



## FICON Configuration

---

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.



### Note

FICON features can be implemented in any switch in the Cisco MDS 9000 Family running Cisco MDS SAN-OS Release 1.3(x) or earlier. While no hardware changes are required, you do need the MAINFRAME\_PKG license to configure FICON parameters (see [Chapter 9, “Obtaining and Installing Licenses”](#)).

---

This chapter includes the following sections:

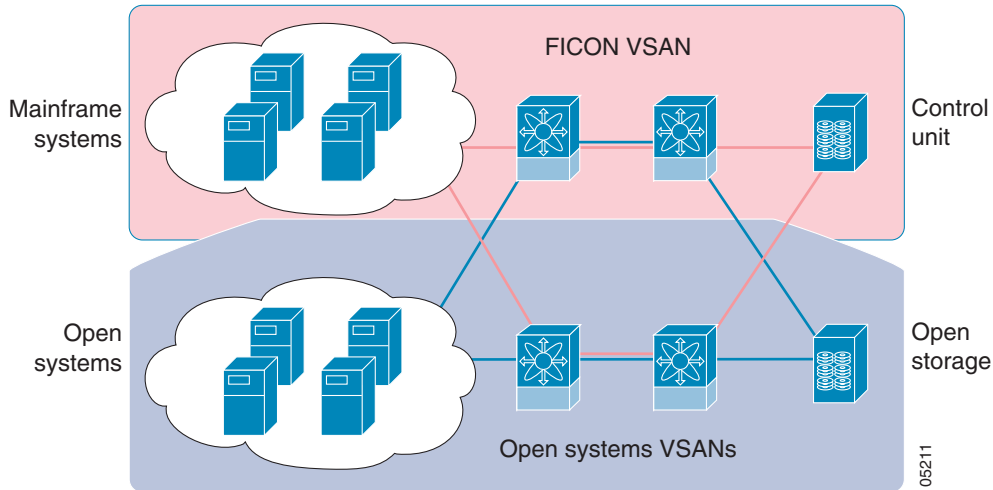
- [About FICON, page 22-2](#)
- [Enabling FICON, page 22-10](#)
- [Configuring FICON Ports, page 22-14](#)
- [FICON Configuration Files, page 22-16](#)
- [Port Swapping, page 22-18](#)
- [Clearing FICON Device Allegiance, page 22-19](#)
- [CUP In-Band Management, page 22-20](#)
- [Fabric Binding Configuration, page 22-20](#)
- [Displaying RLIR Information, page 22-25](#)
- [Calculating FICON Flow Load Balance, page 22-25](#)

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).***

## 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 22-1](#)).

**Figure 22-1 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

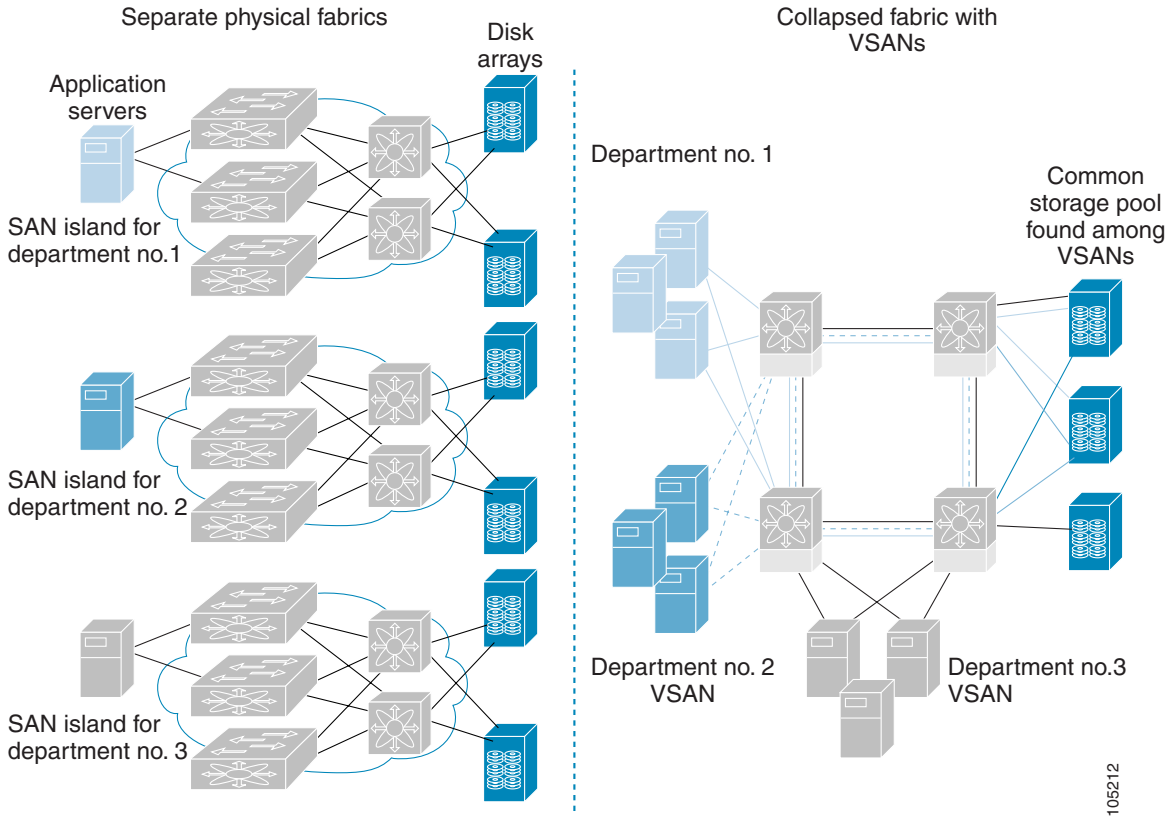
Generally, separate physical fabrics have a high level of switch management and have a higher implementation cost. Further, the ports in each island may be over-provisioned depending on the fabric configuration.

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.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).**

VSANs also help you to move unused ports nondisruptively and provide a common redundant physical infrastructure (see [Figure 22-2](#)).

**Figure 22-2 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 9200 Series 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

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).***

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.

## 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 17, “PortChannel Configuration,”](#) 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 MDS 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 and the 9200 Series.

Refer to the *Cisco MDS 9500 Series Hardware Installation Guide* and the *Cisco MDS 9200 Series 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

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).***

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.

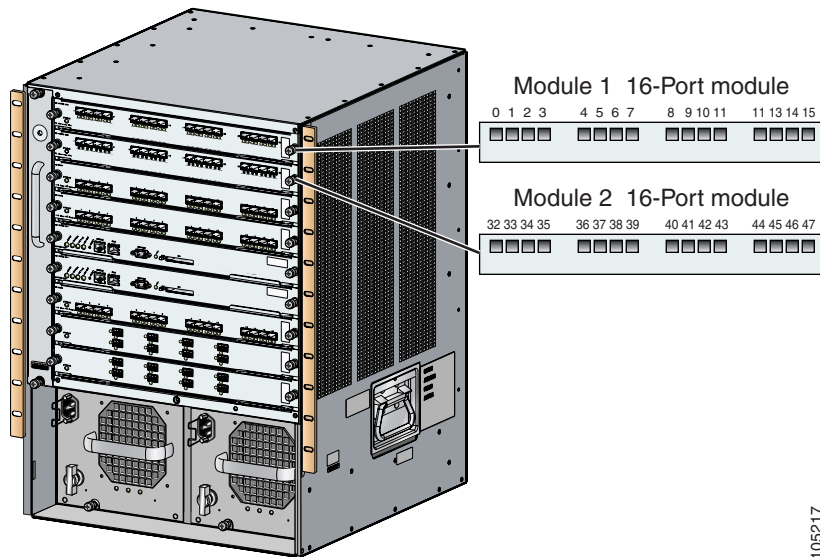
- Infrastructure protection—Common software releases infrastructure protection is available across all Cisco MDS 9000 platforms.
- VSAN technology—The Cisco MDS 9000 Family introduces VSAN technology for hardware-enforced, isolated environments within a single physical fabric for secure sharing of physical infrastructure and enhanced FICON intermix support.
- Port-level configurations—BB\_credits, beacon mode, and port security for each port.
- Alias name configuration—instead of the WWN, for switches and attached node devices.
- 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 [and](#)
- View the local accounting log to locate FICON events.
- 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 [.](#)
- Port address-based configurations—port name, blocked or unblocked state, and the prohibit connectivity attributes. See the [.](#)
- 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 the  section in this chapter.
- Store and apply configuration files.
- FICON and Open Systems Management Server features if installed.
- Enhanced Cascading Support.
- Set the date and time on the switch.
- Configure SNMP trap recipients and community names.
- Call Home configurations—director name, location, description, and contact person.
- Configure preferred domain ID, FC ID persistence, and principle switch priority.
- 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.
- Configure R\_A\_TOV, E\_D\_TOV.
- Perform maintenance tasks for the director including maintaining firmware levels, accessing the director logs, and collecting data to support failure analysis.
- Display and clear port-level incident alerts. [.](#)

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).**

## 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 22-3](#)).

**Figure 22-3** Port Number in the Cisco MDS 9000 Family



105217

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.

**[Send documentation comments to mdsfeedback-doc@cisco.com.](mailto:mdsfeedback-doc@cisco.com)**

Table 22-1 lists the port number assignment for the Cisco MDS 9000 Family of switches and directors.

**Table 22-1 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 9200 Series	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			

## 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 and 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.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).***

## 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.

## Port Addresses

By default, port numbers are the same as port addresses (see the [“Editing FICON Configuration Files” section on page 22-17](#)).

### Implemented and Unimplemented Port Addresses

An implemented port refers to any port address that is available in the chassis.

An unimplemented port refers to any port address that is not available in the chassis.



**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 PortChannel 5, port address 0 is uninstalled in all FICON VSANs.

## 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.



**Note**

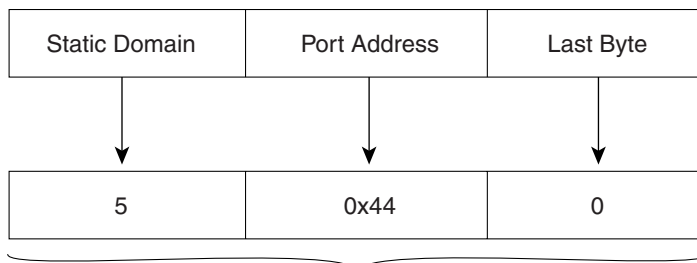
You cannot configure persistent FC IDs in FICON-enabled VSANs.



**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).**

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 22-4](#)).

**Figure 22-4** 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).

113134

## FICON Cascading

The Cisco MDS SAN-OS software allows multiple switches in a FICON network. To configure multiple switches, you must enable and configure fabric binding in that switch.

## FICON VSAN 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 15-15](#).
- Enable in-order delivery on the VSAN.
- Enable (and if required, configure) fabric binding on the VSAN.
- Verify that conflicting persistent FC IDs do not exist in the switch.
- Verify that the configured domain ID and requested domain ID match.
- Add the CUP (area FE) to the zone, if you are using zoning.

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

*Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).*

## Enabling FICON

By default FICON is disabled in all switches in the Cisco MDS 9000 Family. 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.

## Creating FICON VSANs and enabling FICON

When a new FICON VSAN is created, static (insistent) domain IDs, in-order delivery, and fabric binding must be enabled so the FICON VSAN can operate. When you enable the FICON feature in Cisco MDS switches, the following apply:

- The IPL configuration file is automatically created.
- You cannot disable in-order delivery, fabric binding, or static (insistent) domain ID configurations.

To create a FICON VSAN in Fabric Manager, follow these steps:

- 
- Step 1** In Fabric Manager, right-click **All VSANs** in the Logical pane, and click **Create VSAN**. You see the Create VSAN dialog box.
  - Step 2** Select the switches you want to be in the VSAN.
  - Step 3** Enter a VSAN ID.
  - Step 4** Enter the name of the VSAN, if desired.
  - Step 5** Select the type of load balancing, the interop value, and the administrative state for this VSAN.
  - Step 6** Check the **FICON** check box.




---

**Note** You cannot enable interop modes on FICON-enabled VSANs.

---

- Step 7** To enable fabric binding for the selected switches, check that check box.
  - Step 8** Click **Create** to create the new VSAN, or click **Close** to close the dialog without creating the VSAN.
  - Step 9** Open Device Manager for each switch in the FICON VSAN.
  - Step 10** Select **VSANs** from the FC menu. You see the VSANs dialog box.
  - Step 11** Enter the VSAN membership information.
  - Step 12** Click the VSAN you want to become a FICON VSAN and select **Add** from the FICON drop-down list.
  - Step 13** Click **Apply** to save these changes or click **Close** to exit the dialog box without saving changes.
- 

To create a FICON VSAN in Device Manager, follow these steps:

- 
- Step 1** Choose **FC > VSANs**. You see the VSANs configuration dialog box.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).***

- Step 2** Click **Create VSAN**. You see the Create VSAN dialog box.
  - Step 3** Enter a VSAN ID.
  - Step 4** Enter the name of the VSAN, if desired.
  - Step 5** Select the type of load balancing, the interop value, and the administrative state for this VSAN.
  - Step 6** Check the **FICON** check box.
  - Step 7** To enable fabric binding for the selected switches, check that check box.
  - Step 8** Click **Create** to create the FICON VSAN, or click **Close** to close the dialog without creating the FICON VSAN.
- 

## Deleting FICON VSANs

To delete a FICON VSAN in Fabric Manager, follow these steps:

- Step 1** Choose **All VSANS**. You see the VSAN table in the Information pane.
- Step 2** Click anywhere in the row for the VSAN which you want to delete.
- Step 3** Click the **Delete Row** icon to delete the VSAN.



**Note** Deleting the VSAN will also delete the associated FICON configuration file, and the file cannot be recovered.

---

To delete a FICON VSAN in Device Manager, follow these steps:

- Step 1** Choose **FICON > VSANs**. You see the VSAN dialog box.
- Step 2** Click the VSAN you want to disable FICON on.
- Step 3** Select **Remove** from the FICON drop-down list.
- Step 4** Click **Apply** to disable FICON on this VSAN or click **Close** to close the dialog box without making any changes.



**Note** Deleting the VSAN will also delete the associated FICON configuration file, and the file cannot be recovered.

---

[Send documentation comments to mdsfeedback-doc@cisco.com.](mailto:mdsfeedback-doc@cisco.com)

## Viewing FICON Director History

To view FICON director history, follow these steps:

- 
- Step 1** In Device Manager, select **VSANs** from the **FICON** menu. You see the FICON VSAN configuration dialog box.
  - Step 2** Click the **VSANs** tab if it is not already displayed.
  - Step 3** Click anywhere in the row for the VSAN for which you want to configure port information.
  - Step 4** Click the **Director History** button to display a history of FICON-related changes to this switch.
- 

## The code-page Option

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.

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 modify the code-page option using Device Manager, follow these steps:

- 
- Step 1** Select **VSANs** from the **FICON** menu. You see the FICON VSAN configuration dialog box.
  - Step 2** Click the **VSANs** tab if it is not already displayed.
  - Step 3** Choose the code-page option from the drop-down menu in the CodePage field for the FICON VSAN you want to configure.
  - Step 4** Click **Apply** to save these changes or click **Close** to exit the dialog box without saving changes.
- 

## 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.

*Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).*

## FICON Host Control

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 MDS 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 MDS 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.

To allow the host (mainframe) to control the Cisco MDS switch using Device Manager, follow these steps:

- 
- Step 1** Select **VSANs** from the FICON menu. You see the FICON VSAN configuration dialog box.
  - Step 2** Click the **VSANs** tab if it is not already displayed.
  - Step 3** Check the **Offline Sw** check box under Host can to allow the mainframe to move a switch to the offline state.
  - Step 4** Check the **Sync Time** check box under Host can to allow the mainframe to set the system time on the switch.
  - Step 5** Click **Apply** to save these changes or click **Close** to exit the dialog box without saving changes.
- 

## Host Changes FICON Port Parameters

By default, mainframe users are not allowed to configure FICON parameters on Cisco MDS switches—they can only query the switch.

To allow the host (mainframe) to configure FICON parameters on the Cisco MDS switch using Device Manager, follow these steps:

- 
- Step 1** Select **VSANs** from the FICON menu. You see the FICON VSAN configuration dialog box.
  - Step 2** Click the **VSANs** tab if it is not already displayed.
  - Step 3** Check the **By Host** check box under Port Control to allow the mainframe to control a switch.
  - Step 4** Check the **By SNMP** check box under Port Control can to allow SNMP users to configure FICON on the switch.
  - Step 5** Click **Apply** to save these changes or click **Close** to exit the dialog box without saving changes.
- 



### Note

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

---

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).***

## FICON Information Refresh Note

When viewing FICON information through the Device Manager dialog boxes, you must manually refresh the display by clicking the Refresh button in order to see the latest updates. This is true whether you configure FICON through the CLI or through the Device Manager.

There is no automatic refresh of FICON information. This information would be refreshed so often that it would affect performance.

## 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.

## Port Blocking

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).

---

If a port is shut down, unblocking that port does not initialize the port.

## Port Prohibiting

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.



### 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.

---

*Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).*

## Configuring Port Blocking and Port Prohibiting

To configure port blocking or port prohibiting for FICON using Device Manager, follow these steps:

- 
- Step 1** .Select **VSANs** from the FICON menu. You see the FICON VSAN configuration dialog box.
  - Step 2** Click the **VSANs** tab if it is not already displayed.
  - Step 3** Click the **Port Configuration**. You see the FICON Port Configuration dialog box.
  - Step 4** Set the port block and prohibit configuration for the selected FICON VSANs.
  - Step 5** Click **Apply** to save these changes or click **Close** to exit the dialog box without saving changes.
- 

## Entering FICON Port Configuration Information

**Note**

To view the latest FICON information, you must click the **Refresh** button. See the “[FICON Information Refresh Note](#)” section on page 22-14.

---

To display FICON port configuration information, follow these steps:

- 
- Step 1** In Device Manager, select **VSANs** from the FICON menu.  
You see the FICON VSAN configuration dialog box.
  - Step 2** Click the **VSANs** tab.
  - Step 3** Click anywhere in the row for the VSAN for which you want to configure port information.
  - Step 4** Click **Port Configuration** to display the Port Configuration dialog box.
  - Step 5** Enter the Port Configuration information. Click **Apply** to save the configuration information, or click **Cancel** to exit the dialog without saving.
-

*Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).*

## Viewing FICON Port Attributes



### Note

To view the latest FICON information, you must click the **Refresh** button. See the “[FICON Information Refresh Note](#)” section on page 22-14.

To view FICON port attributes, follow these steps:

- 
- Step 1** In Device Manager, select **VSANs** from the FICON menu.  
You see the FICON VSAN configuration dialog box.
- Step 2** Click the **VSANs** tab.
- Step 3** Click anywhere in the row for the VSAN for which you want to configure port information.
- Step 4** Click **Port Attributes** to display the Port Attributes dialog box.
- 

## 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.



*Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).*

## 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 MDS 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.

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.



### Note

---

To view the latest FICON information, you must click the **Refresh** button. See the “[FICON Information Refresh Note](#)” section on page 22-14.

---

## Copying FICON Configuration Files

The Cisco MDS SAN-OS software maintains different configuration files to support a FICON network. These configuration files can be saved using the copy running-config startup-config command, or using Device Manager. FICON configuration files do not contain the following information that is normally saved with the running configuration:



### Note

---

To view the latest FICON information, you must click the **Refresh** button. See the [FICON Information Refresh Note, page 22-14](#) for more information.

---

- Port number to port address mapping
- PortChannel to port number mapping
- Port swap occurrences
- FICON enabled VSANs

FICON configuration files are independent of these parameters. Instead, this information is stored in persistent storage as they can be modified independent of the startup configuration.

## 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.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).***

## Managing FICON Configuration Files In Device Manager

To manage a FICON file using Device Manager, follow these steps:

- 
- Step 1** Select **VSANS** from the **FICON** menu. You see the FICON VSANs dialog box.
  - Step 2** Click the **Files** tab.
  - Step 3** Click **Create** to create a new FICON configuration file.
    - a.** Enter the VSAN ID for the FICON VSAN you want to configure.
    - b.** Enter the file name and the description.
    - c.** Click **Create** to create the new file, or click **Close** to close the dialog without creating the file.
  - Step 4** Click **Copy** to copy the file to a new file.
  - Step 5** Click **Open** to edit the FICON configuration file.
  - Step 6** Click **Delete** to delete the FICON configuration file.
  - Step 7** Click **Apply** to apply the FICON configuration file.
- 

## 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 you check the **Active = Saved** check box on any FICON VSAN, then the swapped configuration is automatically saved to startup. Otherwise, you must explicitly save the running configuration immediately after swapping the ports.

---

Once you swap ports, 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, you must explicitly shut down the port to resume traffic.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).***

## 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 MDS 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 18-5).

## Swapping FICON Ports



### Note

To view the latest FICON information, you must click the **Refresh** button. See the [“FICON Information Refresh Note”](#) section on page 22-14 for more information.

To swap ports using Device Manager, follow these steps:

- Step 1** Select two Fibre Channel ports, by holding down the **CTRL** key and clicking on them with the mouse.
- Step 2** Select **Swap Selected Ports** from the FICON menu.

## 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.



### Caution

This task terminates the currently executing session.

[Send documentation comments to mdsfeedback-doc@cisco.com.](mailto:mdsfeedback-doc@cisco.com)

## 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.

## Fabric Binding Configuration

The Cisco MDS SAN-OS Release 1.3(x) 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.

## Port Security Versus Fabric Binding

Port security and fabric binding are two independent features that can be configured to complement each other (see [Table 22-2](#)).

**Table 22-2** *Fabric Binding and Port Security Comparison*

<b>Fabric Binding</b>	<b>Port Security</b>
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.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).***

**Table 22-2 Fabric Binding and Port Security Comparison (continued)**

<b>Fabric Binding</b>	<b>Port Security</b>
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.

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | Enable the fabric configuration feature.  |
| <b>Step 2</b> | Configure a list of sWWNs and their corresponding domain IDs for devices that are allowed to access the fabric. |
| <b>Step 3</b> | Activate the fabric binding database.   |
| <b>Step 4</b> | Save the fabric binding configuration.  |
| <b>Step 5</b> | 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.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).***

To enable fabric binding using Fabric Manager, follow these steps:

- 
- Step 1** Choose **Fabric > VSAN<sub>xxx</sub> > Fabric Binding** in the Logical Domain pane and then click the **Controls** tab in the Information pane.
  - Step 2** Set the Command drop-down menu to **enable** for the VSAN(s) on which you want to enable fabric binding.
  - Step 3** Click the **Apply Changes** icon in the Information pane to enable fabric binding.
- 

## 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 switches for fabric binding using Fabric Manager, follow these steps:

- 
- Step 1** Choose **Fabric > VSAN<sub>xxx</sub> > Fabric Binding** in the Logical Domain pane and then click the **Config Database** tab in the Information pane.
  - Step 2** Click the **Create Row** icon to add a switch to the list of allowed switches for fabric binding.
  - Step 3** Click the **Apply Changes** icon in the Information pane to enable the fabric binding.
- 

## 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.

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.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).***

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 `forceActivate` option.

To activate fabric binding, follow these steps:

- 
- Step 1** In Fabric Manager, select **Fabric > VSANxxx > Fabric Binding** in the Logical Domain pane and then click the **Actions** tab in the Information pane.
  - Step 2** Set the Action drop-down menu to **activate** or **forceActivate** for the VSAN(s) for which you want to activate fabric binding.
  - Step 3** Click the **Apply Changes** icon in the Information pane to activate the fabric binding.
- 

## 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.



### Caution

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

---

## Deactivating Fabric Binding

To deactivate fabric binding, follow these steps:

- 
- Step 1** In Fabric Manager, select **Fabric > VSANxxx > Fabric Binding** and then click the **Actions** tab in the Information pane.
  - Step 2** Set the Action drop-down menu to **deactivate** for the VSAN(s) for which you want to deactivate fabric binding.
  - Step 3** Click the **Apply Changes** icon to deactivate the fabric binding.
- 

## Fabric Binding CopyActive to Config

To copy the active fabric binding to the configuration file, follow these steps:

- 
- Step 1** In Fabric Manager, select **Fabric > VSANxxx > Fabric Binding** in the Logical Domains pane and then click the **Actions** tab in the Information pane.
  - Step 2** Click the **CopyActive ToConfig** check box for the VSAN(s) for which you want to copy fabric binding.
  - Step 3** Click the **Apply Changes** icon to copy the fabric binding.
-

*Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).*

## Creating a Fabric Binding Configuration

To create a fabric binding configuration, follow these steps:

- 
- Step 1** In Fabric Manager, select **Fabric > VSANxxx > Fabric Binding** in the Logical Domains pane and then click the **Config Database** tab in the Information pane.
  - Step 2** Click **Create** to display the Config Database - Create dialog box.
  - Step 3** Enter the VSAN ID, the peer WWN, and the domain ID.
  - Step 4** Click the **Create Row** icon to create the fabric binding configuration.
- 

## Deleting a Fabric Binding Configuration

To delete a fabric binding configuration, follow these steps:

- 
- Step 1** In Fabric Manager, select **Fabric > VSANxxx > Fabric Binding** in the Logical Domains pane and then click the **Config Database** tab in the Information pane.
  - Step 2** Click in the row for the VSAN for which you want to delete the fabric binding configuration.
  - Step 3** Click the **Delete Row** icon to delete the fabric binding configuration.
- 

## Viewing Fabric Binding Active Database

To view the fabric binding active database, follow these steps:

- 
- Step 1** In Fabric Manager, select **Fabric > VSANxxx > Fabric Binding** and click the **Active Database** tab. You see the active database.
- 

## Viewing Fabric Binding Violations

To view fabric binding violations, follow these steps:

- 
- Step 1** In Fabric Manager, select **Fabric > VSANxxx > Fabric Binding** and click the **Violations** tab. You see the violations.
-



*Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).*

## Clearing Fabric Binding Statistics

To clear fabric binding statistics, follow these steps:

- 
- Step 1** In Fabric Manager, select **Fabric > VSANxxx > Fabric Binding** and click the **Statistics** tab.  
You see the statistics in the Information pane.
  - Step 2** Check the **Clear** check box for the VSAN(s) for which you want to clear statistics.
  - Step 3** Click the **Apply Changes** icon.
- 

## Viewing EFMD Statistics

To view EFMD statistics, follow these steps:

- 
- Step 1** In Fabric Manager, select **Fabric > VSANxxx > Fabric Binding** and click the **EFMD Statistics** tab.
  - Step 2** You see the EFMD statistics.
- 

## Displaying RLIR Information

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

When a Link Incident Record (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 its 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.

To view RLR information using Device Manager, follow these steps:

- 
- Step 1** Choose **FICON > RLIR ERL....** You see the Show RLIR ERL dialog box.
  - Step 2** Click **Close** to close the dialog box.
- 

## Calculating FICON Flow Load Balance

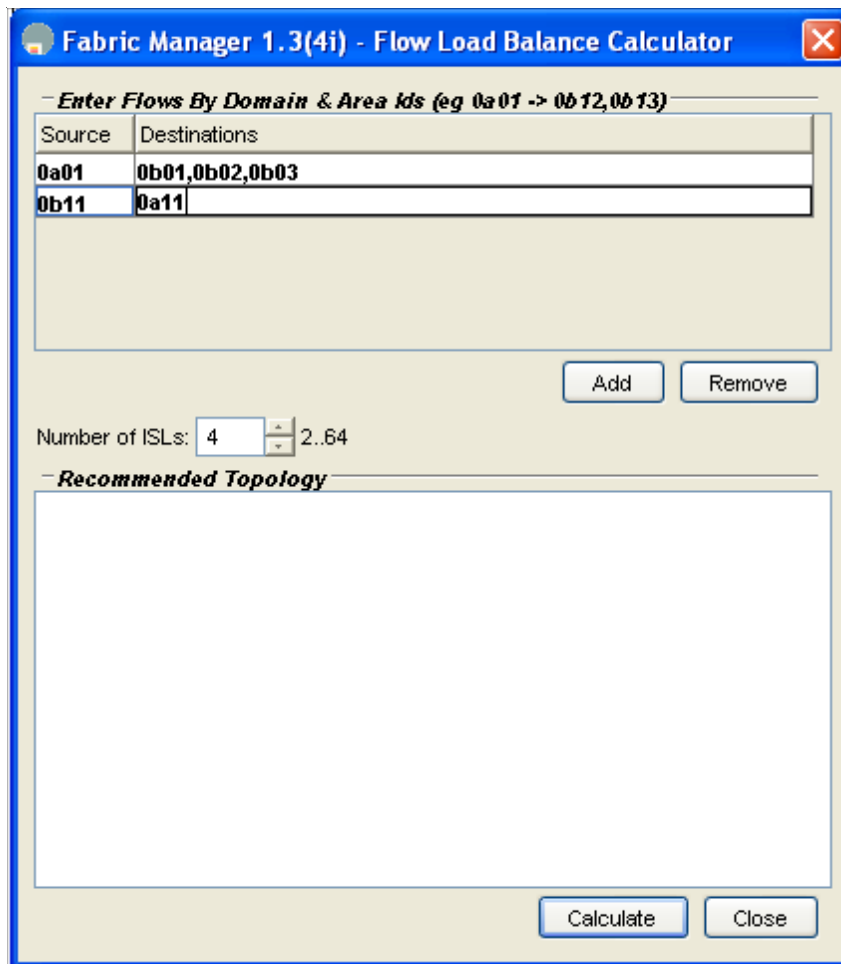
The FICON Flow Load Balance Calculator allows you to get the best load balancing configuration for your FICON flows. The calculator does not rely on any switch or flow discovery in the fabric. It is available from the Fabric Manager Tools menu.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).**

To use the FICON Flow Load Balance calculator, follow these steps:

- Step 1** Click **Tools > Other > FICON Flow Load Balance Calculator**. You see the Flow Load Balance Calculator (see [Figure 22-5](#)).
- Step 2** Click **Add** to enter the source and destination(s) flows.  
Use 2 byte hex (Domain and Area IDs) as shown in [Figure 22-5](#). You can copy and paste these IDs, and then edit them if you need to. To remove a row, select it and click **Remove**.

**Figure 22-5** *Flow Load Balance Calculator - Initial Screen*



- Step 3** Enter (or select) the number of ISLs between the two switches (for example, between Domain ID 0a and 0b in [Figure 22-5](#).)
- Step 4** Click **Calculate** to show the recommended topology

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).**

In the example shown in Figure 22-6, there are 12 ISLs between domains 0a and 0b with 13 flows. In this case, the best balance is 2 Port Channels with 2 members each, and 8 regular ISLs.

Figure 22-6 Flow Load Balance Calculator - Example

**Fabric Manager 1.3(4i) - Flow Load Balance Calculator**

— Enter Flows By Domain & Area Ids (eg 0a01 -> 0b12,0b13)

Source	Destinations
0a01	0b01,0b02,0b03
0b11	0a11,0af0
0a02	0b01,0b02,0b03
0b12	0a11,0a12
0a03	0b04,0b05,0b06

Add Remove

Number of ISLs: 12 2.64

— Recommended Topology

```
# 1: Port Channel with 2 ISL members
# 2: Port Channel with 2 ISL members
# 3: ISL
# 4: ISL
# 5: ISL
# 6: ISL
# 7: ISL
# 8: ISL
# 9: ISL
# 10: ISL
```

Calculate Close



**Note**

If you change flows or ISLs, you must click **Calculate** to see the new recommendation.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com).***