Configuring FICON

Fibre Connection (FICON) interface capabilities enhance the Cisco MDS 9000 Family by supporting both open systems and mainframe storage network environments. Inclusion of Control Unit Port (CUP) support further enhances the MDS offering by allowing in-band management of the switch from FICON processors.

The fabric binding feature helps prevent unauthorized switches from joining the fabric or disrupting current fabric operations. The Registered Link Incident Report (RLIR) application provides a method for a switchport to send a LIR to a registered Nx port.

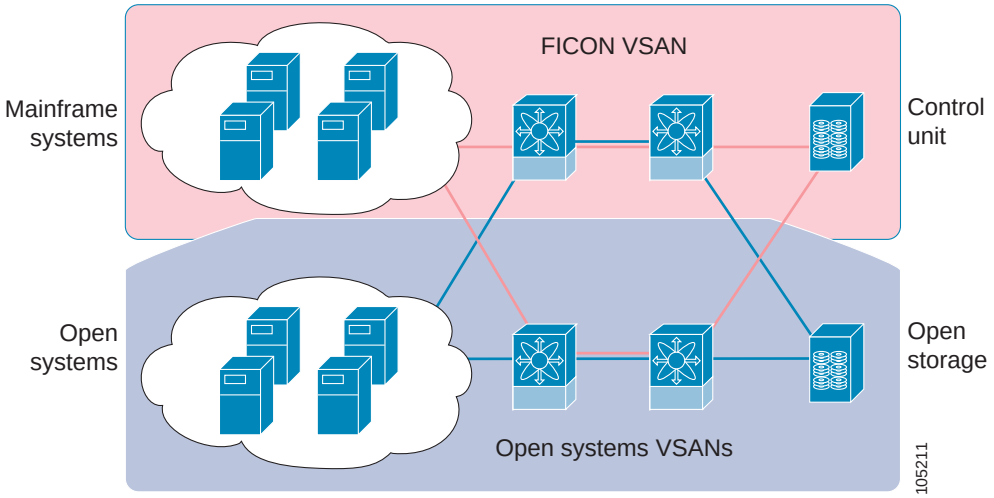
This chapter includes the following sections:

Note FICON features can be implemented in any switch in the Cisco MDS 9000 Family running Cisco MDS SAN-OS Release 1.3 or earlier. While no hardware changes are required, you do need the MAINFRAME_PKG license to configure FICON parameters (see Chapter 3, "Obtaining and Installing Licenses").

About FICON

The Cisco MDS 9000 Family supports the Fibre Channel Protocol (FCP), FICON, iSCSI, and FCIP capabilities within a single, high availability platform. This solution simplifies purchasing, reduces deployment and management costs, and reduces the complex evolution to shared mainframe and open systems storage networks (see Figure 21-1).

Figure 21-1 Shared System Storage Network



FCP and FICON are different FC4 protocols and their traffic are independent of each other. If required, devices using these protocols can be isolated using VSANs.

MDS-Specific FICON Advantages

This section explains the additional FICON advantages in Cisco MDS switches:

- Fabric Optimization with VSANs, page 21-3
- FCIP Support, page 21-4
- PortChannel Support, page 21-4
- VSANs for FICON and FCP Intermixing, page 21-4
- Cisco MDS-Supported FICON Features, page 21-5

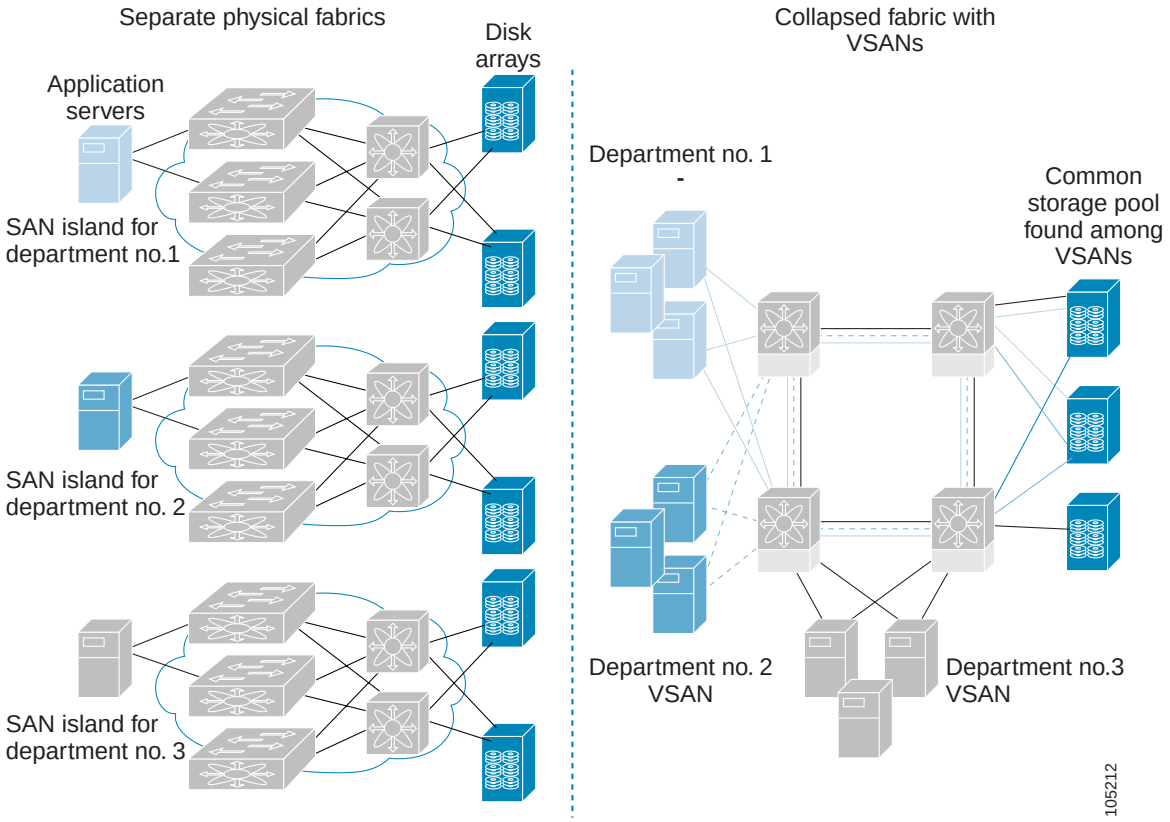
Fabric Optimization with VSANs

Generally, separate physical fabrics have a high level of switch management and have a higher implementation cost. Further, the ports in each island may be over-provisioned depending on the fabric configuration.

By using the Cisco MDS-specific VSAN technology, you can introduce greater efficiency between these physical fabrics by lowering the cost of over-provisioning and reducing the number of switches to be managed.

VSANs also help you to move unused ports nondisruptive and provide a common redundant physical infrastructure (see Figure 21-2).

Figure 21-2 VSAN-Specific Fabric Optimization



VSANs enable global SAN consolidation by allowing you to convert existing SAN islands into virtual SAN islands on a single physical network. It provides hardware-enforced security and separation between applications or departments to allow coexistence on a single network. It also allows virtual rewiring to consolidate your storage infrastructure. You can move assets between departments or applications without the expense and disruption of physical relocation of equipment.

Note While you can configure up to 256 VSANs in any Cisco MDS switch, you can enable FICON in eight of these VSANs.

FCIP Support

The multilayer architecture of the Cisco MDS 9000 Family enables a consistent feature set over a protocol-agnostic switch fabric. Cisco MDS 9500 Series and Cisco MDS 9216 switches transparently integrate Fibre Channel, FICON, and Fibre Channel over IP (FCIP) in one system. The FICON over FCIP feature enables cost-effective access to remotely located mainframe resources. With the Cisco MDS 9000 Family platform, storage replication services such as IBM PPRC and XRC can be extended over metro to global distances using ubiquitous IP infrastructure and simplifying business continuance strategies.

Caution When write-acceleration is enabled in an FCIP interface, a FICON VSAN will not be enabled in that interface. Likewise, if a FCIP interface is up in a FICON VSAN, write-acceleration cannot be enabled on that interface.

See Chapter 22, "Configuring IP Storage" for more information on FCIP.

PortChannel Support

The Cisco MDS implementation of FICON provides support for efficient utilization and increased availability of inter-switch links necessary to build stable large-scale SAN environments. PortChannels ensure an enhanced ISL availability and performance in Cisco MDS switches.

See Chapter 12, "Configuring PortChannels" for more information on PortChannels.

VSANs for FICON and FCP Intermixing

Cisco MDS 9000 Family FICON-enabled switches simplify deployment of even the most complex intermix environments. Multiple logical FICON, Z-Series Linux/FCP, and Open-Systems FCP fabrics can be overlaid onto a single physical fabric by simply creating VSANs as required for each service. VSANs provide both hardware isolation and protocol specific fabric services, eliminating the complexity and potential instability of zone-based intermix schemes.

By default, the FICON feature is disabled in all switches in the Cisco MDS 9000 Family. When the FICON feature is disabled, FC IDs can be allocated seamlessly. Intermixed environments are addressed by the Cisco SAN-OS software. The challenge of mixing Fibre Channel Protocol ((FCP) and FICON protocols are addressed by Cisco MDS switches when implementing VSANs.

Switches and directors in the Cisco MDS 9000 Family support FCP and FICON protocol intermixing at the port level. If these protocols are intermixed in the same switch, you can use VSANs to isolate FCP and FICON ports.

Tip When creating an intermix environment, place all FICON devices in one VSAN (other than the default VSAN) and segregate the FCP switch ports in a separate VSAN (other than the default VSAN). This isolation ensures proper communication for all connected devices.

Cisco MDS-Supported FICON Features

The Cisco MDS 9000 Family FICON features include:

- Flexibility and investment protection—The Cisco MDS 9000 Family shares common switching and service modules across the Cisco MDS 9500 Series as well as the Cisco MDS 9216 Switch.

  Refer to the *Cisco MDS 9500 Series Hardware Installation Guide* and the *Cisco MDS 9216 Switch Hardware Installation Guide).*

- High-availability FICON-enabled director—The Cisco MDS 9500 Series combines nondisruptive software upgrades, stateful process restart and failover, and full redundancy of all major components for a new standard in director-class availability. It supports up to 224 autosensing, 2/1-Gbps, FICON or Fibre Channel FCP ports in any combination in a single chassis and up to 768 Fibre Channel ports in a single rack. The 1.44 Tbps of internal system bandwidth ensures smooth integration of future 10-Gbps modules

  See Chapter 5, “Configuring High Availability.”

- Infrastructure protection—Common software releases infrastructure protection is available across all Cisco MDS 9000 platforms.

  See Chapter 6, “Software Images.”

- VSAN technology—The Cisco MDS 9000 Family introduces VSAN technology for hardware-enforced, isolated environments within a single physical fabric for secure sharing of physical infrastructure and enhanced FICON intermix support.

  See Chapter 9, “Configuring and Managing VSANs.”

- Port-level configurations: BB_credits, beacon mode, and port security for each port.

  See the “Configuring Buffer-to-Buffer Credits” section on page 10-11, “Identifying the Beacon LEDs” section on page 10-15, and Chapter 18, “Configuring Port Security.”

- Configure an alias name, instead of the WWN, for switches and attached node devices.

  See Chapter 13, “Configuring and Managing Zones.”

- Comprehensive security framework—The Cisco MDS 9000 Family supports RADIUS authentication, Simple Network Management Protocol Version 3 (SNMPv3), role-based access control, Secure Shell Protocol (SSH), Secure File Transfer Protocol (SFTP), VSANs, hardware-enforced zoning, ACLs, fabric binding, Fibre Channel Security Protocol (FC-SP), LUN zoning, read-only zones, and VSAN-based access control.

  See Chapter 16, “Configuring Switch Security” and Chapter 17, “Configuring Fabric Security.”

- View the local accounting log to locate FICON events (see the “Local AAA” section on page 16-15).

- Unified storage management—Cisco MDS 9000 FICON-enabled switches are fully IBM CUP standard compliant for in-band management using the IBM S/A OS/390 I/O operations console.

  See the “CUP In-band Management” section on page 21-28.

- Port address-based configurations—port name, blocked or unblocked state, and the prohibit connectivity attributes

  See the “Configuring FICON Ports” section on page 21-21.

- Display the following information:
  - Individual Fibre Channel ports, such as the port name, port number, Fibre Channel address, operational state, type of port, and login data.
  - Nodes attached to ports.

  - Port performance and statistics.

  See "Displaying FICON Information" section on page 21-29.

- Store and apply configuration files.

  See the "FICON Configuration Files" section on page 21-23/

- FICON and Open Systems Management Server features if installed.

  See the "VSANs for FICON and FCP Intermixing" section on page 21-4.

- Enhanced Cascading Support

  See the "CUP In-band Management" section on page 21-28.

- Set the date and time on the switch.

  See the "Configuring FICON Host Control" section on page 21-17.

- Configure SNMP trap recipients and community names.

  See the "FICON SNMP Control" section on page 21-18.

- Call Home configurations—director name, location, description, and contact person.

  See Chapter 23, "Configuring Call Home."

- Configure preferred domain ID, FC ID persistence, and principle switch priority.

  See Chapter 24, "Configuring Domain Parameters."

- Sophisticated SPAN diagnostics—The Cisco MDS 9000 Family provides industry-first intelligent diagnostics, protocol, decoding, and network analysis tools as well as integrated call-home capability for added reliability, faster problem resolution, and reduced service costs.

  See Chapter 28, "Monitoring Network Traffic Using SPAN."

- Configure R_A_TOV, E_D_TOV.

  See the "Configuring FC Timers" section on page 29-2.

- Perform maintenance tasks for the director including maintaining firmware levels, accessing the director logs, and collecting data to support failure analysis.

  See Chapter 31, "Monitoring System Processes and Logs."

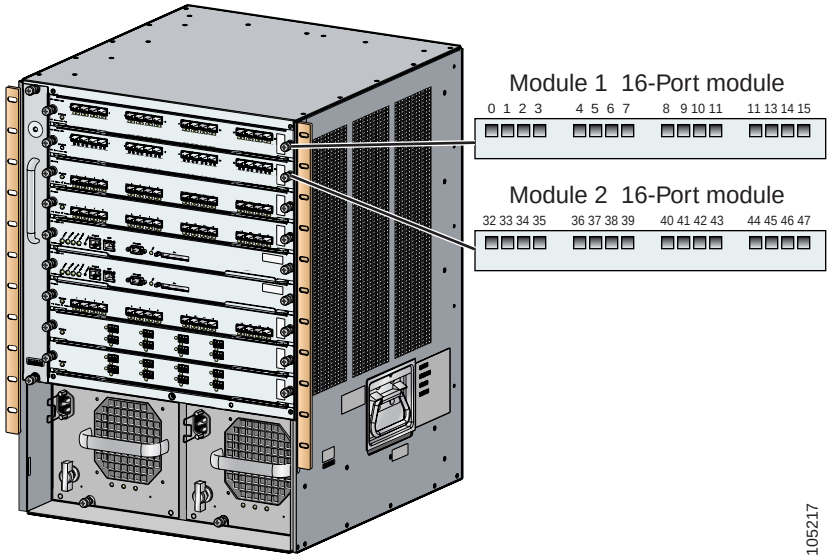
- Display and clear port-level incident alerts.

  "Clearing RLIR Information" section on page 21-49.

FICON Port Numbering

With reference to the FICON feature, ports in Cisco MDS switches are identified by a statically defined 8-bit value known as the *port number*. Port numbers are assigned based on the module and the slot in the chassis. Port numbers cannot be changed and the first port in a switch always starts with a 0 (see Figure 21-3).

Figure 21-3 Port Number in the Cisco MDS 9000 Family



The FICON port number is assigned based on the front panel location of the port and is specific to the slot in which the module resides. Even if the module is a 16-port module, 32-port numbers are assigned to that module—regardless of the module type (16-port or 32-port), the module's physical presence in the chassis, or the port status (up or down).

Note Only Fibre Channel, PortChannel, and FCIP ports are mapped to FICON port numbers. Other types of interfaces do not have a corresponding port number.

Table 21-1 lists the port number assignment for the Cisco MDS 9000 Family of switches and directors.

Table 21-1 FICON Port Numbering in the Cisco MDS 9000 Family

Product	Slot Number	Implemented Port Allocation		Unimplemented Ports	Notes
		To Ports	To PortChannel/FCIP		
Cisco MDS 9120 Switch	Not applicable	0 through 19	20 through 55	56 through 253 and port 255	--
Cisco MDS 9140 Switch	Not applicable	0 through 39	40 through 65	66 through 253 and port 255	--

Table 21-1 FICON Port Numbering in the Cisco MDS 9000 Family

Product	Slot Number	Implemented Port Allocation		Unimplemented Ports	Notes
		To Ports	To PortChannel/FCIP		
Cisco MDS 9216 Switch	Slot 1	0 through 31	64 through 89	90 through 253 and port 255	Similar to a switching module.
	Slot 2	32 through 63			The first 16 port numbers in a 16-port module are used and the rest remain unused.
Cisco MDS 9506 Director	Slot 1	0 through 31	128 through 153	154 through 253 and port 255	
	Slot 2	32 through 63			
	Slot 3	64 through 95			
	Slot 4	96 through 127			
	Slot 5	None			Supervisor modules are not allocated port numbers.
	Slot 6	None			
Cisco MDS 9509 Director	Slot 1	0 through 31	224 through 249	250 through 253 and port 255	The first 16 port numbers in a 16-port module are used and the rest remain unused.
	Slot 2	32 through 63			
	Slot 3	64 through 95			
	Slot 4	96 through 127			
	Slot 5	None			Supervisor modules are not allocated port numbers.
	Slot 6	None			
	Slot 7	128 through 159			The first 16 port numbers in a 16-port module are used and the rest remain unused.
	Slot 8	160 through 191			
	Slot 9	192 through 223			

Port Addresses

By default, port numbers are the same as port addresses. You can swap the port addresses by issuing the **ficon swap portnumber** command (see the "Port Swapping" section on page 21-26).

Implemented and Unimplemented Port Addresses

An implemented port refers to any port address that is available in the chassis. See Table 21-1.

An unimplemented port refers to any port address that is not available in the chassis. See Table 21-1.

Tip An unimplemented port is prohibited from communicating with an implemented port in a FICON setup and cannot be configured.

Installed and Uninstalled Ports

An installed port refers to a port for which all required hardware is present. A specified port number in a VSAN can be implemented, and yet not installed, if any of the following conditions apply:

- The module is not present—for example, if module 1 is not physically present in slot 1 in a Cisco MDS 9509 Director, ports 0 to 31 are considered uninstalled.
- The small form-factor pluggable (SFP) port is not present—for example, if a 16-port module is inserted in slot 2 in a Cisco MDS 9509 Director, ports 48 to 63 are considered uninstalled.
- The port is not in a FICON-enabled VSAN—for example, if port 4 (of a 16-port module in slot 1) is configured in FICON-enabled VSAN 2, then only port 4 is installed and ports 0 to 3 and 5 to 15 are uninstalled—even if they are implemented in VSAN 2.

  Another scenario is if VSANs 1 through 5 are FICON-enabled, and trunking-enabled interface fc1/1 has VSANs 3 through 10, then port address 0 is uninstalled in VSAN 1 and 2.
- The port is part of a PortChannel—for example, if interface fc 1/1 is part of PortChanne1 5, port address 0 is uninstalled in all FICON VSANs.

  See the "Implemented Port Allocation" section on page 21-7 and the "To PortChannel/FCIP" section on page 21-7.

FICON Port Numbering Guidelines

The following guidelines apply to FICON port numbers:

- Supervisor modules do not have port number assignments.
- Port numbers are VSAN independent. Fibre Channel port numbers do not change based on VSANs or TE ports.
- Each PortChannel must be explicitly associated with a FICON port number.
- When the port number for a physical PortChannel becomes uninstalled, the relevant PortChannel configuration is applied to the physical port.
- Each FCIP tunnel must be explicitly associated with a FICON port number. If the port numbers are not assigned for PortChannels or for FCIP tunnels, the associated ports will not come up.

  See the "FCIP and PortChannel Port Numbers" section on page 21-9.

FCIP and PortChannel Port Numbers

FCIP and PortChannels cannot be used in a FICON-enabled VSAN unless they are explicitly bound to a port number.

See the "Binding Port Numbers to PortChannels" section on page 21-20 and the "Binding Port Numbers to FCIP Interfaces" section on page 21-20.

To find the first available port number to bind a FCIP or PortChannel interface use the **show ficon first-available port-number** command (see Example 21-3).

Tip The **show ficon vsan portaddress brief** command displays the port number to interface mapping. You can assign port numbers in the PortChannel/FCIP range which are not already assigned to a PortChannel or FCIP interface (see Example 21-4).

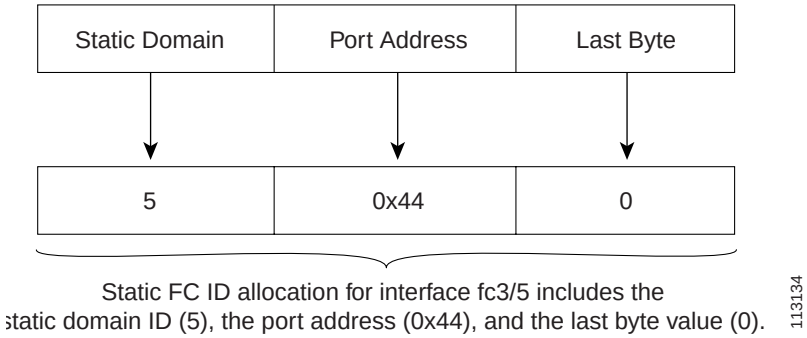
FC ID Allocation

FICON requires a predictable and static FC ID allocation scheme. When FICON is enabled, the FC ID allocated to a device is based on the port address of the port to which it is attached. The port address forms the middle byte of the fabric address. Additionally, the last byte of the fabric address should be the same for all devices in the fabric. By default, the last byte value is 0 and can be configured (see the "Configuring the FC ID Last Byte" section on page 21-16).

Note You cannot configure persistent FC IDs in FICON-enabled VSANs.

Cisco MDS switches have a dynamic FC ID allocation scheme. When FICON is enabled or disabled on a VSAN, all the ports are flapped to switch from the dynamic to static FC IDs and vice versa (see Figure 21-3).

Figure 21-4 Static FC ID Allocation for FICON



Static FC ID allocation for interface fc3/5 includes the static domain ID (5), the port address (0x44), and the last byte value (0).

FICON Cascading

The Cisco SAN-OS software allows multiple switches in a FICON network. To configure multiple switches, you must enabled and configure fabric binding in that switch (see the "Fabric Binding Configuration" section on page 21-37).

Cisco MDS FICON Prerequisites

To ensure that a FICON VSAN is operationally up, be sure to verify the following requirements:

- Set the default zone to permit, if you are not using the zoning feature.

  See the "The Default Zone" section on page 13-11.
- Enable in-order delivery on the VSAN.

  See the "In-Order Delivery" section on page 19-10.
- Enable (and if required, configure) fabric binding on the VSAN.

  See the "Fabric Binding Configuration" section on page 21-37.
- Verify that conflicting persistent FC IDs do not exist in the switch.

  See Chapter 24, "Configuring Domain Parameters."
- Verify that the configured domain ID and requested domain ID match.

  See Chapter 24, "Configuring Domain Parameters."
- Add the CUP (area FE) to the zone, if you are using zoning.

  See the "CUP In-band Management" section on page 21-28.

If any of these requirements are not met, the FICON feature cannot be enabled.

Enabling FICON

By default FICON is disabled in all switches in the Cisco MDS 9000 Family. You can enable FICON on a per VSAN basis in one of three ways:

- By using the automated **setup ficon** command.

  See the "Setting Up a Basic FICON Configuration" section on page 21-12.
- Manually addressing each prerequisite.

  See the "Manually Enabling FICON" section on page 21-15.
- By using the Device Manager (refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*).

Effects of Enabling FICON

When you enable the FICON feature in Cisco MDS switches, the following apply:

- You cannot disable in-order delivery for the FICON-enabled VSAN.
- You cannot disable fabric binding or static domain ID configurations for the FICON-enabled VSAN.
- The load balancing scheme is changed to Source ID (SID)—Destination ID (DID). You cannot change it back to SID—DID—OXID.
- The IPL configuration file is automatically created.

  See the "FICON Configuration Files" section on page 21-23.

Setting Up a Basic FICON Configuration

This section steps you through the procedure to set up FICON on a specified VSAN in a Cisco MDS 9000 Family switch.

Note Press **Ctrl-C** at any prompt to skip the remaining configuration options and proceed with what is configured until that point.

Tip If you do not wish to answer a previously configured question, or if you wish to skip answers to any questions, press **Enter**. If a default answer is not available (for example, switch name), the switch uses what was previously configured and skips to the next question.

To enable and set up FICON, follow these steps.

Step 1 Issue the **setup ficon** command at the EXEC command mode.

```
switch# setup ficon
                --- Ficon Configuration Dialog ---

This setup utility will guide you through basic Ficon Configuration
on the system.

Press Enter if you want to skip any dialog. Use ctrl-c at anytime
to skip all remaining dialogs.
```

Step 2 Enter **yes** (the default is **yes**) to enter the basic FICON configuration setup.

```
Would you like to enter the basic configuration dialog (yes/no) [yes]: yes
```

The FICON setup utility guides you through the basic configuration process. Press **Ctrl-C** at any prompt to end the configuration process.

Step 3 Enter the VSAN number for which FICON should be enabled.

```
Enter vsan [1-4093]:2
```

Step 4 Enter **yes** (the default is **yes**) to create a new VSAN.

```
vsan 2 does not exist, create it? (yes/no) [yes]: yes
```

Step 5 Enter **yes** (the default is **yes**) to confirm your VSAN choice:

```
Enable ficon on this vsan? (yes/no) [yes]: yes
```

Note At this point, the software creates the VSAN if it does not already exist.

Step 6 Enter the domain ID number for the specified FICON VSAN.

```
Configure domain-id for this ficon vsan (1-239):2
```

Step 7 Enter **yes** (the default is **no**) to set up FICON in cascaded mode. If you enter **no**, skip to Step 8 (see "CUP In-band Management" section on page 21-28).

```
Would you like to configure ficon in cascaded mode: (yes/no) [no]: yes
```

a. Assign the peer WWN for the FICON: CUP.

```
Configure peer wwn (hh:hh:hh:hh:hh:hh:hh:hh): 11:00:02:01:aa:bb:cc:00
```

b. Assign the peer domain ID for the FICON: CUP

```
Configure peer domain (1-239) :4
```

c. Enter **yes** if you wish to configure additional peers (and repeat Steps 7a and 7b). Enter **no**, if you do wish to configure additional peers.

```
Would you like to configure additional peers: (yes/no) [no]: no
```

Step 8 Enter **yes** (the default is **yes**) to deny SNMP permission to modify existing port connectivity parameters (see the "FICON SNMP Control" section on page 21-18).

```
Enable SNMP to modify port connectivity parameters? (yes/no) [yes]: yes
```

Step 9 Enter **no** (the default is **no**) to disable the host (mainframe) to modify the port connectivity parameters, if required (see the "Configuring FICON Host Control" section on page 21-17).

```
Disable Host from modifying port connectivity parameters? (yes/no) [no]: no
```

Step 10 Enter **yes** (the default is **yes**) to enable the **active equals saved** feature (see the "Automatically Saving the Running Configuration" section on page 21-19).

```
Enable active=saved? (yes/no) [yes]: yes
```

Step 11 Enter **yes** (the default is **yes**) if you wish to configure additional FICON VSANs.

```
Would you like to configure additional ficon vsans (yes/no) [yes]: yes
```

Step 12 Review and edit the configuration that you have just entered.

Step 13 Enter **no** (the default is **no**) if you are satisfied with the configuration.

Note For documentation purposes, the following configuration displays three VSANs with different FICON settings. These settings provide a sample output for different FICON scenarios.

```
The following configuration will be applied:

fcdomain domain 2 static vsan 1
fcdomain restart disruptive vsan 1
fabric-binding database vsan 1
swwn 11:00:02:01:aa:bb:cc:00 domain 4
fabric-binding activate vsan 1
zone default-zone permit vsan 1
ficon vsan 1
no host port control

fcdomain domain 3 static vsan 2
fcdomain restart disruptive vsan 2
fabric-binding activate vsan 2 force
zone default-zone permit vsan 2
ficon vsan 2
no host port control
no active equals saved

vsan database
vsan 3
fcdomain domain 5 static vsan 3
fcdomain restart disruptive vsan 3
fabric-binding activate vsan 3 force
zone default-zone permit vsan 3
ficon vsan 3
```

```
no snmp port control
no active equals saved

Would you like to edit the configuration? (yes/no) [no]: no
```

Step 14 Enter **yes** (the default is **yes**) to use and save this configuration. The implemented commands are displayed. After FICON is enabled for the specified VSAN, you are returned to the EXEC mode switch prompt.

```
Use this configuration and apply it? (yes/no) [yes]: yes

`fcdomain domain 2 static vsan 1`
`fcdomain restart disruptive vsan 1`
`fabric-binding database vsan 1`
`swwn 11:00:02:01:aa:bb:cc:00 domain 4`
`fabric-binding activate vsan 1`
`zone default-zone permit vsan 1`
`ficon vsan 1`
`no host port control`

`fcdomain domain 3 static vsan 2`
`fcdomain restart disruptive vsan 2`
`fabric-binding activate vsan 2 force`
`zone default-zone permit vsan 2`
`ficon vsan 2`
`no host port control`
`no active equals saved`
```

Note If a new VSAN is created, two additional commands are displayed— **vsan database** and **vsan** *number*.

```
`vsan database`
`vsan 3`
`in-order-guarantee vsan 3`
`fcdomain domain 2 static vsan 3`
`fcdomain restart disruptive vsan 3`
`fabric-binding activate vsan 3 force`
`zone default-zone permit vsan 3`
`ficon vsan 3`
`no snmp port control`
Performing fast copy config...done.
switch#
```

Manually Enabling FICON

Tip This section describes the procedure to manually enabled FICON on a VSAN. If you have already enabled FICON on the required VSAN using the automated setup (recommended), skip to the "Automatically Saving the Running Configuration" section on page 21-19.

To manually enable FICON on a VSAN, follow these steps:

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

Step 2	`switch(config)# vsan database`
	`switch(config-vsan-db)# vsan 5`
	`switch(config-vsan-db)# do show vsan usage`
	`4 vsan configured`
	`configured vsans:1-2,5,26`
	`vsans available for configuration:3-4,6-25,27-4093`
	`switch(config-vsan-db)# exit`
		Enables VSAN 5.

Step 3	`switch(config)# in-order-guarantee vsan 5`	Activates in-order delivery for VSAN 5. See Chapter 19, "Configuring Fibre Channel Routing Services and Protocols."
Step 4	`switch(config)# fcdomain domain 2 static vsan 2`	Configures the domain ID for VSAN 2. See Chapter 24, "Configuring Domain Parameters."
Step 5	`switch(config)# fabric-binding activate vsan 2 force`	Activates fabric binding on VSAN 2. See the "Fabric Binding Configuration" section on page 21-37.
Step 6	`switch(config)# zone default-zone permit vsan 2`	Sets the default zone to permit for VSAN 2. See the "CUP In-band Management" section on page 21-28.
Step 7	`switch(config)# ficon vsan 2` `switch(config-ficon)#`	Enables FICON on VSAN 2.
	`switch(config)# no ficon vsan 6`	Disables the FICON feature on VSAN 6.
Step 8	`switch(config-ficon)# no host port control`	Prohibits mainframe users from moving the switch to an offline state. See the "Allowing the Host to Move the Switch Offline" section on page 21-17.

Configuring Code Page

FICON strings are coded in Extended Binary-Coded Decimal Interchange Code (EBCDIC) format. Refer to your mainframe documentation for details on the code page options.

Use the **code-page** command to configure the EBCDIC format. Cisco MDS switches support **international-5**, **france**, **brazil**, **germany**, **italy**, **japan**, **spain-latinamerica**, **uk**, and **us-canada** (default) EBCDIC format options.

Tip This is an optional configuration. If you are not sure of the EBCDIC format to be used, we recommend retaining the **us-canada** (default) option.

To configure the **code-page** option in a VSAN, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ficon vsan 2` `switch(config-ficon)#`	Enables FICON on VSAN 2.
Step 3	`switch(config-ficon)# code-page italy`	Configures the **italy** EBCDIC format.
	`switch(config-ficon)# no code-page`	Reverts to the factory default of using the **us-canada** EBCDIC format.

Configuring the FC ID Last Byte

Caution If the FICON feature is configured in cascaded mode, the Cisco MDS Switches use ISLs to connect to other switches.

FICON requires the last byte of the fabric address to be the same for all allocated FC IDs. By default, this value is set to 0. You can only change the FC ID last byte when the FICON switch is in the offline state

See the "Moving a FICON VSAN to an Offline State" section on page 21-27.

To assign the last byte for the FC ID, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ficon vsan 2` `switch(config-ficon)#`	Enables FICON on VSAN 2.
Step 3	`switch(config-ficon)# fcid-last-byte 12`	Assigns the last byte FC ID for the fabric address.
	`switch(config-ficon)# no fcid-last-byte 3`	Removes the configured last byte FC ID for the fabric address and reverts to the factory default of 0.

Configuring FICON Host Control

The commands included in this section allow the host (mainframe) to control the Cisco MDS switch.

Allowing the Host to Move the Switch Offline

By default, hosts are allowed to move the switch to an offline state.

Use the **host control switch offline** command to allow the host to move the switch to an offline state.

To allow the host to move the switch to an offline state, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ficon vsan 2` `switch(config-ficon)#`	Enables FICON on VSAN 2.
Step 3	`switch(config-ficon)# no host control switch offline`	Prohibits mainframe users from moving the switch to an offline state.
	`switch(config-ficon)# host control switch offline`	Allows the host to move the switch to an offline state (default) and shuts down the ports.

Allowing the Host to Change FICON Port Parameters

By default, mainframe users are allowed to configure FICON parameters on Cisco MDS switches—they can only query the switch.

Use the **host port control** command to permit mainframe users to configure FICON parameters.

To configure mainframe access, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ficon vsan 2` `switch(config-ficon)#`	Enables FICON on VSAN 2.
Step 3	`switch(config-ficon)# no host port control`	Prohibits mainframe users from configuring FICON parameters on the Cisco MDS switch.
	`switch(config-ficon)# host port control`	Allows mainframe users to configure FICON parameters on the Cisco MDS switch (default).

Allowing the Host to Control the Time Stamp

By default, the clock in each VSAN is the same as the switch hardware clock. Each VSAN in a Cisco MDS switch represents a virtual director. The clock and time present in each virtual director can be different.To maintain separate clocks for each VSAN, the Cisco SAN-OS software maintains the difference of the VSAN-specific clock and the hardware-based director clock. When a host (mainframe) sets the time, the Cisco SAN-OS software updates this difference between the clocks. When a host reads the clock, it computes the difference between the VSAN-clock and the current director hardware clock and presents a value to the mainframe.

The VSAN-clock's current time is reported in the output of **show ficon vsan** *vsan-id*, **show ficon**, and **show accounting log** commands.

To configure host control, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ficon vsan 2` `switch(config-ficon)#`	Enables FICON on VSAN 2.
Step 3	`switch(config-ficon)# no host set-timestamp`	Prohibits mainframe users from changing the VSAN-specific clock.
	`switch(config-ficon)# host set-timestamp`	Allows the host to set the clock on this switch (default).

Clearing Time Stamps

Note You can clear time stamps only from the Cisco MDS switch—not the mainframe.

Use the **clear ficon vsan** *vsan-id* **timestamp** command in EXEC mode to clear the VSAN-clock.

```
switch# clear ficon vsan 20 timestamp
```

FICON SNMP Control

By default, SNMP users can configure FICON parameters through the Cisco MDS 9000 Family Fabric Manager.

Note If you disable SNMP use in the Cisco MDS switch, you cannot configure FICON parameters using the Fabric Manager.

Configuring FICON SNMP Control

You can prohibit this access, if required, by issuing the **no snmp port control** command.

To configure SNMP control, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ficon vsan 2` `switch(config-ficon)#`	Enables FICON on VSAN 2.
Step 3	`switch(config-ficon)# no snmp port control`	Prohibits SNMP users from configuring FICON parameters.
	`switch(config-ficon)# snmp port control`	Allows SNMP users to configure FICON parameters (default).

Automatically Saving the Running Configuration

Table 21-2 displays the results of **active equals saved** command and the implicit **copy running start** command in various scenarios.

If **active equals saved** is enabled in any FICON-enabled VSAN in the fabric, then the following apply (see Number 1 and 2 in Table 21-2):

- All configuration changes (FICON-specific or not) are automatically saved to persistent storage (implicit **copy running start**) and stored in the startup configuration.
- FICON-specific configuration changes are immediately saved to the IPL file (see the "FICON Configuration Files" section on page 21-23).

If **active equals saved** is not enabled in any FICON-enabled VSAN in the fabric, then FICON-specific configuration changes are not saved in the IPL file and an implicit **copy running start** is not issued—you must issue the **copy running start** command explicitly (see Number 3 in Table 21-2):

Table 21-2 Saving the Active FICON and Switch Configuration

Number	FICON-enabled VSAN?	`active equals saved` Command Enabled?	Implicit[1] `copy running start` Command Issued?	Notes
1	Yes	Yes (in all FICON VSANs)	Implicit	FICON changes written to the IPL file. Non-FICON changes saved to startup configuration and persistent storage.
2		Yes (even in one FICON VSAN)	Implicit	FICON changes written to IPL file for only the VSAN which has active equals saved enabled. Non-FICON changes saved to startup configuration and persistent storage.
3		Not in any FICON VSAN	Not implicit	FICON changes are not written to the IPL file. Non-FICON changes are saved in persistent storage—only if you explicitly issue the **copy running start** command.
4	No	Not applicable		

1. When the Cisco SAN-OS software implicitly issues a `copy running start` command in the Cisco MDS switch, only a binary configuration is generated—an ASCII configuration is not generated (see Example 21-17). If you wish to generate an additional ASCII configuration at this stage, you must explicitly issue the `copy running start` command again.

Note If **active equals saved** is enabled, the Cisco SAN-OS software ensures that you do not have to perform the **copy running startup** command for the FICON configuration as well. If your switch or fabric consists of multiple FICON -enabled VSANs, and one of these VSANs have **active equals saved** enabled, changes made to the non-FICON configuration results in all configurations being saved to the startup configuration.

To automatically save the running configuration, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ficon vsan 2` `switch(config-ficon)#`	Enables FICON on VSAN 2.
Step 3	`switch(config-ficon)# active equals saved`	Enables the automatic save feature for all VSANs in the switch or fabric.
	`switch(config-ficon)# no active equals saved`	Disables automatic save for this VSAN.

Binding Port Numbers to PortChannels

Caution All port number assignments to PortChannels/FCIP interfaces are lost (cannot be retrieved) when FICON is disabled on all VSANs.

You can bind (or associate) a PortChannel with a FICON port number to bring up that interface.

To bind a PortChannel with a FICON port number, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# interface Port-channel 1` `switch(config-if)#`	Enters the PortChannel interface configuration mode.
Step 3	`switch(config-if)# ficon portnumber 234`	Assigns the FICON port number to the selected PortChannel port.

Binding Port Numbers to FCIP Interfaces

You can bind (or associate) a FCIP interface with a FICON port number to bring up that interface.

To bind a FCIP interface with a FICON port number, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch1(config)# interface fcip 51` `switch1(config-if)#`	Creates a FCIP interface (51).
Step 3	`switch(config-if)# ficon portnumber 208`	Assigns the FICON port number to the selected FCIP interface.

Configuring FICON Ports

You can perform FICON configurations on a per-port address basis in the Cisco MDS 9000 Family of switches.

Even if a port is uninstalled, the port address-based configuration is accepted by the Cisco MDS switch. This configuration is applied to the port when the port becomes installed.

Blocking Ports

If you block a port, the port is retained in the operationally down state. If you unblock a port, a port initialization is attempted. When a port is blocked, data and control traffic are not allowed on that port.

Physical Fibre Channel port blocks will continue to transmit an Off-Line State (OLS) primitive sequence on a blocked port.

Caution You cannot block or prohibit the CUP port (0XFE).

Note The **shutdown**/**no shutdown** port state is independent of the **block**/**no block** port state. If a port is shutdown, unblocking that port will not initialize the port.

To block or unblock port addresses in a VSAN, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ficon vsan 2` `switch(config-ficon)#`	Enables FICON on VSAN 2.
Step 3	`switch(config-ficon)# portaddress 1 - 5` `switch(config-ficon-portaddr)#`	Selects port address 1 to 5 for further configuration.
Step 4	`switch(config-ficon-portaddr)# block`	Disables a range of port addresses and retains it in the operationally down state.
	`switch(config-ficon-portaddr)# no block`	Enables the selected port address and reverts to the factory default of the port address not being blocked.

Prohibiting Ports

To prevent implemented ports from talking to each other, you can configure prohibits between two or more ports. If you prohibit ports, the specified ports are prevented from communicating with each other.

Note Unimplemented ports are always prohibited.

Tip You cannot prohibit a PortChannel or FCIP interface.

Prohibit configurations are always symmetrically applied—if you prohibit Port 0 from talking to port 15, port 15 is automatically prohibited from talking to port 0.

To prohibit port addresses in a VSAN, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ficon vsan 2` `switch(config-ficon)#`	Enables FICON on VSAN 2.
Step 3	`switch(config-ficon)# portaddress 7` `switch(config-ficon-portaddr)#`	Selects port address 7 for further configuration.
Step 4	`switch(config-ficon-portaddr)# prohibit portaddress 3-5`	Prohibits port address 7 in VSAN 2 from talking to ports 3, 4, and 5.
	`switch(config-ficon-portaddr)# no prohibit portaddress 5`	Removes port address 5 from a previously prohibited state.

Note If an interface is already configured in E or TE mode and you try to prohibit that port, your prohibit configuration is rejected. Similarly, if a port is not up and you prohibit that port, the port is not allowed to come up in E mode nor in TE mode.

Assigning Port Address Names

To assign a port address name, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ficon vsan 2` `switch(config-ficon)#`	Enables FICON on VSAN 2.
Step 3	`switch(config-ficon)# portaddress 7` `switch(config-ficon-portaddr)#`	Selects port address 7 for further configuration.
Step 4	`switch(config-ficon-portaddr)# name SampleName`	Assigns a name to the port address. **Note** The port address name is restricted to 24 alphanumeric characters.
	`switch(config-ficon-portaddr)# no name SampleName`	Deletes a previously configured port address name.

FICON Configuration Files

You can save up to 16 FICON configuration files on each FICON-enabled VSAN (in persistent storage). The file format is proprietary to IBM. These files can be read and written by IBM hosts using the in-band CUP protocol. Additionally, you can use the Cisco MDS CLI or Fabric Manager applications to operate these FICON configuration files.

Note Multiple FICON configuration files with the same name can exist in the same switch, provided they reside in different VSANs. For example, you can create a configuration file named XYZ in both VSAN 1 and VSAN 3.

When you enable the FICON feature in a VSAN, the switches always use the startup FICON configuration file, called IPL. This file is created with a default configuration as soon as FICON is enabled in a VSAN.

Caution When FICON is disabled on a VSAN, all the FICON configuration files are irretrievably lost.

FICON configuration files contain the following configuration for each implemented port address:

- Block
- Prohibit mask
- Port address name

Note Normal configuration files used by Cisco MDS switches include FICON-enabled attributes for a VSAN, port number mapping for PortChannels and FCIP interfaces, port number to port address mapping, port and trunk allowed VSAN configuration for ports, in-order guarantee, configuring static domain ID, and fabric binding configuration.

See the "Working with Configuration Files" section on page 4-23 for details on the normal configuration files used by Cisco MDS switches.

Accessing FICON Configuration Files

Only one user can access the configuration file at any given time:

- If this file is being accessed by user 1, user 2 cannot access this file.
- If user 2 does attempt to access this file, an error is issued to user 2.
- If user 1 is inactive for more than 15 seconds, the file is automatically closed and available for use by any other permitted user.

FICON configuration files can be accessed by any host, SNMP, or CLI user who is permitted to access the switch. The locking mechanism in the Cisco SAN-OS software restricts access to one user at a time per file. This lock applies to newly created files and previously saved files. Before accessing any file, you must lock the file and obtain the file key. A new file key is used by the locking mechanism for each lock request. The key is discarded when the lock timeout of 15 seconds expires. The lock timeout value cannot be changed.

Applying the FICON Configuration Files

The configuration from the saved files can be applied to the running configuration by using the **ficon vsan** *number* **apply file** *filename* command. For example:

```
switch# ficon vsan 2 apply file SampleFile
```

Editing FICON Configuration Files

The configuration file submode allows you to create and edit FICON configuration files. If a specified file does not exist, it is created. Up to 16 files can be saved. Each file name is restricted to eight alphanumeric characters.

To edit the contents of a specified FICON configuration file, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# ficon vsan 2` `switch(config-ficon)#`	Enables FICON on VSAN 2.
Step 3	`switch(config-ficon)# file IplFile1` `switch(config-ficon-file)#`	Accesses the FICON configuration file called IplFile1 for VSAN 2. If this file does not exist, it is created. **Note** All FICON file names are restricted to eight alphanumeric characters.
	`switch(config-ficon)# no file IplFileA`	Deletes a previously created FICON configuration file.
Step 4	`switch(config-ficon-file)# portaddress 3` `switch(config-ficon-file-portaddr)#`	Enters the submode for port address 3 to edit the contents of the configuration file named IplFile1. **Note** The running configuration is not applied to the current configuration. The configuration is only applied when the **ficon vsan** *number* **apply file** *filename* command is issued.
Step 5	`switch(config-ficon-file-portaddr)# prohibit portaddress 5`	Edits the content of the configuration file named IplFile1 by prohibiting port address 5 from accessing port address 3.
Step 6	`switch(config-ficon-file-portaddr)# block`	Edits the content of the configuration file named IplFile1 by blocking a range of port addresses and retaining them in the operationally down state.
Step 7	`switch(config-ficon-file-portaddr)# name P3`	Edits the content of the configuration file named IplFile1 by assigning the name P3 to port address 3. If the name did not exist, it is created. If it existed, it is overwritten.

Copying FICON Configuration Files

Use the **ficon vsan** *vsan-id* **copy file** *exiting-file-name save-as-file-name* command in EXEC mode to copy an existing FICON configuration file.

```
switch# ficon vsan 20 copy file IPL IPL3
```

You can see the list of existing configuration files by issuing the **show ficon vsan** *vsan-id* command.

```
switch# show ficon vsan 20
Ficon information for VSAN 20
  Ficon is online
  VSAN is active
  Host port control is Enabled
  Host offline control is Enabled
  User alert mode is Disabled
  SNMP port control is Enabled
  Host set director timestamp is Enabled
  Active=Saved is Enabled
  Number of implemented ports are 240
  Key Counter is 5
  FCID last byte is 0
  Date/Time is same as system time (Wed Dec 3 20:10:45.924591 2003)
  Device Allegiance not locked
  Codepage is us-canada
  Saved configuration files
    IPL
    IPL3
```

Port Swapping

The FICON port swap feature is only provided for maintenance purposes.

The FICON port swapping feature causes all configuration associated with *old-port-number* and *new port-number* to be swapped, including VSAN configurations.

Cisco MDS switches allow port swapping for non-existent ports as follows:

- Only FICON-specific configurations (prohibit, block, and port address mapping) are swapped.
- No other system configuration is swapped.
- All other system configurations are only maintained for existing ports.

Tip If **active equals saved** is enabled on any FICON VSAN, then the swapped configuration is automatically saved to startup. Otherwise, you must explicitly issue the **copy running startup** command immediately after swapping the ports.

Once you issue the **ficon swap portnumber** *old-port-number new-port-number* command, the switch automatically performs the following actions:

- Shuts down both the old and new ports.
- Swaps the port configuration.
- If you attempt to bring the port up by specifying the **after swap noshut** option (after the *new-port-number* variable), you must explicitly issue the **no shutdown** command to resume traffic.

The **ficon swap portnumber** command is only associated with the two ports concerned. You must issue this VSAN-independent command from EXEC mode.

To swap physical Fibre Channel ports, follow these steps:

Step 1 Issue the **ficon swap portnumber** *old-port-number new-port-number* command in EXEC mode.

The specified ports are operationally shut down.

Step 2 Physically swap the front panel port cables between the two ports.

Step 3 Issue the **no shutdown** command on each port to enable traffic flow.

Note If you specify the **ficon swap portnumber** *old-port-number new-port-number* **after swap noshut** command, the ports are automatically initialized.

Port Swapping Guidelines

Be sure to follow these guidelines when using the FICON port swap feature:

- Port swapping is not supported for logical ports (PortChannels, FCIP links). Neither the *old-port-number* nor the *new-port-number* can be a logical port.
- Port swapping is not supported between physical ports that are part of a PortChannel. Neither the *old-port-number* nor the *new-port-number* can be a physical port that is part of a PortChannel.

- Before performing a port swap, the Cisco SAN-OS software performs a compatibility check. If the two ports have incompatible configurations, the port swap is rejected with an appropriate reason code. For example, if a port with BB_credits as 25 is being swapped with an OSM port for which a maximum of 12 BB_credits is allowed (not a configurable parameter), the port swapping operation is rejected.
- If ports have default values (for some incompatible parameters), then a port swap operation is allowed and the ports retain their default values. If you swap a 16-port module with a 32-port module, the BB_credits will no longer be compatible and the ports can be swapped. If BB_credits are not configured, the default settings will still be in effect at the time of the swap.

Note The 32-port module guidelines also apply for port swapping configurations (see the "32-Port Configuration Guidelines" section on page 10-8).

Moving a FICON VSAN to an Offline State

Use the EXEC-level **ficon vsan** *vsan-id* **offline** command to log out all ports in the VSAN that needs to be suspended.

Use the EXEC-level **ficon vsan** *vsan-id* **online** command to remove the offline condition and to allow ports to log on again.

Note This command can be issued by the host if the host is allowed to do so (see the "Allowing the Host to Move the Switch Offline" section on page 21-17).

Clearing FICON Device Allegiance

FICON requires serialization of access among multiple mainframes, CLI, and SNMP sessions be maintained on Cisco MDS 9000 Family switches by controlling device allegiance for the currently executing session. Any other session is denied permission to perform configuration changes unless the required allegiance is available.

You can clear the current device allegiance by issuing the **clear ficon vsan** *vsan-id* **allegiance** command in EXEC mode.

```
switch# clear ficon vsan 1 allegiance
```

Caution This command aborts the currently executing session.

CUP In-band Management

The Control Unit Port (CUP) protocol configures access control and provides unified storage management capabilities from a mainframe computer. Cisco MDS 9000 FICON-enabled switches are fully IBM CUP standard compliant for in-band management using the IBM S/A OS/390 I/O operations console.

Note The CUP specification is proprietary to IBM.

CUP is supported by switches and directors in the Cisco MDS 9000 Family. The CUP function allows the mainframe to manage the Cisco MDS switches.

Host communication includes control functions such as blocking and unblocking ports, as well as monitoring and error reporting functions.

Placing CUPs in a Zone

To place the CUP in a zone, follow these steps.

Step 1 Set the default zone to permit for the required VSAN.

```
switch# config t
switch(config)# zone default-zone permit vsan 20
```

Step 2 Issue the **show fcns database** command for the required VSAN and obtain the required FICON CUP WWN.

```
switch# show fcns database vsan 20

VSAN 20:
--------------------------------------------------------------------------
FCID        TYPE  PWWN                    (VENDOR)        FC4-TYPE:FEATURE
--------------------------------------------------------------------------
0x0d0d00    N     50:06:04:88:00:1d:60:83 (EMC)           FICON:CU
0x0dfe00    N     25:00:00:0c:ce:5c:5e:c2 (Cisco)         FICON:CUP
0x200400    N     50:05:07:63:00:c2:82:d3 (IBM)           scsi-fcp FICON:CU f..
0x200800    N     50:05:07:64:01:40:15:0f (IBM)           FICON:CH
0x20fe00    N     20:00:00:0c:30:ac:9e:82 (Cisco)         FICON:CUP

Total number of entries = 5
```

Note If more than one `FICON:CUP WWN` exists in this fabric, be sure to add all the `FICON:CUP WWN` PWWNs to the required zone. The previous example displays multiple `FICON:CUP` occurrences to indicate a cascade configuration.

Step 3 Add the identified FICON:CUP WWN to the zone database.

```
switch(config)# zone name Zone1 vsan 20
switch(config-zone)# member pwwn 25:00:00:0c:ce:5c:5e:c2
```

Displaying FICON Information

Use the **show** commands to display all FICON information configured on this switch (see Examples 21-1 to 21-16).

Receiving FICON Alerts

In Example 21-1 the **user alert mode is enabled** output confirms that you will receive an alert to indicate any changes in the FICON configuration.

Example 21-1 Displays Configured FICON Information

```
switch# show ficon
Ficon information for VSAN 20
  Ficon is online
  VSAN is active
  Host port control is Enabled
  Host offline control is Enabled
  User alert mode is Enabled
  SNMP port control is Enabled
  Host set director timestamp is Enabled
  Active=Saved is Disabled
  Number of implemented ports are 240
  Key Counter is 73723
  FCID last byte is 0
  Date/Time is set by host to Sun Jun 26 00:04:06.991999 1904
  Device allegiance is locked by Host
  Codepage is us-canada
  Saved configuration files
    IPL
    _TSIRN00
```

Displaying FICON Port Address Information

Examples 21-2 to 21-5 display FICON Port Address information.

Example 21-2 Displays Port Address Information

```
switch# show ficon vsan 2 portaddress
Port Address 1 is not installed in vsan 2
    Port number is 1, Interface is fc1/1
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255

Port Address 2 is not installed in vsan 2
    Port number is 2, Interface is fc1/2
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255
...
Port Address 239 is not installed in vsan 2
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255
```

```
Port Address 240 is not installed in vsan 2
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255
```

Example 21-3 Displays the Available Port Numbers

```
switch# show ficon first-available port-number
Port number 129(0x81) is available
```

In Example 21-4, the interface column is populated with the corresponding interface if the port number is installed. If the port number is uninstalled, this space remains blank and indicates an unbound port number. For example, 56 is an unbound port number in Example 21-4.

Example 21-4 Displays Port Address Information in a Brief Format

```
switch# show ficon vsan 2 portaddress 50-55 brief
--------------------------------------------------------------------------------
Port    Port    Interface          Admin     Status           Oper   FCID
Address Number                     Blocked                    Mode
--------------------------------------------------------------------------------
50      50      fc2/18            on        fcotAbsent       --     --
51      51      fc2/19            off       fcotAbsent       --     --
52      52      fc2/20            off       fcotAbsent       --     --
53      53      fc2/21            off       fcotAbsent       --     --
54      54      fc2/22            off       notConnected     --     --
55      55      fc2/23            off       up               FL     0xea0000
56     56                         off       up               FL     0xea0000
```

Example 21-5 displays the counters in FICON version format 1 (32-bit format)

Example 21-5 Displays Port Address Counter Information

```
switch# show ficon vsan 20 portaddress 8 counters
Port Address 8(0x8) is up in vsan 20
    Port number is 8(0x8), Interface is fc1/8
    Version presented 1, Counter size 32b
    242811 frames input, 9912794 words
      484 class-2 frames, 242302 class-3 frames
      0 link control frames, 0 multicast frames
      0 disparity errors inside frames
      0 disparity errors outside frames
      0 frames too big, 0 frames too small
      0 crc errors, 0 eof errors
      0 invalid ordered sets
      0 frames discarded c3
      0 address id errors
    116620 frames output, 10609188 words
      0 frame pacing time
    0 link failures
    0 loss of sync
    0 loss of signal
    0 primitive seq prot errors
    0 invalid transmission words
    1 lrr input, 0 ols input, 5 ols output
    0 error summary
```

Displaying IPL File Information

Examples 21-6 to 21-5 display FICON Port Address information.

Example 21-6 Displays the Contents of the Specified FICON Configuration File

```
switch# show ficon vsan 3 file IPL
FICON configuration file IPL      in vsan 3
    Port address 1
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255

    Port address 2
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255

    Port address 3
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255

    Port address 4
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255

...
Port address 80
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255

    Port address 254
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,81-253,255
```

Example 21-7 Displays All FICON Configuration Files

```
switch# show ficon vsan 2
Ficon information for VSAN 2
  Ficon is enabled
  VSAN is active
  Host control is Enabled
  Host offline control is Enabled
  Clock alert mode is Disabled
  User alert mode is Disabled
  SNMP control is Disabled
  Active=Saved is Disabled
  Number of implemented ports are 240
  Key Counter is 9
  FCID last byte is 0
  Date/Time is same as system time(Sun Dec 14 01:26:30.273402 1980)
  Device Allegiance not locked
  Codepage is us-canada
  Saved configuration files
    IPL
    IPLFILE1
```

Example 21-8 Displays the Specified Port Addresses for a FICON Configuration File

```
switch# show ficon vsan 2 file iplfile1 portaddress 1-7
FICON configuration file IPLFILE1 in vsan 2
    Port address 1
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,241-253,255

    Port address 2
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,241-253,255

    Port address 3
        Port name is P3
        Port is not blocked
        Prohibited port addresses are 0,241-253,255
...
    Port address 7
        Port name is
        Port is not blocked
        Prohibited port addresses are 0,241-253,255
```

Displaying the Configured FICON State

If FICON is not enabled on a VSAN, you cannot view the port address information for that VSAN (see Example 21-9 and Example 21-10).

Example 21-9 Displays the Specified Port Address When FICON Is Disabled

```
switch# show ficon vsan 1 portaddress 55
FICON not enabled
```

Example 21-10 Displays the Specified Port Address When FICON Is Enabled

```
switch# show ficon vsan 2 portaddress 55
Port Address 55 is not installed in vsan 2
    Port number is 55, Interface is fc2/23
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255
    Admin port mode is FL
    Port mode is FL, FCID is 0xea0000
```

Displaying a Ports Administrative State

Examples 21-11 to 21-12 display the administrative state of a FICON port. If the port is blocked, the **show ficon vsan** *number* **portaddress** *number* command displays the blocked state of the port. If a specific port is prohibited, this command also displays the specifically prohibited port (3) along with the ports that are prohibited by default (0, 241 to 253, and 255). If a name is assigned, that name is also displayed.

Example 21-11 Displays an Administratively Unblocked Port

```
switch# show ficon vsan 2 portaddress 2
Port Address 2(0x2) is not installed in vsan 2
    Port number is 2(0x2), Interface is fc1/2
    Port name is
    Port is not admin blocked
    Prohibited port addresses are 0,241-253,255(0,0xf1-0xfd,0xff)
    Admin port mode is auto
    Peer was type model manufactured by
```

Example 21-12 Displays an Administratively Blocked Port

```
switch# show ficon vsan 2 portaddress 1
Port Address 2(0x2) is not installed in vsan 2
    Port number is 2(0x2), Interface is fc1/2
    Port name is SampleName
    Port is admin blocked
    Prohibited port addresses are 0,241-253,255(0,0xf1-0xfd,0xff)
    Admin port mode is auto
    Peer was type model manufactured by
```

Displaying Control Unit Information

Example 21-13 displays configured control device information.

Example 21-13 Displays Control Unit Information

```
switch# show ficon control-device sb3
Control Unit Image:0x80b9c2c
VSAN:20 CU:0x20fe00 CUI:0 CUD:0 CURLP:(nil)
ASYNC LP:(nil) MODE:1 STATE:1 CQ LEN:0 MAX:0
PRIMARY LP:   VSAN:0 CH:0x0 CHI:0 CU:0x0 CUI:0
ALTERNATE LP: VSAN:0 CH:0x0 CHI:0 CU:0x0 CUI:0

Logical Path:0x80b9fb4
VSAN:20 CH:0x200600 CHI:15 CU:0x20fe00 CUI:0 STATE:1 FLAGS:0x1
LINK: OH:0x0 OC:0x0 IH:0x0 IC:0x0
DEV:  OH:0x0 OC:0x0 IH:0x0 IC:0x0
SENSE: 00 00 00 00 00 00 00 46
       30 20 00 00 00 00 00 00
       00 00 00 00 00 00 00 00
       00 00 00 00 00 00 00 00
IUI:0x0 DHF:0x0 CCW:0x0 TOKEN:0x0 PCCW:0x0 FCCW:0x0 PTOKEN:0x0 FTOKEN:0x0
CMD:0x0 CCW_FLAGS:0x0 CCW_COUNT:0 CMD_FLAGS:0x0 PRIO:0x0 DATA_COUNT:0
STATUS:0x0 FLAGS:0x0 PARAM:0x0 QTP:0x0 DTP:0x0
CQ LEN:0 MAX:0 DESTATUS:0x0
```

Displaying Buffer Information

In Example 21-14, the `Key Counter` column displays the 32-bit value maintained by Cisco MDS switches. This value is incremented when any port changes state in that VSAN. The key counter (a 32-bit value) is incremented when a FICON-related configuration is changed. Host programs can increment this value at the start of the channel program and then perform operations on multiple ports. The director history buffer keeps a log of which port address configuration was changed for each key-counter value.

The director history buffer provides a mechanism to determine the change in the port state from the previous time when a value was contained in the key counter.

Example 21-14 Displays the History Buffer for the Specified VSAN

```
switch# show ficon vsan 20 director-history
Director History Buffer for vsan 20
-------------------------------------------
Key Counter           Ports Address
                      Changed
-------------------------------------------
74556                 43
74557                 44
74558                 45
74559                 46
74560                 47
74561                 48
74562                 49
74563                 50
74564                 51
74565                 52
74566                 53
74567                 54
74568                 55
74569                 56
74570                 57
74571                 58
74572                 59
74573                 60
74574                 61
74575                 62
74576                 63
74577                 64
74578
74579
74580                 1-3,5,10,12,14-16,34-40,43-45,47-54,56-57,59-64
74581                 3,5
74582                 64
74583
74584                 1-3,10,12,14-16,34-40,43-45,47-54,56-57,59-64
74585                 1
74586                 2
74587                 3
```

Displaying FICON Information in the Running Configuration

Example 21-15 displays the FICON-related information in the running configuration.

Example 21-15 Displays the Running Configuration Information

```
switch# show running-config
Building Configuration ...
in-order-guarantee
vsan database
  vsan 11 name "FICON11" loadbalancing src-dst-id
  vsan 75 name "FICON75" loadbalancing src-dst-id

fcdomain domain 11 static vsan 11
fcdomain domain 119 static vsan 75

fcdroplatency network 100 vsan 11
fcdroplatency network 500 vsan 75

fabric-binding enable
fabric-binding database vsan 11
  swwn 20:00:00:0d:ec:01:20:c0 domain 10
fabric-binding database vsan 75
  swwn 20:00:00:0d:ec:00:d6:40 domain 117
fabric-binding activate vsan 11
fabric-binding activate vsan 75

ficon vsan 75

interface port-channel 1
  ficon portnumber 0x80
  switchport mode E

snmp-server user mblair network-admin auth md5 0x688fa3a2e51ba5538211606e59ac292
7 priv 0x688fa3a2e51ba5538211606e59ac2927 localizedkey
snmp-server user wwilson network-admin auth md5 0x688fa3a2e51ba5538211606e59ac29
27 priv 0x688fa3a2e51ba5538211606e59ac2927 localizedkey
snmp-server host 171.71.187.101 traps version 2c public udp-port 1163
snmp-server host 172.18.2.247 traps version 2c public udp-port 2162

vsan database
  vsan 75 interface fc1/1
...
interface mgmt0
  ip address 172.18.47.39 255.255.255.128
  switchport speed 100
  switchport duplex full

no system health

ficon vsan 75
  file IPL
```

Displaying FICON Information in the Startup Configuration

Example 21-16 displays the FICON-related information in the startup configuration.

Example 21-16 Displays the Startup Configuration

```
switch# show startup-config
...
ficon vsan 2
file IPL
```

Example 21-17 displays the switch response to an implicitly-issued copy running start command. In this case, only a binary configuration is saved until you explicitly issue the **copy running start** command again (see Table 21-2)

Example 21-17 Displays the Startup Configuration Status

```
switch# show startup-config
No ASCII config available since configuration was last saved internally
on account of 'active=saved' mode.
Please perform an explicit 'copy running startup` to get ASCII configuration
```

Displaying FICON-Related Log Information

Example 21-18 and Example 21-19 display the logging information for FICON-related configurations.

Example 21-18 Displays Logging Levels for the FICON Feature

```
switch# show logging level ficon
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
ficon                   2                       2

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

Example 21-19 Displays FICON -Related Log File Contents

```
switch# show logging logfile
...
2004 Feb 25 15:38:50 vegas6 %PORT-5-IF_UP: %$VSAN 75: 2004 Wed Feb 25 13:22:04.
131183%$ Interface fc1/8 is up in mode F
 2004 Feb 25 15:38:50 vegas6 %PORT-5-IF_UP: %$VSAN 75: 2004 Wed Feb 25 13:22:04.
131217%$ Interface fc1/9 is up in mode F
...
2004 Feb 25 15:39:09 vegas6 %PORT-5-IF_TRUNK_UP: %$VSAN 75: 2004 Wed Feb 25 13:
22:23.131121%$ Interface fc2/1, vsan 75 is up
 2004 Feb 25 15:39:09 vegas6 %PORT-5-IF_TRUNK_UP: %$VSAN 75: 2004 Wed Feb 25 13:
22:23.131121%$ Interface fc2/2, vsan 75 is up
 2004 Feb 25 15:39:09 vegas6 %PORT-5-IF_TRUNK_UP: %$VSAN 75: 2004 Wed Feb 25 13:
...
2004 Feb 25 23:22:36 vegas6 %PORT-5-IF_UP: %$VSAN 75: 2004 Wed Feb 25 21:05:42.
99916%$ Interface fc3/6 is up in mode F
 2004 Feb 25 23:22:37 vegas6 %PORT-5-IF_UP: %$VSAN 75: 2004 Wed Feb 25 21:05:43.
...
```

Fabric Binding Configuration

The Cisco SAN-OS Release 1.3 fabric binding feature ensures ISLs are only enabled between specified switches in the fabric binding configuration. Fabric binding is configured on a per-VSAN basis and can only be implemented in FICON VSANs. You can still perform fabric binding configuration in a non-FICON VSAN—these configurations will only come into effect after FICON is enabled.

This feature helps prevent unauthorized switches from joining the fabric or disrupting current fabric operations. It uses the Exchange Fabric Membership Data (EFMD) protocol in FICON networks to ensure that the list of authorized switches is identical in all switches in the fabric.

This section contain the following topics:

Port Security Versus Fabric Binding

Port security and fabric binding are two independent features that can be configured to complement each other (see Table 21-3).

Table 21-3 Fabric Binding and Port Security Comparison

Fabric Binding	Port Security
Uses a set of sWWN and a persistent Domain ID.	Uses pWWNs/nWWNs or fWWNs/switch WWNs.
Binds the fabric at the switch level.	Binds devices at the interface level.
Authorizes only the configured sWWN stored in the fabric binding database to participate in the fabric.	Allows a preconfigured set of Fibre Channel devices to logically connect to a SAN port(s). The switchport, identified by a WWN or interface number, connects to a Fibre Channel device (a host or another switch), also identified by a WWN. By binding these two devices, you lock these two ports into a group (list).
Activation is required on a per VSAN basis.	Activation is required on a per VSAN basis.
User defines specific switches that are allowed to connect to the fabric, regardless of the physical port to which the peer switch is connected.	User specifies the specific physical port(s) to which another device can connect.
Does not learn logging in switches.	Learns about switches or devices if in learning mode.

Port-level checking for xE-ports

- switch login uses both port binding as well as the fabric binding feature for a given VSAN.
- Binding checks are done on the port VSAN:
  - E-port security binding check is done on port VSAN.
  - TE-port security binding check is done in each allowed VSAN.

While port security complements fabric binding, they are independent features and can be enabled or disabled separately.

Fabric Binding Enforcement

To enforce fabric binding, configure the switch world wide name (sWWN) to specify the xE port connection for each switch. Enforcement of fabric binding policies are done on every activation and when the port tries to come up. However, enforcement of fabric binding at the time of activation happens only if the VSAN is a FICON VSAN. The fabric binding feature requires all sWWNs connected to a switch and their persistent domain IDs to be part of the fabric binding active database.

To configure fabric binding in each switch in the fabric, follow these steps.

Step 1 Enable the fabric configuration feature.

Step 2 Configure a list of sWWNs and their corresponding domain IDs for devices that are allowed to access the fabric.

Step 3 Activate the fabric binding database.

Step 4 Save the fabric binding configuration.

Step 5 Verify the fabric binding configuration.

Enabling Fabric Binding

The fabric binding feature must be enabled in each switch in the fabric that participates in the fabric binding. By default, this feature is disabled in all switches in the Cisco MDS 9000 Family. The configuration and verification commands for the fabric binding feature are only available when fabric binding is enabled on a switch. When you disable this configuration, all related configurations are automatically discarded.

To enable fabric binding on any participating switch, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# fabric-binding enable`	Enables fabric binding on that switch.
	`switch(config)# no fabric-binding enable`	Disables (default) fabric binding on that switch.

View the status of the fabric binding feature of an fabric binding-enabled switch by issuing the **show fabric-binding status** command.

```
switch# show fabric-binding status
VSAN 1 :Activated database
VSAN 4 :No Active database
```

Configuring a List of Switch WWNs in a Fabric

A user-specified fabric binding list contains a list of switch WWNs (sWWNs) within a fabric. If a sWWN attempts to join the fabric, and that sWWN is not in the list or the sWWN is using a domain ID that differs from the one specified in the allowed list, the ISL between the switch and the fabric is automatically isolated in that VSAN and the switch is denied entry into the fabric.

The persistent domain ID must be specified along with the sWWN. Domain ID authorization is required in FICON VSANs where the domains are statically configured and the end devices reject a domain ID change in all switches in the fabric.

To configure a list of sWWNs and domain IDs, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# fabric-binding database vsan 5` `switch(config-fabric-binding)#`	Enters the fabric binding submode for the specified VSAN.
	`switch(config)# no fabric-binding database vsan 10`	Deletes the fabric binding database for the specified VSAN.
Step 3	`switch(config-fabric-binding)# swwn 21:00:05:30:23:11:11:11 domain 102`	Adds the sWWN and domain ID of a switch to the configured database list.
Step 4	`switch(config-fabric-binding)# swwn 21:00:05:30:23:1a:11:03 domain 101`	Adds the sWWN and domain ID of another switch to the configured database list.
Step 5	`switch(config-fabric-binding)# no swwn 21:00:15:30:23:1a:11:03 domain 101`	Deletes the sWWN and domain ID of a switch from the configured database list.
Step 6	`switch(config-fabric-binding)# exit` `switch(config)#`	Exits the fabric binding submode.

Activating Fabric Binding

The fabric binding maintains a configuration database (config-database) and an active database. The config-database is a read-write database that collects the configurations you perform. These configurations are only enforced upon activation. This activation overwrites the active database with the contents of the config database. The active database is read-only and is the database that checks each switch that attempts to log in.

By default, the fabric binding feature is not activated. You cannot activate the switch if entries existing in the config database conflict with the current state of the fabric. For example, one of the already logged in switches may be denied login by the config database. You can choose to forcefully override these situations.

Note After activation, any already logged in switch that violates the current active database will be logged out, and all switches that were previously denied login because of fabric binding restrictions are reinitialized.

To activate the fabric binding feature, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# fabric-binding activate vsan 1`	Activates the fabric binding database for the specified VSAN.
	`switch(config)# no fabric-binding activate vsan 10`	Deactivates the fabric binding database for the specified VSAN.

Forcing Fabric Binding Activation

If the database activation is rejected due to one or more conflicts listed in the previous section, you may decide to proceed with the activation by using the **force** option.

To forcefully activate the fabric binding database, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# fabric-binding activate vsan 3 force`	Activates the fabric binding database for the specified VSAN forcefully—even if the configuration is not acceptable.
	`switch(config)# no fabric-binding activate vsan 1 force`	Reverts to the previously configured state or to the factory default (if no state is configured).

Saving Fabric Binding Configurations

When you save the fabric binding configuration, the config database and the active database are both saved to the startup configuration and are available after a reboot.

- Use the **fabric-binding database copy vsan** command to copy from the active database to the configuration database. If the configured database is empty, this command is not accepted.

  ```
  switch# fabric-binding database copy vsan 1
  ```

- Use the **fabric-binding database diff active vsan** command to view the differences between the active database and the config database. This command can be used when resolving conflicts.

  ```
  switch# fabric-binding database diff active vsan 1
  ```

- Use the **fabric-binding database diff config vsan** command to obtain information on the differences between the config database and the active database.

  ```
  switch# fabric-binding database diff config vsan 1
  ```

Caution You cannot deactivate or disable fabric binding in a FICON-enabled VSAN.

Clearing the Fabric Binding Statistics

Use the **clear fabric-binding statistics** command to clear all existing statistics from the fabric binding database for a specified VSAN.

```
switch# clear fabric-binding statistics vsan 1
```

Deleting the Fabric Binding Database

Use the **no fabric-binding** command in configuration mode to delete the configured database for a specified VSAN.

```
switch(config)# no fabric-binding database vsan 1
```

Verifying Fabric Binding Configurations

Use the **show** commands to display all fabric binding information configured on this switch (see Examples 21-20 to 21-28).

Example 21-20 Displays Configured Fabric Binding Database Information

```
switch# show fabric-binding database
-------------------------------------------------
Vsan   Logging-in Switch WWN     Domain-id
-------------------------------------------------
1      21:00:05:30:23:11:11:11   0x66(102)
1      21:00:05:30:23:1a:11:03    0x19(25)
1      20:00:00:05:30:00:2a:1e   0xea(234)
4      21:00:05:30:23:11:11:11   0x66(102)
4      21:00:05:30:23:1a:11:03    0x19(25)
61     21:00:05:30:23:1a:11:03    0x19(25)
61     21:00:05:30:23:11:11:11   0x66(102)
[Total 7 entries]
```

Example 21-21 Displays Active Fabric Binding Information

```
switch# show fabric-binding database active
-------------------------------------------------
Vsan   Logging-in Switch WWN     Domain-id
-------------------------------------------------
1      21:00:05:30:23:11:11:11   0x66(102)
1      21:00:05:30:23:1a:11:03    0x19(25)
1      20:00:00:05:30:00:2a:1e   0xea(234)
61     21:00:05:30:23:1a:11:03    0x19(25)
61     21:00:05:30:23:11:11:11   0x66(102)
61     20:00:00:05:30:00:2a:1e   0xef(239)
```

Example 21-22 Displays Active VSAN-Specific Fabric Binding Information

```
switch# show fabric-binding database active vsan 61
-------------------------------------------------
Vsan   Logging-in Switch WWN     Domain-id
-------------------------------------------------
61     21:00:05:30:23:1a:11:03    0x19(25)
61     21:00:05:30:23:11:11:11   0x66(102)
61     20:00:00:05:30:00:2a:1e   0xef(239)
[Total 3 entries]
```

Example 21-23 Displays Configured VSAN-Specific Fabric Binding Information

```
switch# show fabric-binding database vsan 4
-------------------------------------------------
Vsan   Logging-in Switch WWN     Domain-id
-------------------------------------------------
4      21:00:05:30:23:11:11:11   0x66(102)
4      21:00:05:30:23:1a:11:03    0x19(25)
[Total 2 entries]
```

Example 21-24 Displays Fabric Binding Statistics

```
switch# show fabric-binding statistics
Statistics For VSAN: 1
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 4
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 61
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 345
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 346
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 347
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 348
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 789
```

```
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
Statistics For VSAN: 790
-----------------------
Number of sWWN permit: 0
Number of sWWN deny  : 0

Total Logins permitted  : 0
Total Logins denied     : 0
```

Example 21-25 Displays Fabric Binding Status for Each VSAN

```
switch# show fabric-binding status
VSAN 1 :Activated database
VSAN 4 :No Active database
VSAN 61 :Activated database
VSAN 345 :No Active database
VSAN 346 :No Active database
VSAN 347 :No Active database
VSAN 348 :No Active database
VSAN 789 :No Active database
VSAN 790 :No Active database
```

Example 21-26 Displays Fabric Binding Violations

```
switch# show fabric-binding violations
-------------------------------------------------------------------------------
VSAN Switch WWN [domain] Last-Time [Repeat count] Reason
-------------------------------------------------------------------------------
3 20:00:00:05:30:00:4a:1e [*] Nov 25 05:44:58 2003 [2] sWWN not found
3 20:00:00:05:30:00:4a:1e [0xeb] Nov 25 05:46:14 2003 [2] Domain mismatch
4 20:00:00:05:30:00:4a:1e [*] Nov 25 05:46:25 2003 [1] Database mismatch
```

Note In VSAN 100, the ***** indicates that the sWWN itself was not found in the list. In VSAN 2, the sWWN was found in the list, but has a domain ID mismatch.

Example 21-27 Displays EFMD Statistics

```
switch# show fabric-binding efmd statistics

EFMD Protocol Statistics for VSAN 1
---------------------------------------
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0

EFMD Protocol Statistics for VSAN 4
---------------------------------------
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0
```

```
EFMD Protocol Statistics for VSAN 61
---------------------------------------
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0
```

Example 21-28 Displays EFMD Statistics for a Specified VSAN

```
switch# show fabric-binding efmd statistics vsan 4

EFMD Protocol Statistics for VSAN 4
---------------------------------------
Merge Requests -> Transmitted : 0 , Received : 0
Merge Accepts  -> Transmitted : 0 , Received : 0
Merge Rejects  -> Transmitted : 0 , Received : 0
Merge Busy     -> Transmitted : 0 , Received : 0
Merge Errors   -> Transmitted : 0 , Received : 0
```

Displaying RLIR Information

The Registered Link Incident Report (RLIR) application provides a method for a switchport to send an Link Incident Record (LIR) to a registered Nx-port.

When a LIR is detected in FICON-enabled switches in the Cisco MDS 9000 Family from a RLIR Extended Link Service (ELS). It sends that record to the members in it's Established Registration List (ERL).

In case of multi-switch topology, a Distribute Registered Link Incident Record (DRLIR) Inter Link Service (ILS) is sent to all reachable remote domains along with the RLIR ELS. On receiving the DRLIR ILS, the switch extracts the RLIR ELS and sends to the members of the ERL.

The Nx-ports interested in receiving the RLIR ELS send Link Incident Record Registration (LIRR) ELS request to the management server on the switch. The RLIRs are processed on a per-VSAN basis.

The RLIR application is highly available and the data is written to persistent storage when the **copy running-config startup-config** command is issued.

The **show rlir statistics** command displays the complete statistics of LIRR, RLIR, and DRLIR frames. It lists the number of frames received, sent, and rejected. Specify the VSAN ID to obtain VSAN statistics for a specific VSAN. If you do not specify the VSAN ID, then the statistics are shown for all active VSANs (see Examples 21-29 and 21-30).

Example 21-29 Displays RLIR Statistics for All VSANs

```
switch# show rlir statistics

Statistics for VSAN: 1
----------------------

Number of LIRR received      = 0
Number of LIRR ACC sent      = 0
Number of LIRR RJT sent      = 0
Number of RLIR sent          = 0
Number of RLIR ACC received  = 0
Number of RLIR RJT received  = 0
Number of DRLIR received     = 0
Number of DRLIR ACC sent     = 0
Number of DRLIR RJT sent     = 0
Number of DRLIR sent         = 0
Number of DRLIR ACC received = 0
Number of DRLIR RJT received = 0

Statistics for VSAN: 100
------------------------

Number of LIRR received      = 26
Number of LIRR ACC sent      = 26
Number of LIRR RJT sent      = 0
Number of RLIR sent          = 815
Number of RLIR ACC received  = 815
Number of RLIR RJT received  = 0
Number of DRLIR received     = 417
Number of DRLIR ACC sent     = 417
Number of DRLIR RJT sent     = 0
Number of DRLIR sent         = 914
Number of DRLIR ACC received = 828
Number of DRLIR RJT received = 0
```

Example 21-30 Displays RLIR Statistics for a Specified VSAN

```
switch# show rlir statistics vsan 4

Statistics for VSAN: 4
------------------------

Number of LIRR received      = 0
Number of LIRR ACC sent      = 0
Number of LIRR RJT sent      = 0
Number of RLIR sent          = 0
Number of RLIR ACC received  = 0
Number of RLIR RJT received  = 0
Number of DRLIR received     = 0
Number of DRLIR ACC sent     = 0
Number of DRLIR RJT sent     = 0
Number of DRLIR sent         = 0
Number of DRLIR ACC received = 0
Number of DRLIR RJT received = 0
```

The **show rlir erl** command shows the list of Nx-ports that are registered to receive the RLIRs with the switch. If the VSAN ID is not specified, the details are shown for all active VSANs (see Examples 21-31 and 21-32).

Example 21-31 Displays All ERLs

```
switch# show rlir erl

Established Registration List for VSAN: 2
-------------------------------------------
FC-ID       LIRR FORMAT    REGISTERED FOR
-------------------------------------------
0x0b0200    0x18           always receive
Total number of entries = 1

Established Registration List for VSAN: 100
-------------------------------------------
FC-ID       LIRR FORMAT    REGISTERED FOR
-------------------------------------------
0x0b0500    0x18           conditional receive
0x0b0600    0x18           conditional receive
Total number of entries = 2
```

In Example 21-31, if the `Registered For` column states that an FC ID is `conditional receive`, the source port is registered as a valid recipient of subsequent RLIRs. This source port is selected as an RLIR recipient only if no other ERL recipient is selected.

In Example 21-31, if the `Registered For` column states that an FC ID is `always receive`, the source port is registered as a valid recipient of subsequent RLIRs. This source port is always selected as an LIR recipient.

Note If an *always receive* RLIR is not registered for any N-port or if the delivery of an RLIR fails for one of those ports, then the RLIR is sent to a port registered to *conditional receive* RLIRs.

Example 21-32 Displays ERLs for the Specified VSAN

```
switch# show rlir erl vsan 100
Established Registration List for VSAN: 100
-------------------------------------------------
FC-ID       LIRR FORMAT    REGISTERED FOR
-------------------------------------------------
0x0b0500    0x18           conditional receive
0x0b0600    0x18           conditional receive

Total number of entries = 2
```

Note In Examples 21-33, 21-34, and 21-35, if the host time stamp (marked by the *) is available, it is printed along with the switch time stamp. If the host time stamp is not available, only the switch time stamp is printed.

Example 21-33 Displays the LIR History

```
switch# show rlir history

Link incident history
--------------------------------------------------------------------------------
*Host Time Stamp
 Switch Time Stamp          Port   Interface   Link Incident
--------------------------------------------------------------------------------

*Sun Nov 30 21:47:28 2003
 Sun Nov 30 13:47:55 2003     2        fc1/2   Implicit Incident
*Sun Nov 30 22:00:47 2003
 Sun Nov 30 14:01:14 2003     2        fc1/2   NOS Received
*Sun Nov 30 22:00:55 2003
 Sun Nov 30 14:01:22 2003     2        fc1/2   Implicit Incident
*Mon Dec 1 20:14:26 2003
 Mon Dec  1 12:14:53 2003     4        fc1/4   Implicit Incident
*Mon Dec 1 20:14:26 2003
 Mon Dec  1 12:14:53 2003     4        fc1/4   Implicit Incident
*Thu Dec 4 04:43:32 2003
 Wed Dec  3 20:43:59 2003     2        fc1/2   NOS Received
*Thu Dec 4 04:43:41 2003
 Wed Dec  3 20:44:08 2003     2        fc1/2   Implicit Incident
*Thu Dec 4 04:46:53 2003
 Wed Dec  3 20:47:20 2003     2        fc1/2   NOS Received
*Thu Dec 4 04:47:05 2003
 Wed Dec  3 20:47:32 2003     2        fc1/2   Implicit Incident
*Thu Dec 4 04:48:07 2003
 Wed Dec  3 20:48:34 2003     2        fc1/2   NOS Received
*Thu Dec 4 04:48:39 2003
 Wed Dec  3 20:49:06 2003     2        fc1/2   Implicit Incident
*Thu Dec 4 05:02:20 2003
 Wed Dec  3 21:02:47 2003     2        fc1/2   NOS Received
*Thu Dec 4 05:02:29 2003
 Wed Dec  3 21:02:56 2003     2        fc1/2   Implicit Incident
*Thu Dec 4 05:02:47 2003
 Wed Dec  3 21:03:14 2003     4        fc1/4   NOS Received
*Thu Dec 4 05:02:54 2003
 Wed Dec  3 21:03:21 2003     4        fc1/4   Implicit Incident
*Thu Dec 4 05:02:54 2003
 Wed Dec  3 21:03:21 2003     4        fc1/4   Implicit Incident
...
```

Example 21-34 Displays Recent LIRs for a Specified Interface

```
switch# show rlir recent interface fc1/1-16
Recent link incident records
------------------------------------------------------------------------------
*Host Time Stamp
 Switch Time Stamp          Port   Interface   Link Incident
------------------------------------------------------------------------------
*Thu Dec 4 05:02:29 2003
 Wed Dec  3 21:02:56 2003     2        fc1/2   Implicit Incident
*Thu Dec 4 05:02:54 2003
 Wed Dec  3 21:03:21 2003     4        fc1/4   Implicit Incident
```

Example 21-35 Displays Recent LIRs for a Specified Port Number

```
switch# show rlir recent portnumber 1-16
Recent link incident records
------------------------------------------------------------------------------
*Host Time Stamp
 Switch Time Stamp          Port   Interface   Link Incident
------------------------------------------------------------------------------
*Thu Dec 4 05:02:29 2003
 Wed Dec  3 21:02:56 2003     2        fc1/2   Implicit Incident
*Thu Dec 4 05:02:54 2003
 Wed Dec  3 21:03:21 2003     4        fc1/4   Implicit Incident
```

Clearing RLIR Information

Use the **clear rlir statistics** command to clear all existing statistics for a specified VSAN.

```
switch# clear rlir statistics vsan 1
```

Use the **clear rlir history** command to clear the RLIR history where all link incident records are logged for all interfaces.

```
switch# clear rlir history
```

Use the **clear rlir recent interface** command to clear the most recent RLIR information for a specified interface.

```
switch# clear rlir recent interface fc 1/2
```

Use the **clear rlir recent portnumber** command to clear the most recent RLIT information for a specified port number.

```
switch# clear rlir recent portnumber 16
```

Default Settings

Table 21-4 lists the default settings for FICON features.

Table 21-4 Default FICON Settings

Parameters	Default
FICON feature	Disabled.
Port numbers	Are the same as port addresses.
FC ID last byte value	0 (zero).
EBCDIC format option	US-Cananda.
Switch offline state	Hosts are allowed to move the switch to an offline state.
Mainframe users	Allowed to configure FICON parameters on Cisco MDS switches.
Clock in each VSAN	Same as the switch hardware clock.
Host clock control	Allows host to set the clock on this switch.
SNMP users	Configure FICON parameters.
Port address	Not blocked
Prohibitted ports	0, 241 to 253, and 255.

Table 21-5 lists the default settings for fabric binding features.

Table 21-5 Default Fabric Binding Settings

Parameters	Default
Fabric binding	Disabled.