoneset distribute vsan Command (EXEC Mode)	zoneset distribute full vsan Command (Configuration Mode)
Distributes the full zone set immediately.	Does not distribute the full zone set immediately.
Does not distribute the full zone set information along with the active zone set during activation, deactivation, or merge process.	Remembers to distribute the full zone set information along with the active zone set during activation, deactivation, and merge processes.

This section describes zone set distribution and includes the following topics:

Enabling Full Zone Set Distribution

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

To enable full zone set and active zone set distribution to all switches on a per VSAN basis, 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.

Enabling a One-Time Distribution

Use the **zoneset distribute vsan** *vsan-id* command in EXEC mode to perform this distribution.

```
switch# zoneset distribute vsan 2
Zoneset distribution initiated. check zone status
```

This command only distributes the full zone set information; it does not save the information to the startup configuration. You must explicitly issue the **copy running-config startup-config** command to save the full zone set information to the startup configuration.

Note The **zoneset distribute vsan** *vsan-id* command is supported in **interop 2** and **interop 3** modes, not in **interop 1** mode.

Use the **show zone status vsan** *vsan-id* command to check the status of the one-time zone set distribution request.

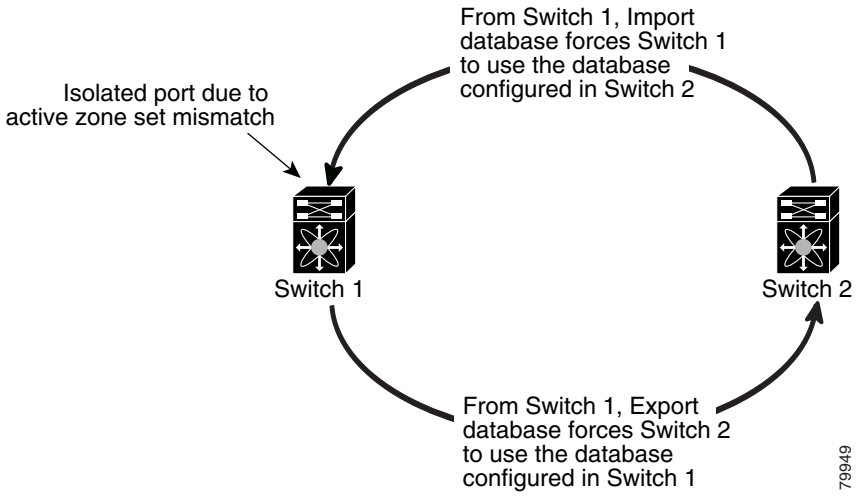
```
switch# show zone status vsan 2
VSAN: 3 default-zone: permit distribute: active only Interop: 100
    mode:basic merge-control:allow session:none
    hard-zoning:enabled
Default zone:
    qos:low broadcast:disabled ronly:disabled
Full Zoning Database :
    Zonesets:0  Zones:0 Aliases: 0
Active Zoning Database :
    Name: nozoneset  Zonesets:1  Zones:2
Status: Zoneset distribution completed at 04:01:06 Aug 28 2004
```

About Recovering from Link Isolation

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

- Import the neighboring switch's active zone set database and replace the current active zone set (see Figure 3-5).
- 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.

Figure 3-5 Importing and Exporting the Database



Importing and Exporting Zone Sets

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

	Command	Purpose
Step 1	`switch# zoneset import interface fc1/3 vsan 2`	Imports the zone set from the adjacent switch connected through the fc 1/3 interface for VSAN 2.
	`switch# zoneset import interface fc1/3 vsan 2-5`	Imports the zone set from the adjacent switch connected through the fc 1/3 interface for VSANs ranging from 2 through 5.
Step 2	`switch# zoneset export vsan 5`	Exports the zone set to the adjacent switch connected through VSAN 5.
	`switch# zoneset export vsan 5-8`	Exports the zone set to the adjacent switch connected through the range of VSANs 5 through 8.

Note Issue the **import** and **export** commands from a single switch. Importing from one switch and exporting from another switch can lead to isolation again.

Zone Set Duplication

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

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

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

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.

This section includes the following topics:

Copying Zone Sets

On the Cisco MDS Family switches, you cannot edit an active zone set. However, you can copy an active zone set to create a new zone set that you can edit.

To make a copy of a zone set, follow this step:

	Command	Purpose
Step 1	`switch# zone copy active-zoneset full-zoneset vsan 2` `Please enter yes to proceed.(y/n) [n]? y`	Makes a copy of the active zone set in VSAN 2 to the full zone set.
	`switch# zone copy vsan 3 active-zoneset scp://guest@myserver/tmp/active_zoneset.txt`	Copies the active zone in VSAN 3 to a remote location using SCP.

Caution If the Inter-VSAN Routing (IVR) feature is enabled and if IVR zones exist in the active zone set, then a zone set copy operation copies all the IVR zones to the full zone database. To prevent copying to the IVR zones, you must explicitly remove them from the full zone set database before performing the copy operation. Refer to the *Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide* for more information on the IVR feature.

About Backing Up and Restoring Zones

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

Note Backup option is available to switches that run Cisco NX-OS Release 4.1(3) or later. Restore option is only supported on Cisco Fabric Manager Release 4.1(3) or later.

Renaming Zones, Zone Sets, and Aliases

To rename a zone, zone set, fcalias, or zone-attribute-group, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zoneset rename oldname newname vsan 2`	Renames a zone set in the specified VSAN.
	`switch(config)# zone rename oldname newname vsan 2`	Renames a zone in the specified VSAN.
	`switch(config)# fcalias rename oldname newname vsan 2`	Renames a fcalias in the specified VSAN.
	`switch(config)# zone-attribute-group rename oldname newname vsan 2`	Renames a zone attribute group in the specified VSAN.
Step 3	`switch(config)# zoneset activate name newname vsan 2`	Activates the zone set and updates the new zone name in the active zone set.

Cloning Zones, Zone Sets, FC Aliases, and Zone Attribute Groups

To clone a zone, zone set, fcalias, or zone-attribute-group, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zoneset clone oldname newname vsan 2`	Clones a zone set in the specified VSAN.
	`switch(config)# zone clone oldname newname vsan 2`	Clones a zone in the specified VSAN.
	`switch(config)# fcalias clone oldname newname vsan 2`	Clones a fcalias in the specified VSAN.
	`switch(config)# zone-attribute-group clone oldname newname vsan 2`	Clones a zone attribute group in the specified VSAN.
Step 3	`switch(config)# zoneset activate name newname vsan 2`	Activates the zone set and updates the new zone name in the active zone set.

Clearing the Zone Server Database

You can clear all configured information in the zone server database for the specified VSAN.

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

```
switch# clear zone database vsan 2
```

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

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

Advanced Zone Attributes

This section describes advanced zone attributes and includes the following topics:

About Zone-Based Traffic Priority

The zoning feature provides an additional segregation mechanism to prioritize select zones in a fabric and set up access control between devices. Using this feature, you can configure the quality of service (QoS) priority as a zone attribute. You can assign the QoS traffic priority attribute to be high, medium, or low. By default, zones with no specified priority are implicitly assigned a low priority. Refer to the *Cisco MDS 9000 NX-OS Family Quality of Service Configuration Guide* for more information.

To use this feature, you need to obtain the ENTERPRISE_PKG license (refer tothe *Cisco NX-OS Family Licensing Guide*) and you must enable QoS in the switch (refer to the *Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide*).

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.

Caution If zone-based QoS is implemented in a switch, you cannot configure the interop mode in that VSAN.

Configuring Zone-Based Traffic Priority

To configure the zone priority, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zone name QosZone vsan 2` `switch(config-zone)#`	Configures an alias name (QosZone) and enters zone configuration submode.

	Command	Purpose
Step 3	`switch(config-zone)# attribute qos priority high`	Configures this zone to assign high priority QoS traffic to each frame matching this zone.
	`switch(config-zone)# attribute qos priority medium`	Configures this zone to assign medium priority QoS traffic to each frame matching this zone.
	`switch(config-zone)# attribute qos priority low`	Configures this zone to assign low priority QoS traffic to each frame matching this zone.
	`switch(config-zone)# no attribute qos priority high`	Reverts to using the default low priority for this zone.
Step 4	`switch(config-zone)# exit` `switch(config)#`	Returns to configuration mode.
Step 5	`switch(config)# zoneset name QosZoneset vsan 2` `switch(config-zoneset)#`	Configures a zone set called QosZoneset for the specified VSAN (vsan 2) and enters zone set configuration submode. **Tip** To activate a zone set, you must first create the zone and a zone set.
Step 6	`switch(config-zoneset)# member QosZone`	Adds QosZone as a member of the specified zone set (QosZoneset). **Tip** If the specified zone name was not previously configured, this command will return the `Zone not present` error message.
Step 7	`switch(config-zoneset)# exit` `switch(config)#`	Returns to configuration mode.
Step 8	`switch(config)# zoneset activate name QosZoneset vsan 2`	Activates the specified zone set.

Configuring Default Zone QoS Priority Attributes

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

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

To configure the QoS priority attributes for a default zone, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# zone default-zone vsan 1` `switch(config-default-zone)#`	Enters the default zone configuration submode.

	Command	Purpose
Step 3	`switch(config-default-zone)# attribute qos priority high`	Sets the QoS priority attribute for frames matching these zones.
	`switch(config-default-zone)# no attribute qos priority high`	Removes the QoS priority attribute for the default zone and reverts to default low priority.

About Broadcast Zoning

Note Broadcast zoning is not supported on the Cisco Fabric Switch for HP c-Class BladeSystem and the Cisco Fabric Switch for IBM BladeCenter.

You can configure broadcast frames in the basic zoning mode. By default, broadcast zoning is disabled and broadcast frames are sent to all Nx ports in the VSAN. When enabled, broadcast frames are only sent to Nx ports in the same zone, or zones, as the sender. Enable broadcast zoning when a host or storage device uses this feature.

Table 3-2 identifies the rules for the delivery of broadcast frames.

Table 3-2 Broadcasting Requirements

Active Zoning?	Broadcast Enabled?	Frames Broadcast?	Comments
Yes	Yes	Yes	Broadcast to all Nx ports that share a broadcast zone with the source of broadcast frames.
No	Yes	Yes	Broadcast to all Nx ports.
Yes	No	No	Broadcasting is disabled.

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

Caution If broadcast zoning is enabled on a switch, you cannot configure the interop mode in that VSAN.

Configuring Broadcast Zoning

To broadcast frames in the basic zoning mode, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# zone broadcast enable vsan 2`	Broadcasts frames for the specified VSAN.
	`switch(config)# no zone broadcast enable vsan 3`	Disables (default) broadcasting for the specified VSAN.

	Command	Purpose
Step 3	`switch(config)# zone name BcastZone vsan 2` `switch(config-zone)#`	Creates a broadcast zone in the specified VSAN and enters zone configuration submode.
Step 4	`switch(config-zone)# member pwwn 21:00:00:20:37:f0:2e:4d`	Adds the specified member to this zone.
Step 5	`switch(config-zone)# attribute broadcast`	Specifies this zone to be broadcast to other devices.

Step 6	`switch(config-zone)# end`
	`switch# show zone vsan 2`
	`zone name bcast-zone vsan 2`
	`attribute broadcast`
	`pwwn 21:00:00:e0:8b:0b:66:56`
	`pwwn 21:00:00:20:37:f0:2e:4d`
		Displays the broadcast configuration.

To configure the **broadcast** attribute for a default zone, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# zone default-zone vsan 1` `switch(config-default-zone)#`	Enters the default zone configuration submode.
Step 3	`switch(config-default-zone)# attribute broadcast`	Sets broadcast attributes for the default zone.
	`switch(config-default-zone)# no attribute broadcast`	Reverts the default zone attributes to read-write (default).

About Smart Zoning

Smart zoning implements hard zoning of large zones with fewer hardware resources than was previously required. The traditional zoning method allows each device in a zone to communicate with every other device in the zone. The administrator is required to manage the individual zones according to the zone configuration guidelines. Smart zoning eliminates the need to create a single initiator to single target zones. By analyzing device-type information in the FCNS, useful combinations can be implemented at the hardware level by the Cisco MDS NX-OS software, and the combinations that are not used are ignored. For example, initiator-target pairs are configured, but not initiator-initiator.

The device type information of each device in a smart zone is automatically populated from the Fibre Channel Name Server (FCNS) database as host, target, or both. This function allows the optimal utilization of a hardware device to permit only possible pairs of devices to communicate. In the event of a special situation, such as a disk controller that needs to communicate with another disk controller, smart zoning defaults can be overridden by the administrator to allow complete control.

Note Smart Zoning can be enabled at VSAN level but can also be disabled at zone level.

Smart Zoning Member Configuration

Table 3-3 displays the supported smart zoning member configurations.

Table 3-3 Smart Zoning Configuration

Feature	Supported
PWWN	Yes
FCID	Yes
FCalias	Yes
Device-alias	Yes
Interface	No
IP address	No
Symbolic nodename	No
FWWN	No
Domain ID	No

Enabling Smart Zoning on a VSAN

To configure the **smart zoning** for a VSAN, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# zone smart-zoning enable vsan 1` `switch(config)#`	Enables smart zoning on a VSAN.
	`switch(config)# no zone smart-zoning enable vsan 1`	Disables smart zoning on a VSAN.

Setting Default Value for Smart Zoning

To set the default value, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# system default zone smart-zone enable` `switch(config)#`	Enables smart zoning on a VSAN that are created based on the specified default value.
Step 3	`switch(config)# no system default zone smart-zone enable` `switch(config)#`	Disables smart zoning on a VSAN.

Converting Zones Automatically to Smart Zoning

To fetch the device-type information from nameserver and to add that information to the member, follow the steps below: This can be performed at zone, zoneset, FCalias, and VSAN levels.

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# zone convert smart-zoning fcalias name <alias-name> vsan <vsan no>`	Fetches the device type information from the nameserver for the fcalias members.
Step 3	`switch(config)# zone convert smart-zoning zone name <zone name> vsan <vsan no>`	Fetches the device type information from the nameserver for the zone members.
Step 4	`switch(config)# zone convert smart-zoning zoneset name <zoneset name> vsan <vsan no>`	Fetches the device type information from the nameserver for all the zones and fcalias members in the specified zoneset.
Step 5	`switch(config)# zone convert smart-zoning vsan <vsan no>`	Fetches the device type information from the nameserver for all the zones and fcalias members for all the zonesets present in the VSAN.

Configuring Device Types for Zone Members

To configure the device types for zone members, follow this step:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config-zoneset-zone)# member device-alias <name> both`	Configures the device type for the device-alias member as both. For every supported member-type, init, target, and both are supported.
Step 3	`switch(config-zoneset-zone)# member pwwn <number> target`	Configures the device type for the pwwn member as target. For every supported member-type, init, target, and both are supported.
Step 4	`switch(config-zoneset-zone)# member fcid <number>`	Configures the device type for the FCID member. There is no specific device type that is configured. For every supported member-type, init, target, and both are supported. **Note** When there is no specific device type configured for a zone member, at the backend, zone entries that are generated are created as device type both.

Removing Smart Zoning Configuration

To remove the smart zoning configuration, follow this steps:

	Command	Purpose
Step 1	`switch(config)# clear zone smart-zoning fcalias name <alias-name> vsan <vsan no>`	Removes the device type configuration for all the members of the specified fcalias.
Step 2	`switch(config)# clear zone smart-zoning zone name <zone name> vsan <vsan no>`	Removes the device type configuration for all the members of the specified zone.
Step 3	`switch(config)# clear zone smart-zoning zoneset name <zoneset name> vsan <vsan no>`	Removes the device type configuration for all the members of the zone and fcalias for the specified zoneset.
Step 4	`switch(config)# clear zone smart-zoning vsan <vsan no>`	Removes the device type configuration for all the members of the zone and fcalias of all the specified zonesets in the VSAN.

Disabling Smart Zoning at Zone Level

To disable smart zoning at the zone level, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# zone name zone1 vsan 1`	Configures a zone name.
Step 3	`switch(config-zone)# no attribute disable-smart-zoning`	Smart Zoning is disabled for the selected zone. **Note** This command only disables the smart zoning for the selected zone and does not remove the device type configurations.

About LUN Zoning

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

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

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

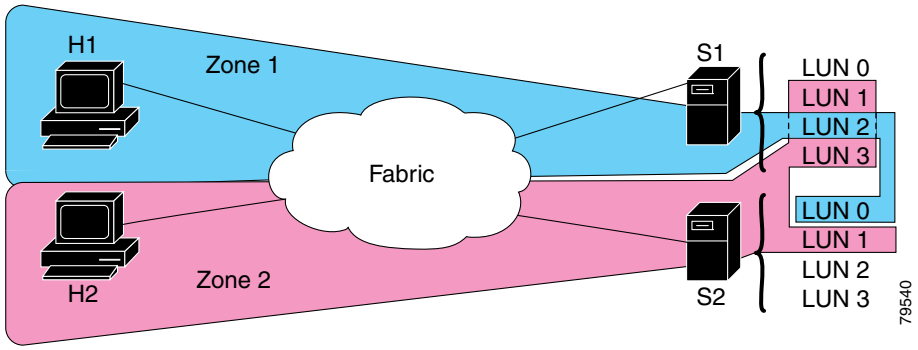
Note When LUN 0 is not included within a zone, then, as per standards requirements, control traffic to LUN 0 (for example, REPORT_LUNS, INQUIRY) is supported, but data traffic to LUN 0 (for example, READ, WRITE) is denied.

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

Note Unzoned LUNs automatically become members of the default zone.

Figure 3-6 shows a LUN-based zone example.

Figure 3-6 LUN Zoning Access



Configuring a LUN-Based Zone

To configure a LUN-based zone, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# zone name LunSample vsan 2` `switch(config-zone)#`	Configures a zone called LunSample for the specified VSAN (vsan 2) and enters zone configuration submode.
Step 3	`switch(config-zone)# member pwwn 10:00:00:23:45:67:89:ab lun 0x64`	Configures a zone member based on the specified pWWN and LUN value. **Note** The CLI interprets the LUN identifier value as a hexadecimal value whether or not the **0x** prefix is included. LUN 0x64 in hex format corresponds to 100 in decimal format.
	`switch(config-zone)# member fcid 0x12465 lun 0x64`	Configures a zone member based on the FC ID and LUN value.

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 "Configuring a LUN-Based Zone" section on page 3-26.

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

Caution If you make any errors when assigning LUNs, you might lose data.

About Read-Only Zones

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. 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, the read-only zone takes 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 either the FAT16 or FAT32 file system is used with the previously mentioned Windows operating systems.

Configuring Read-Only Zones

To configure read-only zones, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# zone name Sample2 vsan 2` `switch(config-zone)#`	Configures a zone called Sample2 for the specified VSAN (vsan 2) and enters zone configuration submode.

	Command	Purpose
Step 3	`switch(config-zone)# attribute read-only`	Sets read-only attributes for the Sample2 zone. **Note** The default is read-write for all zones.
	`switch(config-zone)# no attribute read-only`	Reverts the Sample2 zone attributes to read-write.

To configure the **read-only** option for a default zone, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# zone default-zone vsan 1` `switch(config-default-zone)#`	Enters the default zone configuration submode.
Step 3	`switch(config-default-zone)# attribute read-only`	Sets read-only attributes for the default zone.
	`switch(config-default-zone)# no attribute read-only`	Reverts the default zone attributes to read-write (default).

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, VSAN, or alias, or keywords such as **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 3-1 to 3-16.

Example 3-1 Displays Zone Information for All VSANs

```
switch# 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

zone name Techdocs vsan 3
  ip-address 10.15.0.0 255.255.255.0

zone name Zone21 vsan 5
  pwwn 21:00:00:20:37:a6:be:35
  pwwn 21:00:00:20:37:a6:be:39
  fcid 0xe000ef
  fcid 0xe000e0
  symbolic-nodename iqn.test
  fwwn 20:1f:00:05:30:00:e5:c6
  fwwn 12:12:11:12:11:12:12:10
```

```
  interface fc1/5 swwn 20:00:00:05:30:00:2a:1e
  ip-address 12.2.4.5 255.255.255.0
  fcalias name Alias1 vsan 1
    pwwn 21:00:00:20:37:a6:be:35

zone name Zone2 vsan 11
  interface fc1/5 pwwn 20:4f:00:05:30:00:2a:1e

zone name Zone22 vsan 6
  fcalias name Alias1 vsan 1
    pwwn 21:00:00:20:37:a6:be:35

zone name Zone23 vsan 61
  pwwn 21:00:00:04:cf:fb:3e:7b lun 0000
```

Example 3-2 Displays Zone Information for a Specific VSAN

```
switch# 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 3-3 Displays 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 3-4 Displays 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 3-5 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 3-6 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 3-7 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 3-8 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 3-9 Displays LUN Zone Statistics

```
switch# show zone statistics lun-zoning
LUN zoning statistics for VSAN: 1
************************************************************
S-ID: 0x123456, D-ID: 0x22222, LUN: 00:00:00:00:00:00:00:00
------------------------------------------------------------
Number of Inquiry commands received:            10
Number of Inquiry data No LU sent:               5
Number of Report LUNs commands received:        10
Number of Request Sense commands received:       1
Number of Other commands received:               0
Number of Illegal Request Check Condition sent:  0

S-ID: 0x123456, D-ID: 0x22222, LUN: 00:00:00:00:00:00:00:01
------------------------------------------------------------
Number of Inquiry commands received:             1
Number of Inquiry data No LU sent:               1
Number of Request Sense commands received:       1
Number of Other commands received:               0
Number of Illegal Request Check Condition sent:  0
```

Example 3-10 Displays LUN Zone Statistics

```
switch# show zone statistics read-only-zoning
Read-only zoning statistics for VSAN: 2
************************************************************
S-ID: 0x33333, D-ID: 0x11111, LUN: 00:00:00:00:00:00:00:64
```

```
-------------------------------------------------------------
Number of Data Protect Check Condition Sent:    12
```

Example 3-11 Displays Active Zone Sets

```
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 3-12 Displays Brief Descriptions of Zone Sets

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

Example 3-13 Displays Active Zones

```
switch# show zone active
zone name Zone2 vsan 1
* fcid 0x6c01ef [pwwn 21:00:00:20:37:9c:48:e5]

zone name IVRZ_IvrZone1 vsan 1
  pwwn 10:00:00:00:77:99:7a:1b
* fcid 0xce0000 [pwwn 10:00:00:00:c9:2d:5a:dd]

zone name IVRZ_IvrZone4 vsan 1
* fcid 0xce0000 [pwwn 10:00:00:00:c9:2d:5a:dd]
* fcid 0x6c01ef [pwwn 21:00:00:20:37:9c:48:e5]

zone name Zone1 vsan 1667
  fcid 0x123456

zone name $default_zone$ vsan 1667
```

Example 3-14 Displays Active Zone Sets

```
switch# show zoneset active
zoneset name ZoneSet4 vsan 1
  zone name Zone2 vsan 1
  * fcid 0x6c01ef [pwwn 21:00:00:20:37:9c:48:e5]

  zone name IVRZ_IvrZone1 vsan 1
    pwwn 10:00:00:00:77:99:7a:1b
  * fcid 0xce0000 [pwwn 10:00:00:00:c9:2d:5a:dd]

zoneset name QosZoneset vsan 2
  zone name QosZone vsan 2
  attribute qos priority high
  * fcid 0xce0000 [pwwn 10:00:00:00:c9:2d:5a:dd]
  * fcid 0x6c01ef [pwwn 21:00:00:20:37:9c:48:e5]
```

```
Active zoneset vsan 1667
  zone name Zone1 vsan 1667
    fcid 0x123456

  zone name $default_zone$ vsan 1667
```

Example 3-15 Displays Zone Status

```
switch# show zone status
VSAN: 1 default-zone: deny distribute: full Interop: Off
    mode:basic merge-control:allow session:none
    hard-zoning:enabled
Default zone:
    qos:low broadcast:disabled ronly:disabled
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
    mode:basic merge-control:allow session:none
    hard-zoning:enabled
Default zone:
    qos:low broadcast:disabled ronly:disabled
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
    mode:basic merge-control:allow session:none
    hard-zoning:enabled
Default zone:
    qos:low broadcast:disabled ronly:disabled
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
```

Use the **show zone** command to display the zone attributes for all configured zones.

Example 3-16 Displays Zone Statistics

```
switch# show zone
zone name lunSample vsan 1              <----------------Read-write attribute
zone name ReadOnlyZone vsan 2
    attribute read-only                 <----------------Read-only attribute
```

Use the **show running** and **show zone active** commands to display the configured interface-based zones (see Example 3-17 and Example 3-18).

Example 3-17 Displays the Interface-Based Zones

```
switch# show running
zone name if-zone vsan 1
      member interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2
```

```
        member fwwn 20:4f:00:0c:88:00:4a:e2
        member interface fc2/1 swwn 20:00:00:05:30:00:4a:9e
        member pwwn 22:00:00:20:37:39:6b:dd
```

Example 3-18 Displays the fWWNs and Interfaces in an Active Zone

```
switch# show zone active
zone name if-zone vsan 1
  * fcid 0x7e00b3 [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
  * fcid 0x7e00b1 [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
  * fcid 0x7e00ac [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
  * fcid 0x7e00b3 [fwwn 20:4f:00:0c:88:00:4a:e2]
  * fcid 0x7e00b1 [fwwn 20:4f:00:0c:88:00:4a:e2]
  * fcid 0x7e00ac [fwwn 20:4f:00:0c:88:00:4a:e2]
    interface fc2/1 swwn 20:00:00:05:30:00:4a:9e
```

A similar output is also available on the remote switch (see Example 3-19).

Example 3-19 Displays the Local Interface Active Zone Details for a Remote Switch

```
switch# show zone active
zone name if-zone vsan 1
  * fcid 0x7e00b3 [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
  * fcid 0x7e00b1 [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
  * fcid 0x7e00ac [interface fc2/15 swwn 20:00:00:0c:88:00:4a:e2]
  * fcid 0x7e00b3 [fwwn 20:4f:00:0c:88:00:4a:e2]
  * fcid 0x7e00b1 [fwwn 20:4f:00:0c:88:00:4a:e2]
  * fcid 0x7e00ac [fwwn 20:4f:00:0c:88:00:4a:e2]
    interface fc2/1 swwn 20:00:00:05:30:00:4a:9e
```

Example 3-20 Displays the Zone Status for a VSAN

```
switch# show zone status vsan 1
VSAN: 1 default-zone: deny distribute: full Interop: default
    mode: enhanced merge-control: allow
    session: none
    hard-zoning: enabled broadcast: enabled
    smart-zoning: enabled
```

Example 3-21 Displays the Zone Policy for a VSAN

```
switch# show zone policy vsan 1
Vsan: 1
   Default-zone: deny
   Distribute: full
   Broadcast: enable
   Merge control: allow
   Generic Service: read-write
   Smart-zone: enabled
```

Example 3-22 Displays how to Disable Smart-zoning Attribute Configured for a Zone

```
config# zone-attribute-group name <name> vsan 1
config-attribute-group# disable-smart-zoning
config-attribute-group# exit
config# zone commit vsan 1
```

Example 3-23 Displays how to Auto-convert Zones

```
config# show zoneset vsan 1
zoneset name ZSv1 vsan 1
  zone name ddasZone vsan 1
    device-alias Init1
    device-alias Init2
    device-alias Init3
    device-alias Target1


config# zone convert smart-zoning vsan 1
config# show zoneset vsan1
zoneset name ZSv1 vsan 1
  zone name ddasZone vsan 1
    device-alias Init1  init
    device-alias Init2  init
    device-alias Init3  init
    device-alias Target1
```

Example 3-24 Displays how to Clear Device type Configuration for Members

```
config# show zoneset vsan 1
zoneset name ZSv1 vsan 1
  zone name ddasZone vsan 1
    device-alias Init1  init
    device-alias Init2  init
    device-alias Init3  init
    device-alias Target1

config# clear zone smart-zoning vsan1

config# show zoneset vsan 1
zoneset name ZSv1 vsan 1
  zone name ddasZone vsan 1
    device-alias Init1
    device-alias Init2
    device-alias Init3
    device-alias Target1
```

Enhanced Zoning

The zoning feature complies with the FC-GS-4 and FC-SW-3 standards. Both standards support the basic zoning functionalities explained in the previous section and the enhanced zoning functionalities described in this section.

This section includes the following topics:

About Enhanced Zoning

Table 3-4 lists the advantages of the enhanced zoning feature in all switches in the Cisco MDS 9000 Family.

Table 3-4 Advantages of Enhanced Zoning

Basic Zoning	Enhanced Zoning	Enhanced Zoning Advantages
Administrators can make simultaneous configuration changes. Upon activation, one administrator can overwrite another administrator's changes.	Performs all configurations within a single configuration session. When you begin a session, the switch locks the entire fabric to implement the change.	One configuration session for the entire fabric to ensure consistency within the fabric.
If a zone is part of multiple zone sets, you create an instance of this zone in each zone set.	References to the zone are used by the zone sets as required once you define the zone.	Reduced payload size as the zone is referenced. The size is more pronounced with bigger databases.
The default zone policy is defined per switch. To ensure smooth fabric operation, all switches in the fabric must have the same default zone setting.	Enforces and exchanges the default zone setting throughout the fabric.	Fabric-wide policy enforcement reduces troubleshooting time.
To retrieve the results of the activation on a per switch basis, the managing switch provides a combined status about the activation. It does not identify the failure switch.	Retrieves the activation results and the nature of the problem from each remote switch.	Enhanced error reporting eases the troubleshooting process.
To distribute the zoning database, you must reactivate the same zone set. The reactivation may affect hardware changes for hard zoning on the local switch and on remote switches.	Implements changes to the zoning database and distributes it without reactivation.	Distribution of zone sets without activation avoids hardware changes for hard zoning in the switches.
The MDS-specific zone member types (IPv4 address, IPv6 address, symbolic node name, and other types) may be used by other non-Cisco switches. During a merge, the MDS-specific types can be misunderstood by the non-Cisco switches.	Provides a vendor ID along with a vendor-specific type value to uniquely identify a member type.	Unique vendor type.
The fWWN-based zone membership is only supported in Cisco interop mode.	Supports fWWN-based membership in the standard interop mode (interop mode 1).	The fWWN-based member type is standardized.

Changing from Basic Zoning to Enhanced Zoning

To change to the enhanced zoning mode from the basic mode, follow these steps:

Step 1 Verify that all switches in the fabric are capable of working in the enhanced mode.

If one or more switches are not capable of working in enhanced mode, then your request to move to enhanced mode is rejected.

Step 2 Set the operation mode to enhanced zoning mode. By doing so, you will automatically start a session, acquire a fabric wide lock, distribute the active and full zoning database using the enhanced zoning data structures, distribute zoning policies and then release the lock. All switches in the fabric then move to the enhanced zoning mode.

Tip After moving from basic zoning to enhanced zoning, we recommend that you save the running configuration.

Changing from Enhanced Zoning to Basic Zoning

The standards do not allow you to move back to basic zoning. However, Cisco MDS switches allow this move to enable you to downgrade and upgrade to other Cisco SAN-OS or Cisco NX-OS releases.

To change to the basic zoning mode from the enhanced mode, follow these steps:

Step 1 Verify that the active and full zone set do not contain any configuration that is specific to the enhanced zoning mode.

If such configurations exist, delete them before proceeding with this procedure. If you do not delete the existing configuration, the Cisco NX-OS software automatically removes them.

Step 2 Set the operation mode to basic zoning mode. By doing so, you will automatically start a session, acquire a fabric wide lock, distribute the zoning information using the basic zoning data structure, apply the configuration changes and release the lock from all switches in the fabric. All switches in the fabric then move to basic zoning mode.

Note If a switch running Cisco SAN-OS Release 2.0(1b) and NX-OS 4(1b) or later, with enhanced zoning enabled is downgraded to Cisco SAN-OS Release 1.3(4), or earlier, the switch comes up in basic zoning mode and cannot join the fabric because all the other switches in the fabric are still in enhanced zoning mode.

Enabling Enhanced Zoning

By default, the enhanced zoning feature is disabled in all switches in the Cisco MDS 9000 Family.

To enable enhanced zoning in a VSAN, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# zone mode enhanced vsan 3000` `Set zoning mode command initiated. Check zone status`	Enables enhanced zoning in the specified VSAN.
	`switch(config)# no zone mode enhanced vsan 150` `Set zoning mode command initiated. Check zone status`	Disables enhanced zoning in the specified VSAN.

Modifying the Zone Database

Modifications to the zone database is done within a session. A session is created at the time of the first successful configuration command. On creation of a session, a copy of the zone database is created. Any changes done within the session are performed on this copy of the zoning database. These changes in the copy zoning database are not applied to the effective zoning database until you commit the changes. Once you apply the changes, the session is closed.

If the fabric is locked by another user and for some reason the lock is not cleared, you can force the operation and close the session. You must have permission (role) to clear the lock in this switch and perform the operation on the switch from where the session was originally created.

To commit or discard changes to the zoning database in a VSAN, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# zone commit vsan 2` `No pending info found`	Applies the changes to the enhanced zone database and closes the session.
	`switch(config)# zone commit vsan 3 force`	Forcefully applies the changes to the enhanced zone database and closes the session created by another user.
	`switch(config)# no zone commit vsan 2`	Discards the changes to the enhanced zone database and closes the session.
	`switch(config)# no zone commit vsan 3 force`	Forcefully discards the changes to the enhanced zone database and closes the session created by another user.

Releasing Zone Database Locks

To release the session lock on the zoning database on the switches in a VSAN, use the **no zone commit vsan** command from the switch where the database was initially locked.

```
switch# config t
switch(config)# no zone commit vsan 2
```

If session locks remain on remote switches after using the **no zone commit vsan** command, you can use the **clear zone lock vsan** command on the remote switches.

```
switch# clear zone lock vsan 2
```

Note We recommend using the **no zone commit vsan** command first to release the session lock in the fabric. If that fails, use the **clear zone lock vsan** command on the remote switches where the session is still locked.

Creating Attribute Groups

In enhanced mode, you can directly configure attributes using attribute groups.

To configure attribute groups, follow these steps:

Step 1 Create an attribute group.

```
switch# conf t
switch(config)# zone-attribute-group name SampleAttributeGroup vsan 2
switch(config-attribute-group)#
```

Step 2 Add the attribute to an attribute-group object.

```
switch(config-attribute-group)# readonly
switch(config-attribute-group)# broadcast
switch(config-attribute-group)# qos priority medium
```

Step 3 Attach the attribute-group to a zone.

```
switch(config)# zone name Zone1 vsan 2
switch(config-zone)# attribute-group SampleAttributeGroup
switch(config-zone)# exit
switch(config)#
```

Step 4 Activate the zone set.

```
switch(config)# zoneset activate name Zoneset1 vsan 2
```

The attribute-groups are expanded and only the configured attributes are present in the active zone set.

Merging the Database

The merge behavior depends on the fabric-wide merge control setting:

- Restrict—If the two databases are not identical, the ISLs between the switches are isolated.
- Allow—The two databases are merged using the merge rules specified in Table 3-5.

Table 3-5 Database Zone Merge Status

Local Database	Adjacent Database	Merge Status	Results of the Merge
The databases contain zone sets with the same name[1] 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[1] but different members.		Failed.	ISLs are isolated.

Table 3-5 Database Zone Merge Status (continued)

Local Database	Adjacent Database	Merge Status	Results of the Merge
Empty.	Contains data.	Successful.	The adjacent database information populates the local database.
Contains data.	Empty.	Successful.	The local database information populates the adjacent database.

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.

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.

Merge Process

The merge process operates as follows:

1. The software compares the protocol versions. If the protocol versions differ, then the ISL is isolated.
2. If the protocol versions are the same, then the zone policies are compared. If the zone policies differ, then the ISL is isolated.
3. If the zone merge options are the same, then the comparison is implemented based on the merge control setting.
   a. If the setting is restrict, the active zone set and the full zone set should be identical. Otherwise the link is isolated.
   b. If the setting is allow, then the merge rules are used to perform the merge.

Configuring Zone Merge Control Policies

To configure merge control policies, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# zone merge-control restrict vsan 4`	Configures a restricted merge control setting for this VSAN.
	`switch(config)# no zone merge-control restrict vsan 2`	Defaults to using the allow merge control setting for this VSAN.
	`switch(config)# zone commit vsan 4`	Commits the changes made to VSAN 4.

Preventing Zones From Flooding FC2 Buffers

By using the **zone fc2 merge throttle enable** command you can throttle the merge requests that are sent from zones to FC2 and prevent zones from flooding FC2 buffers. This command is enabled by default. This command can be used to prevent any zone merge scalability problem when you have a lot of zones. Use the **show zone status** command to view zone merge throttle information.

Permitting or Denying Traffic in the Default Zone

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 5`	Permits traffic flow to default zone members.
	`switch(config)# no zone default-zone permit vsan 3`	Denies traffic flow to default zone members and reverts to factory default.
Step 3	`switch(config)# zone commit vsan 5`	Commits the changes made to VSAN 5.

Broadcasting a Zone

You can specify an enhanced zone to restrict broadcast frames generated by a member in this zone to members within that zone. Use this feature when the host or storage devices support broadcasting.

Table 3-6 identifies the rules for the delivery of broadcast frames.

Table 3-6 Broadcasting Requirements

Active Zoning?	Broadcast Enabled?	Frames Broadcast?	Comments
Yes	Yes	Yes	Broadcast to all Nx ports that share a broadcast zone with the source of broadcast frames.
No	Yes	Yes	Broadcast to all Nx ports.
Yes	No	No	Broadcasting is disabled.

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

To broadcast frames in the enhanced zoning mode, follow these steps:

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

	Command	Purpose
Step 2	`switch(config)# zone-attribute-group name BroadcastAttr vsan 2`	Configures the zone attribute group for the required VSAN.
	`switch(config)# no zone-attribute-group name BroadAttr vsan 1`	Removes the zone attribute group for the required VSAN.

Step 3	`switch(config-attribute-group)# broadcast`
	`switch(config-attribute-group)# exit`
	`switch(config)#`
		Creates a broadcast attribute for this group and exits this submode.

	`switch(config-attribute-group)# no broadcast`	Removes broadcast attribute for this group and exits this submode.
Step 4	`switch(config)# zone name BroadcastAttr vsan 2` `switch(config-zone)#`	Configures a zone named BroadcastAttr in VSAN 2.

Step 5	`switch(config-zone)# member pwwn 21:00:00:e0:8b:0b:66:56`
	`switch(config-zone)# member pwwn 21:01:00:e0:8b:2e:80:93`
	`switch(config-zone)# attribute-group name BroadcastAttr`
	`switch(config-zone)# exit`
	`switch(config)#`
		Adds the specified members to this zone and exits this submode.

Step 6	`switch(config)# zone commit vsan 1`
	`Commit operation initiated`
	`switch(config)# end`
		Applies the changes to the enhanced zone configuration and exits this submode.

Step 7	`switch# show zone vsan 1`
	`zone name BroadcastAttr vsan 1`
	`zone-attribute-group name BroadcastAttr vsan 1`
	`broadcast`
	`pwwn 21:00:00:e0:8b:0b:66:56`
	`pwwn 21:01:00:e0:8b:2e:80:93`
		Displays the broadcast configuration

Configuring System Default Zoning Settings

You can configure default settings for default zone policies, full zone distribution, and generic service permissions for new VSANs on the switch. To configure switch-wide default settings, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# system default zone default-zone permit`	Configures permit as the default zoning policy for new VSANs on the switch.
	`switch(config)# no system default zone default-zone permit`	Configures deny (default) as the default zoning policy for new VSANs on the switch.
Step 3	`switch(config)# system default zone distribute full`	Enables full zone database distribution as the default for new VSANs on the switch.
	`switch(config)# no system default zone distribute full`	Disables (default) full zone database distribution as the default for new VSANs on the switch. Only the active zone database is distributed.

	Command	Purpose
Step 4	`switch(config)# system default zone gs read`	Configures read only as the default generic service permission for new VSANs on the switch.
	`switch(config)# system default zone gs read-write`	Configures (default) read-write as the default generic service permission for new VSANs on the switch.
	`switch(config)# no system default zone gs read-write`	Configures none(deny) as the default generic service permission for new VSANs on the switch.

Note Since VSAN 1 is the default VSAN and is always present on the switch, the **system default zone** commands have no effect on VSAN 1.

Configuring Zone Generic Service Permission Settings

Zone generic service permission setting is used to control zoning operation through generic service (GS) interface. The zone generic service permission can be read-only, read-write or none (deny).

To configure generic service (GS) settings, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# zone gs read vsan 3000`	Configures gs permission value as read only in the specified vsan.
	`switch(config)# zone gs read-write vsan 3000`	Configures gs permission value as read-write in the specified vsan.
	`switch(config)# no zone gs read-write vsan 3000`	Configures gs permission value as none(deny) in the specified vsan.

Displaying Enhanced Zone Information

You can view any zone information by using the **show** command. See Examples 3-25 to 3-37.

Example 3-25 Displays the Active Zone Set Information for a Specified VSAN

```
switch# show zoneset active vsan 2
zoneset name testzoneset vsan 2
  zone name testzone vsan 2
    attribute read-only
    attribute broadcast
    attribute qos priority high
    pwwn 21:01:00:e0:8b:2e:a3:8a
    pwwn 22:00:00:0c:50:02:cb:59

  zone name $default_zone$ vsan 2
    attribute read-only
    attribute qos priority high
```

```
    attribute broadcast]
```

Example 3-26 Displays the Zone Set Information or a Specified VSAN

```
switch# show zoneset vsan 2
zoneset name testzoneset vsan 2
  zone name testzone vsan 2
    zone-attribute-group name testattgp vsan 2
      read-only
      broadcast
      qos priority high
    pwwn 21:01:00:e0:8b:2e:a3:8a
    pwwn 22:00:00:0c:50:02:cb:59

zoneset name testzoneset2 vsan 2
  zone name testzone2 vsan 2
    pwwn 21:01:00:e0:8b:2e:68:8a
    pwwn 22:00:00:0c:50:02:cb:80

zoneset name testzoneset3 vsan 2
  zone name testzone3 vsan 2
    pwwn 21:01:00:e0:8b:2e:68:8a
    pwwn 22:00:00:0c:50:02:cb:80
```

Example 3-27 Displays the Zone Attribute Group Information for a Specified VSAN

```
switch# show zone-attribute-group vsan 2
zone-attribute-group name $default_zone_attr_group$ vsan 2
  read-only
  qos priority high
  broadcast
zone-attribute-group name testattgp vsan 2
  read-only
  broadcast
  qos priority high
```

Example 3-28 Displays the fcalias Information for the Specified VSAN

```
switch# show fcalias vsan 2
fcalias name testfcalias vsan 2
 pwwn 21:00:00:20:37:39:b0:f4
 pwwn 21:00:00:20:37:6f:db:dd
 pwwn 21:00:00:20:37:a6:be:2f
```

Example 3-29 Displays the Zone Status for the Specified VSAN

```
switch# show zone status vsan 2
VSAN: 2 default-zone: permit distribute: active only Interop: 100
    mode:basic merge-control:allow session:none
    hard-zoning:enabled
Default zone:
    qos:low broadcast:disabled ronly:disabled
Full Zoning Database :
    Zonesets:3  Zones:3 Aliases: 0 Attribute-groups: 2
Active Zoning Database :
    Name: testzoneset  Zonesets:1  Zones:2
Status:
```

Example 3-30 Displays an Active Zone Status for the Specified VSAN

```
switch# show zone status vsan 1
VSAN: 1 default-zone: permit distribute: full Interop: 100
    mode: enhanced merge-control: allow session: active <--------Indicates an active session.
    Hard zoning is enabled
Default zone:
    qos:low broadcast:disabled ronly:disabled
Full Zoning Database :
    Zonesets:4  Zones:4 Aliases: 0 Attribute-groups: 1
Active Zoning Database :
    Database Not Available
Status: Set zoning mode complete at 10:36:48 Aug 18 2004
```

Example 3-31 Displays the Pending Zone Set Information for the VSAN to be Committed

```
switch# show zoneset pending vsan 2
No pending info found
```

Example 3-32 Displays the Pending Zone Information for the VSAN to be Committed

```
switch# show zone pending vsan 2
No pending info found
```

Example 3-33 Displays the Pending Zone Information for the VSAN to be Committed

```
switch# show zone-attribute-group pending vsan 2
No pending info found
```

Example 3-34 Displays the Pending Active Zone Set Information for the VSAN to be Committed

```
switch# show zoneset pending active vsan 2
No pending info found
```

Example 3-35 Displays the Difference Between the Pending and Effective Zone Information for the Specified VSAN

```
switch# show zone pending-diff vsan 2
zone name testzone vsan 2
   -  member pwwn 21:00:00:20:37:4b:00:a2
   +  member pwwn 21:00:00:20:37:60:43:0c
```

Exchange Switch Support (ESS) defines a mechanism for two switches to exchange various supported features (see Example 3-36).

Example 3-36 Displays the ESS Information for All Switches in the Specified VSAN

```
switch# show zone ess vsan 2
ESS info on VSAN 2 :
    Domain : 210, SWWN : 20:02:00:05:30:00:85:1f, Cap1 : 0xf3, Cap2 : 0x0
```

Example 3-37 Displays the Pending fcalias Information for the VSAN to be Committed

```
switch# show fcalias pending vsan 2
No pending info found
```

Compacting the Zone Database for Downgrading

Prior to Cisco SAN-OS Release 3.0(1), only 2000 zones are supported per VSAN. If you add more than 2000 zones to a VSAN, a configuration check is registered to indicate that downgrading to a previous release could cause you to lose the zones over the limit. To avoid the configuration check, delete the excess zones and compact the zone database for the VSAN. If there are 2000 zones or fewer after deleting the excess zones, the compacting process assigns new internal zone IDs and the configuration can be supported by Cisco SAN-OS Release 2.x or earlier. Perform this procedure for every VSAN on the switch with more than 2000 zones.

Note A merge failure occurs when a switch supports more than 2000 zones per VSAN but its neighbor does not. Also, zone set activation can fail if the switch has more than 2000 zones per VSAN and not all switches in the fabric support more than 2000 zones per VSAN.

To delete zones and compact the zone database for a VSAN, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# no zone name ExtraZone vsan 10`	Deletes a zone to reduce the number of zones to 2000 or fewer.
Step 3	`switch(config)# zone compact vsan 10`	Compacts the zone database for VSAN 10 to recover the zone ID released when a zone was deleted.

Zone and Zone Set Analysis

To better manage the zones and zone sets on your switch, you can display zone and zone set information using the **show zone analysis** command (see Example 3-38 through Example 3-42).

Example 3-38 Full Zoning Analysis

```
switch# show zone analysis vsan 1
Zoning database analysis vsan 1
 Full zoning database
   Last updated at: 15:57:10 IST Feb 20 2006
   Last updated by: Local [ CLI ]
   Num zonesets: 1
   Num zones: 1
   Num aliases: 0
   Num attribute groups: 0
   Formattted size: 36 bytes / 2048 Kb

 Unassigned Zones: 1
   zone name z1 vsan 1
```

Note The maximum size of the full zone database per VSAN is 2000 KB.

Example 3-39 Active Zoning Database Analysis

```
switch# show zone analysis active vsan 1
Zoning database analysis vsan 1
  Active zoneset: zs1 [*]
    Activated at: 08:03:35 UTC Nov 17 2005
    Activated by: Local [ GS ]
    Default zone policy: Deny
    Number of devices zoned in vsan: 0/2 (Unzoned: 2)
    Number of zone members resolved: 0/2 (Unresolved: 2)
    Num zones: 1
    Number of IVR zones: 0
    Number of IPS zones: 0
    Formattted size: 38 bytes / 2048 Kb
```

Note The maximum size of the active zone set database per VSAN is 2000 KB.

Example 3-40 Zone Set Analysis

```
switch# show zone analysis zoneset zs1 vsan 1
Zoning database analysis vsan 1
  Zoneset analysis: zs1
    Num zonesets: 1
    Num zones: 0
    Num aliases: 0
    Num attribute groups: 0
    Formattted size: 20 bytes / 2048 Kb
```

Example 3-41 Displays the Zone Status

```
switch(config)# show zone status
VSAN: 1 default-zone: deny distribute: active only Interop: default
    mode: basic merge-control: allow
    session: none
    hard-zoning: enabled broadcast: unsupported
    smart-zoning: disabled
Default zone:
    qos: none broadcast: unsupported ronly: unsupported
Full Zoning Database :
    DB size: 4 bytes
    Zonesets:0  Zones:0 Aliases: 0
Active Zoning Database :
    Database Not Available
Status:
```

Example 3-42 Displaying the System Defalult Zone

```
switch(config)# show system default zone
system default zone default-zone deny
system default zone distribute active only
system default zone mode basic
system default zone gs read-write
```

```
system default zone smart-zone disabled
```

See the *Cisco MDS 9000 Family Command Reference* for the description of the information displayed in the command output.

Default Settings

Table 3-7 lists the default settings for basic zone parameters.

Table 3-7 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.
Zone based traffic priority	Low.
Read-only zones	Read-write attributes for all zones.
Broadcast frames	Sent to all Nx ports.
Broadcast zoning	Disabled.
Enhanced zoning	Disabled.
Smart Zoning	Disabled.