CHAPTER 28

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 (see Chapter 38, "Configuring Fabric Binding"). The Registered Link Incident Report (RLIR) application provides a method for a switch port to send an LIR to a registered Nx port.

Note Cisco Fabric Manager release 3.x does not support FICON management of Cisco MDS 9000 Family switches running SAN-OS release 2.(x).

This chapter includes the following sections:

About FICON

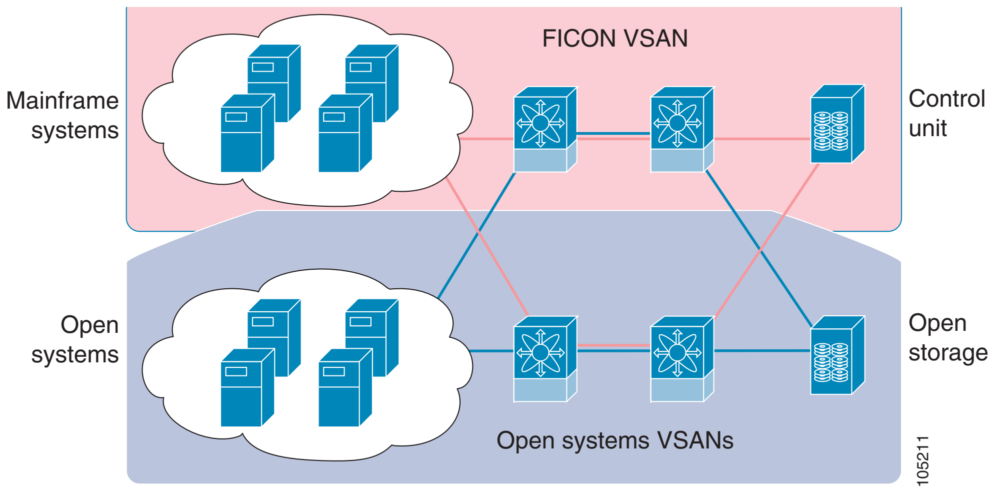
The FICON feature is not supported on:

- Cisco MDS 9120 switches
- Cisco MDS 9124 switches
- Cisco MDS 9140 switches

- The 32-port Fibre Channel switching module
- Cisco Fabric Switch for HP c-Class BladeSystem
- Cisco Fabric Switch for IBM BladeSystem

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 28-1).

Figure 28-1 Shared System Storage Network



FCP and FICON are different FC4 protocols and their traffic is independent of each other. Devices using these protocols should be isolated using VSANs.

This section includes the following topics:

- FICON Requirements, page 28-2
- MDS-Specific FICON Advantages, page 28-3
- FICON Cascading, page 28-7
- FICON VSAN Prerequisites, page 28-7

FICON Requirements

The FICON feature has the following requirements:

- You can implement FICON features in the following switches:
  - Any switch in the Cisco MDS 9500 Series.
  - Any switch in the Cisco MDS 9200 Series (including the Cisco MDS 9222i Multiservice Modular Switch).
  - Cisco MDS 9134 Multilayer Fabric Switch.
  - MDS 9000 Family 18/4-Port Multiservice Module.

- You need the MAINFRAME_PKG license to configure FICON parameters. To extendyour FICON configuration over a WAN link using FCIP, you need the appropriate SAN_EXTN_OVER_IP license for the module you are using. For more information, see Chapter 10, "Obtaining and Installing Licenses".

MDS-Specific FICON Advantages

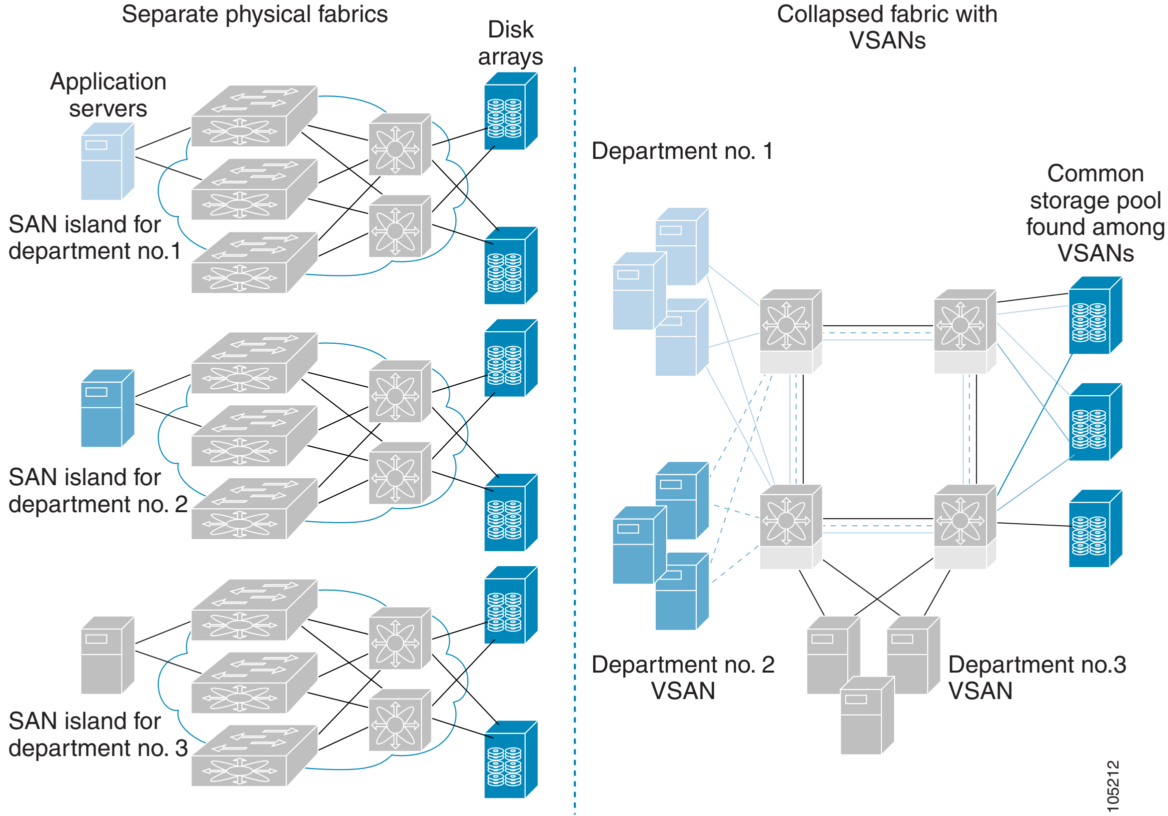
This section explains the additional FICON advantages in Cisco MDS switches and includes the following topics:

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 nondisruptively and provide a common redundant physical infrastructure (see Figure 28-2).

Figure 28-2 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 VSANs in any Cisco MDS switch, you can enable FICON in at most eight of these VSANs. The number of VSANs configured depends on the platform.

Note Mainframe users can think of VSANs as being like FICON LPARs in the MDS SAN fabric. You can partition switch resources into FICON LPARs (VSANs) that are isolated from each other, in much the same way that you can partition resources on a zSeries or DS8000. Each VSAN has its own set of fabric services (such as fabric server and name server), FICON Control Unit Port, domain ID, Fabric Shortest Path First (FSPF) routing, operating mode, IP address, and security profile.

FICON LPARs can span line cards and are dynamic in size. For example, one FICON LPAR with 10 ports can span 10 different line cards. FICON LPARs can also include ports on more than one switch in a cascaded configuration. The consistent fairness of the Cisco MDS 9000 switching architecture means that “all ports are created equal”, simplifying provisioning by eliminating the “local switching” issues seen on other vendors’ platforms.

Addition of ports to a FICON LPAR is a non-disruptive process. The maximum number of ports for a FICON LPAR is 255 due to FICON addressing limitations.

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 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 thus simplifies business continuance strategies.

See Chapter 48, "Configuring FCIP."

PortChannel Support

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

See Chapter 23, "Configuring PortChannels" for more information on PortChannels.

VSANs for FICON and FCP Mixing

Cisco MDS 9000 Family FICON-enabled switches simplify deployment of even the most complex mixed environments. Multiple logical FICON, Z-Series Linux/FCP, and Open-Systems Fibre Channel Protocol (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 mixed 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. Mixed environments are addressed by the Cisco SAN-OS software. The challenge of mixing 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 mixing at the port level. If these protocols are mixed in the same switch, you can use VSANs to isolate FCP and FICON ports.

Tip When creating a mixed 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 528 autosensing, 4/2/1-Gbps, 10-Gbps, FICON or FCP ports in any combination in a single chassis. See Chapter 17, "Configuring High Availability."
- Infrastructure protection—Common software releases provide infrastructure protection across all Cisco MDS 9000 platforms. See Chapter 15, "Software Images."
- VSAN technology—The Cisco MDS 9000 Family provides VSAN technology for hardware-enforced, isolated environments within a single physical fabric for secure sharing of physical infrastructure and enhanced FICON mixed support. See Chapter 1, "Configuring and Managing VSANs."
- Port-level configurations—There are BB_credits, beacon mode, and port security for each port. See the "About Buffer-to-Buffer Credits" section on page 20-20, "Identifying the Beacon LEDs" section on page 20-14, and Chapter 24, "Configuring Trunking."
- Alias name configuration—Provides user-friendly aliases instead of the WWN for switches and attached node devices. See Chapter 30, "Configuring and Managing Zones."
- Comprehensive security framework—The Cisco MDS 9000 Family supports RADIUS and TACACS+ 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 32, "Configuring RADIUS and TACACS+" Chapter 36, "Configuring FC-SP and DHCHAP," and Chapter 38, "Configuring Fabric Binding."
- Traffic encryption—IPSec is supported over FCIP. You can encrypt FICON and Fibre Channel traffic that is carried over FCIP. See Chapter 35, "Configuring IPsec Network Security."
- Local accounting log—View the local accounting log to locate FICON events. See the "MSCHAP Authentication" section on page 32-24 and "Local AAA Services" section on page 32-26.
- 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 28-37.
- Port address-based configurations—Configure port name, blocked or unblocked state, and the prohibit connectivity attributes. See the "Configuring FICON Ports" section on page 28-24.
- You can 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 "Calculating FICON Flow Load Balance" section on page 28-39.
- Configuration files—Store and apply configuration files. See the "FICON Configuration Files" section on page 28-28.
- FICON and Open Systems Management Server features if installed. —See the "VSANs for FICON and FCP Mixing" section on page 28-5.
- Enhanced cascading support—See the "CUP In-Band Management" section on page 28-37.

- Date and time—Set the date and time on the switch. See the "Allowing the Host to Control the Timestamp" section on page 28-22.
- Configure SNMP trap recipients and community names—See the "Configuring SNMP Control of FICON Parameters" section on page 28-22.
- Call Home configurations—Configure the director name, location, description, and contact person. See Chapter 64, "Configuring Call Home."
- Configure preferred domain ID, FC ID persistence, and principal switch priority—See Chapter 25, "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 52, "Monitoring Network Traffic Using SPAN."
- Configure R_A_TOV, E_D_TOV—— See the "Fibre Channel Time Out Values" section on page 29-2.
- Director-level maintenance tasks—Perform maintenance tasks for the director including maintaining firmware levels, accessing the director logs, and collecting data to support failure analysis. See Chapter 59, "Monitoring System Processes and Logs."

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 (see the "Calculating FICON Flow Load Balance" section on page 28-39).

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 "About the Default Zone" section on page 30-21.
- Enable in-order delivery on the VSAN. See Chapter 25, "Configuring Fibre Channel Routing Services and Protocols."
- Enable (and if required, configure) fabric binding on the VSAN. See the "Calculating FICON Flow Load Balance" section on page 28-39. Chapter 38, "Configuring Fabric Binding."
- Verify that conflicting persistent FC IDs do not exist in the switch. See Chapter 25, "Configuring Domain Parameters."
- Verify that the configured domain ID and requested domain ID match. See Chapter 25, "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 28-37.

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

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*. A maximum of 255 port numbers are available. You can use the following port numbering schemes:

- Default port numbers based on the chassis type
- Reserved port numbers

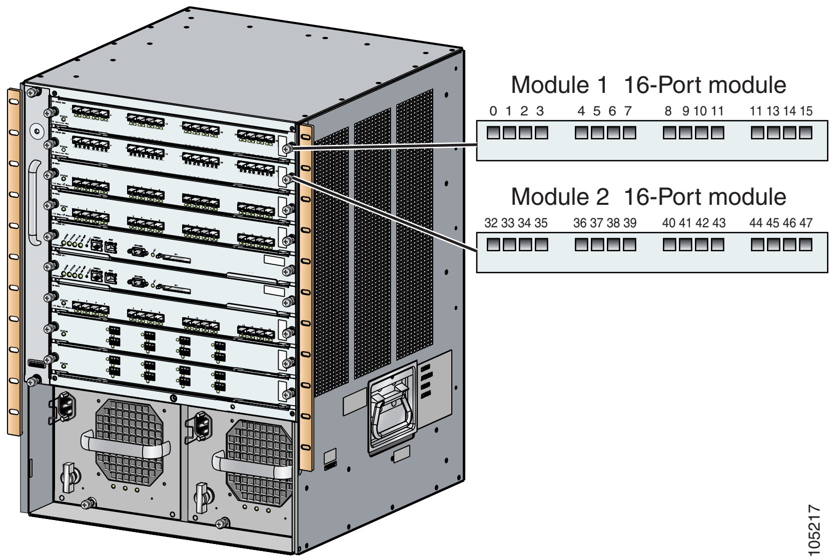
This section includes the following topics:

Note You must enable FICON on the switch before reserving FICON port number (see the About Enabling FICON on a VSAN, page 28-15).

Default FICON Port Numbering Scheme

Default FICON port numbers are assigned by the Cisco MDS SAN-OS software based on the module and the slot in the chassis. The first port in a switch always starts with a zero (0) (see Figure 28-3).

Figure 28-3 Default FICON Port Number in Numbering on the Cisco MDS 9000 Family9509 Switch



The default 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. Thirty-two (32) port numbers are assigned to each slot on all Cisco MDS 9000 Family switches except for the Cisco MDS 9513 Director, which has 16 port numbers assigned for each slot. These default numbers are assigned regardless of the module's physical presence in the chassis, the port status (up or down), or the number of ports on the module (4, 12, 16, 24, or 48). If a module has fewer ports than the number of port numbers assigned to the slot, then the excess port numbers are unused. If a module has more ports than the number of port numbers assigned to the slot, the excess ports cannot be used for FICON traffic unless you manually assign the port numbers.

Note Follow the steps in "Assigning FICON Port Numbers to Slots" section on page 28-13 to make use of excess ports by manually assigning more port numbers to the slot. Before doing this, however, we recommend that you review the default port number assignments for Cisco MDS 9000 switches shown in Table 28-3 on page 28-42, and that you read the following sections to gain a complete understanding of FICON port numbering: "About the Reserved FICON Port Numbering Scheme" section on page 28-11, "FICON Port Numbering Guidelines" section on page 28-12, and "Assigning FICON Port Numbers to Slots" section on page 28-13.

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 28-3 lists the default port number assignment for the Cisco MDS 9000 Family of switches and directors.

Table 28-1 Default 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			
Cisco MDS 9222i Series	Slot 1	0 through 31	64 through 89	90 through 253 and port 255	The first 4, 12, 16, or 24 port numbers in a 4-port, 12-port, 16-port, or 24-port module are used and the rest remain unused. Extra 16 ports on 48-port modules are not allocated numbers.
	Slot 2	32 through 63			
Cisco MDS 9506 Director	Slot 1	0 through 31	128 through 153	154 through 253 and port 255	Supervisor modules are not allocated port numbers.
	Slot 2	32 through 63			
	Slot 3	64 through 95			
	Slot 4	96 through 127			
	Slot 5	None			
	Slot 6	None			
Cisco MDS 9134 Director	Slot 1	0 through 33	34 through 59	60 through 253 and port 255	
Cisco MDS 9509 Director	Slot 1	0 through 31	224 through 249	250 through 253 and port 255	The first 4, 12, 16, or 24 port numbers in a 4-port, 12-port, 16-port, or 24-port module are used and the rest remain unused. Extra 16 ports on 48-port modules are not allocated port numbers.
	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 4, 12, 16, or 24 port numbers are used for a 4-port, 12-port,16-port, or 24-port module and the rest remain unused. Extra 16 ports on 48-port modules are not allocated port numbers.
	Slot 8	160 through 191			
	Slot 9	192 through 223			

Send documentation comments to mdsfeedback-doc@cisco.com

Table 28-1 Default FICON Port Numbering in the Cisco MDS 9000 Family (continued)

Product	Slot Number	Implemented Port Allocation		Unimplemented Ports	Notes
		To Ports	To PortChannel/FCIP		
Cisco MDS 9513 Director	Slot 1	0 through 15	224 through 249	250 through 253 and port 255	The first 4, 12 or 16 port numbers are used for a 4-port, 12-port or 16-port module and the rest remain unused. Extra ports on 24-port, 32-port, and 48-port modules are not allocated port numbers.
	Slot 2	16 through 31			
	Slot 3	32 through 47			
	Slot 4	48 through 63			
	Slot 5	64 through 79			
	Slot 6	80 through 95			
	Slot 7	None			Supervisor modules are not allocated port numbers.
	Slot 8	None			
	Slot 9	96 through 111			The first 4 or 12 port numbers are used for a 4-port or 12-port module and the rest remain unused. Extra ports on 24-port, 32-port, and 48-port modules are not allocated port numbers.
	Slot 10	112 through 127			
	Slot 11	128 through 143			
	Slot 12	144 through 159			
	Slot 13	160 through 175			

Port Addresses

By default, port numbers are the same as port addresses. You can swap the port addresses (see the "Port Swapping" section on page 28-31).

Implemented and Unimplemented Port Addresses

An implemented port refers to any port address that is assigned by default to a slot in the chassis (see Table 28-3). An unimplemented port refers to any port address that is not assigned by default to a slot in the chassis (see Table 28-3).

About the Reserved FICON Port Numbering Scheme

A range of 250 port numbers are available for you to assign to all the ports on a switch. Table 28-3 shows that you can have more than 250 physical ports on a switch and the excess ports do not have port numbers in the default numbering scheme. When you have more than 250 physical ports on your switch, you can have ports without a port number assigned if they are not in a FICON VSAN, or you can assign duplicate port numbers if they are not used in the same FICON VSAN. For example, you can configure port number 1 on interface fc1/1 in FICON VSAN 10 and fc10/1 in FICON VSAN 20.

Note A VSAN can have a maximum of 250 port numbers.

Note FICON port numbers are not changed for ports that are active. You must first disable the interfaces using the **shutdown** command.

Note You can configure port numbers even when no module is installed in the slot.

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.
- For slot 1, ports 0 to 31, or 0 to 15 have been assigned. Only the physical port fc1/5 with port number 4 is in VSAN 2. The rest of the physical ports are not in VSAN 2. The port numbers 0 to 249 are considered implemented for any FICON-enabled VSAN. Therefore, VSAN 2 has port numbers 0 to 249 and one physical port, fc1/4. The corresponding physical ports 0 to 3,and 5 to 249 are not in VSAN 2. When the FICON VSAN port address is displayed, those port numbers with the physical ports not in VSAN 2 are not installed (for example, ports 0 to 3, or 5 to 249).

  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 Table 28-3.

FICON Port Numbering Guidelines

The following guidelines apply to FICON port numbers:

- Supervisor modules do not have port number assignments.
- Port numbers do not change based on TE ports. Since TE ports appear in multiple VSANs, chassis-wide unique port numbers should be reserved for 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, then the associated ports will not come up.

  See the "About Port Numbers for FCIP and PortChannel" section on page 28-13.

Assigning FICON Port Numbers to Slots

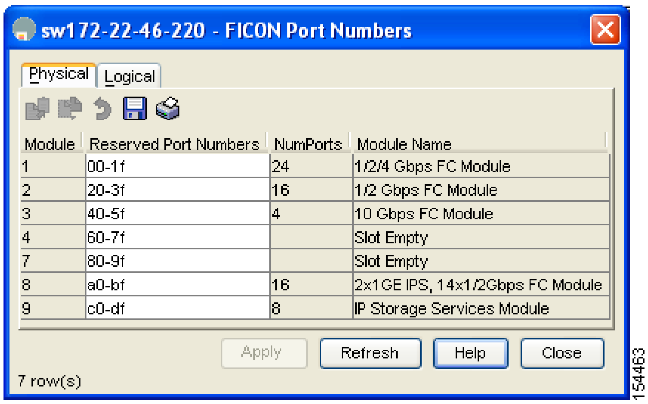
Caution When you assign, change, or release a port number, the port reloads.

To assign FICON port numbers to slots using Device Manager, follow these steps:

Step 1 Click **FICON** and then select **Port Numbers**.

You see the FICON port numbers (see Figure 28-4).

Figure 28-4 FICON Port Numbers



Step 2 Enter the chassis slot port numbers in the Reserved Port Numbers field.

Step 3 Click **Apply**.

About Port Numbers for FCIP and PortChannel

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

See the "Configuring FICON Ports" section on page 28-24 and the "Reserving FICON Port Numbers for FCIP and PortChannel Interfaces" section on page 28-13.

You can use the default port numbers if they are available (see Table 28-1 on page 28-10) or if you reserve port numbers from the pool of port numbers that are not reserved for Fibre Channel interfaces (see the "FICON Port Numbering" section on page 28-8).

Reserving FICON Port Numbers for FCIP and PortChannel Interfaces

You must reserve port numbers for logical interfaces, such as FCIP and PortChannels, if you plan to use them.

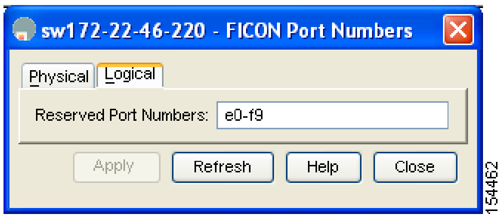
To reserve FICON port numbers for FCIP and PortChannel interfaces using Device Manager, follow these steps:

Step 1 Click **FICON** > **Port Numbers.**

You see the FICON port numbers dialog box (see Figure 28-4).

Step 2 Click the **Logical** tab to see the reserved port numbers for the slot (see Figure 28-5).

Figure 28-5 Reserved Port Numbers for the Selected Slot



Step 3 Enter the chassis slot port numbers. These are the reserved port numbers for one chassis slot. There can be up to 64 port numbers reserved for each slot in the chassis.

Step 4 Click **Apply**.

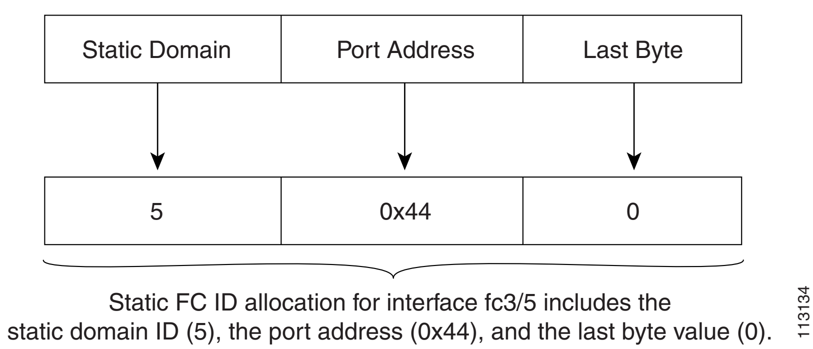
FC ID Allocation

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 "Assigning FC ID Last Byte" section on page 28-20).

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 shut down and restarted to switch from the dynamic to static FC IDs and vice versa (see Figure 28-6).

Figure 28-6 Static FC ID Allocation for FICON



Configuring FICON

By default FICON is disabled in all switches in the Cisco MDS 9000 Family. You can enable FICON on a per VSAN basis by using the Device Manager.

This section includes the following topics:

About Enabling FICON on a VSAN

By default FICON is disabled in all VSANs on the switch.

You can enable FICON on a per VSAN basis in one of the following ways:

- Manually addressing each prerequisite.

  See the "About FICON" section on page 28-1.
- Use Device Manager.

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 "About FICON Configuration Files" section on page 28-29.

Tip Using Device Manager, FICON auto-save can be invoked by multiple users logged on to the same FICON-enabled switch. Device Manager performs a periodic auto-save on any FICON-enabled switch causing increments in the FICON key counter. These increments highlight a change that has actually not occurred. To avoid this we recommend that only one instance of Device Manager monitor a FICON-enabled switch.

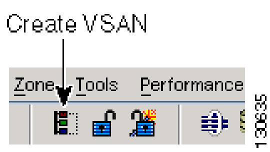
Setting Up a Basic FICON Configuration

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

To create a FICON-enabled VSAN using Fabric Manager, follow these steps:

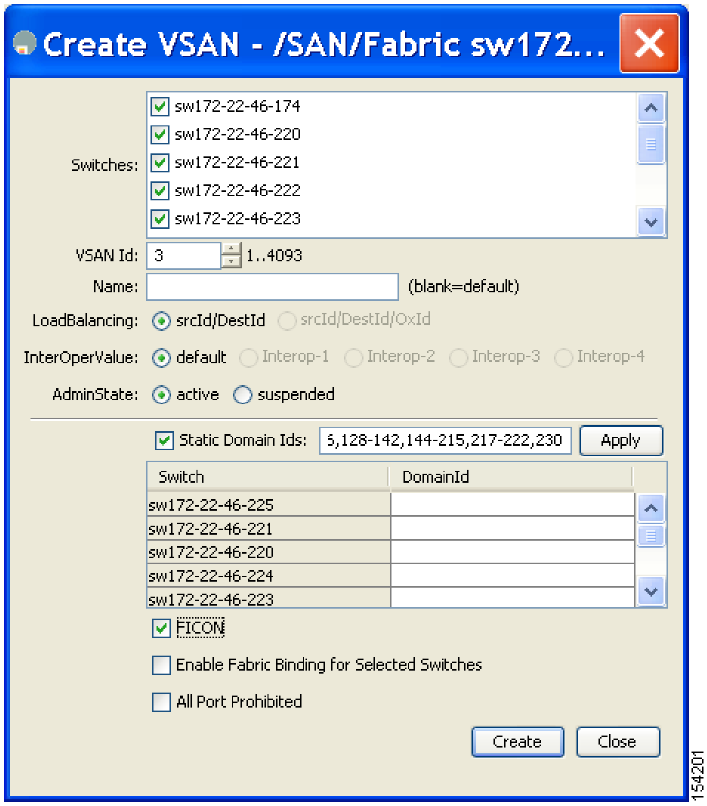
Step 1 Click the **Create VSAN** icon (see Figure 28-7).

Figure 28-7 Create VSAN Icon



You see the Create VSAN dialog box (see Figure 28-8).

Figure 28-8 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 Check the option, if appropriate, to enable fabric binding for the selected switches.

Step 8 Check the All Ports Prohibited option if all ports in this VSAN are prohibited.

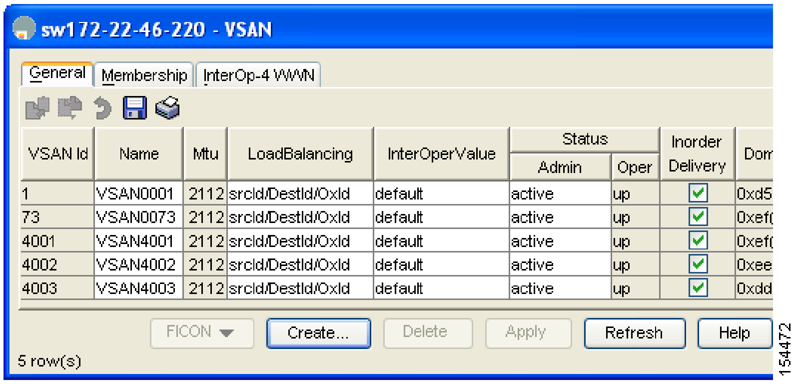
Step 9 Click **Create** to create the VSAN.

Step 10 Choose **Tools** > **Device Manager** to open Device Manager for each switch in the FICON VSAN.

Step 11 Click **FC** > **VSANs**.

You see the VSAN dialog box (see Figure 28-9).

Figure 28-9 VSAN Dialog Box in Device Manager



Step 12 Enter the VSAN membership information.

Step 13 Click the VSAN you want to become a FICON VSAN and select **Add** from the FICON drop-down menu.

Step 14 Click **Apply** to save these changes.

Manually Enabling FICON on a VSAN

Note This section describes the procedure to manually enable FICON on a VSAN. If you have already enabled FICON on therequired VSAN using the automated setup (recommended), skip to the "Automatically Saving the Running Configuration" section on page 28-23.

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

Step 1 Choose **VSAN** > **FICON**.

You see the FICON VSAN configuration information in the Information pane.

Step 2 Select the switch in the VSAN on which you want to enable FICON.

Step 3 Click enable from the Command drop-down menu.

Step 4 Click the **Apply Changes** icon to save these changes.

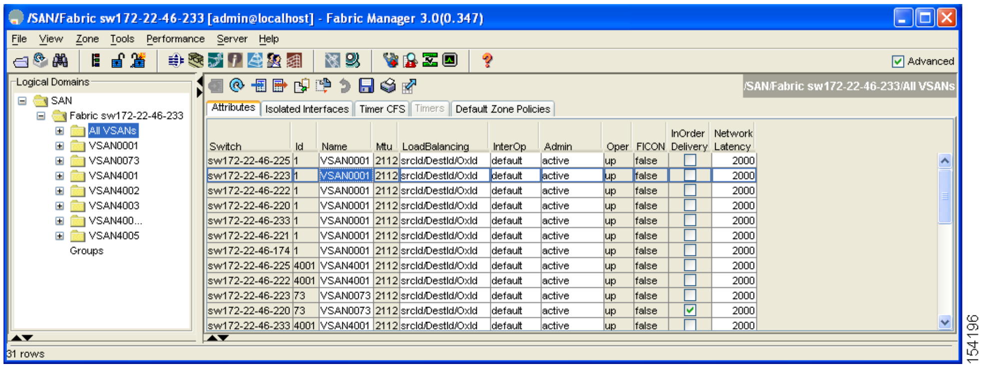
Deleting FICON VSANs

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

Step 1 Select **All VSANS**.

You see the VSAN table in the Information pane (see Figure 28-10).

Figure 28-10 All VSANs Table



Step 2 Click anywhere in the row of the VSAN that you want to delete.

Step 3 Click **Delete Row** to delete the VSAN.

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

Suspending a FICON VSAN

To suspend a FICON VSAN using Fabric Manager, follow these steps:

Step 1 Click **All VSANs**.

You see all the VSANs listed in the Information pane.

Step 2 Select the VSAN that you want to suspend.

Step 3 Set the Admin drop-down menu for a VSAN to **suspended**.

Step 4 Click the **Apply Changes** icon to save these changes.

> **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 28-21).

Configuring 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.

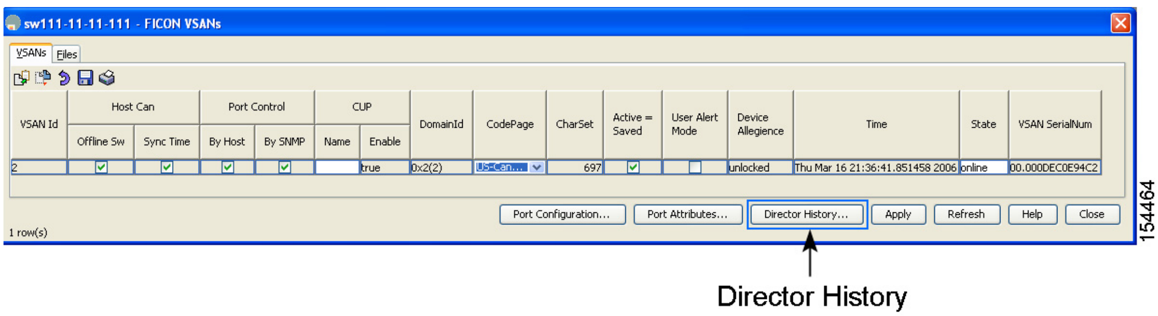
Tip This is an optional configuration. If you are not sure of the EBCDIC format to be used, we recommend retaining the **us-canada** (default) option.

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

Step 1 Choose **FICON** > **VSANs**.

You see the FICON VSAN configuration dialog box (see Figure 28-11). The VSANs tab is the default tab.

Figure 28-11 FICON VSANs Tab in Device Manager



Step 2 Choose an option from the CodePage drop-down menu for the FICON VSAN you want to configure (US-Canada is configured in Figure 28-11).

Step 3 Click **Apply** to save the changes.

Assigning 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.

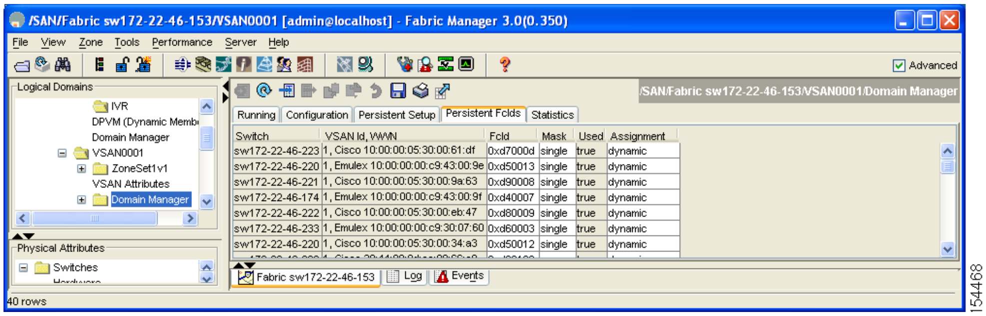
To assign the last byte for the FC ID using Fabric Manager, follow these steps:

Step 1 Choose **All VSANs** > **Domain Manager**.

Step 2 Click the **Persistent FCIDs** tab.

You see the Persistent FcIds tab (see Figure 28-12).

Figure 28-12 Persistent FcIds Tab



Step 3 Select **single** in the Mask column and then assign the entire FC ID at once. The single option allows you to enter the FC ID in the ###### format.

Step 4 Click the **Apply Changes** icon to save these changes.

Allowing the Host to Move the Switch Offline

By default, hosts are allowed to move the switch to an offline state. To do this, the host sends "Set offline" command (x'FD') to CUP (Control Unit Port).

To allow the host (mainframe) to move the switch to an offline state using Fabric Manager, follow these steps:

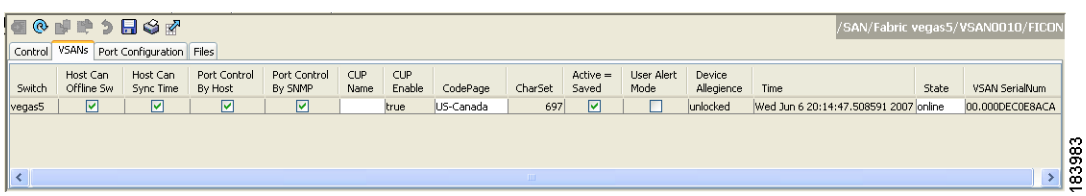
Step 1 Choose **VSAN** > **FICON**.

You see a list of switches under the Control tab in the Information pane.

Step 2 Click the **VSANs** tab.

You see the FICON VSAN configuration information in the Information pane (see Figure 28-13).

Figure 28-13 FICON VSANs in Fabric Manager



Step 3 Check the **Host Can Offline Sw** checkbox to allow the mainframe to move a switch to the offline state.

Step 4 Check the **Host Can Sync Time** checkbox to allow the mainframe to set the system time on the switch.

Step 5 Click the **Apply Changes** icon to save the changes.

Allowing the Host to Change 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 Fabric Manager, follow these steps:

Step 1 Choose **VSAN** > **FICON**.

You see a list of switches under the **Control** tab in the Information pane.

Step 2 Click the **VSANs** tab.

You see the FICON VSAN configuration information in the Information pane (see Figure 28-13).

Step 3 Check the **Port Control By Host** checkbox to allow the mainframe to control a switch.

Step 4 Click the **Apply Changes** icon to save the changes.

Allowing the Host to Control the Timestamp

By default, the clock in each VSAN is the same as the switch hardware clock. Each VSAN in a Cisco MDS 9000 Family 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.

To configure host (mainframe) control for the VSAN time stamp using Fabric Manager, follow these steps:

Step 1 Choose **VSAN** > **FICON**.

You see a list of switches under the Control tab in the Information pane.

Step 2 Click the **VSANs** tab.

You see the FICON VSAN configuration information in the Information pane (see Figure 28-13).

Step 3 Check the **Host Can Sync Time** checkbox to allow the mainframe to set the system time on the switch.

Step 4 Click the **Apply Changes** icon to save these changes.

Configuring SNMP Control of FICON Parameters

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

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

To configure SNMP control of FICON parameters using Fabric Manager, follow these steps:

Step 1 Choose **VSAN > FICON**.

You see a list of switches under the Control tab in the Information pane.

Step 2 Click the **VSANs** tab.

You see the FICON VSAN configuration information in the Information pane (see Figure 28-13).

Step 3 Check the **Port Control By SNMP** checkbox to allow SNMP users to configure FICON on the switch.

Step 4 Click the **Apply Changes** icon to save these changes.

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 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.

About 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 discards the currently executing session.

Automatically Saving the Running Configuration

Cisco MDS SAN-OS provides an option to automatically save any configuration changes to the startup configuration. This ensures that the new configuration is present after a switch reboot. The Active=Saved option can be enable on any FICON VSAN.

Table 28-2 displays the results of the **Active = Saved** option and the implicit copy from the running configuration to the startup configuration (**copy running start**) in various scenarios.

If the Active=Saved option is enabled in any FICON-enabled VSAN in the fabric, then the following apply (see Number 1 and 2 in Table 28-2):

- 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 28-28).

If the Active=Saved option 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 startup** is not issued—you must explicitly save the running configuration to the startup configuration (see number 3 in Table 28-2).

Table 28-2 Saving the Active FICON and Switch Configuration

Number	FICON-enabled VSAN?	`active equals saved` Enabled?	Implicit[1] `copy running start` 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	Yes (even in one FICON VSAN)	Implicit	FICON changes written to IPL file for only the VSAN that has **active equals saved** option enabled. Non-FICON changes saved to startup configuration and persistent storage.
3	Yes	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.

Step 1 Choose **VSAN** > **FICON**.

You see a list of switches under the Control tab in the Information pane.

Step 2 Click the **VSANs** tab.

You see the FICON VSAN configuration information in the Information pane (see Figure 28-13).

Step 3 Check the **Active=Saved** check box to automatically save the running configuration to the startup configuration whenever there is a FICON configuration change.

Step 4 Click the **Apply Changes** icon to save these changes.

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.

This section includes the following topics:

- Configuring Port Blocking, page 28-25

- Viewing ESCON Style Ports, page 28-26
- Port Prohibiting, page 28-26
- Assigning a Port Address Name, page 28-27
- About RLIR, page 28-27
- Displaying RLIR Information, page 28-27

Configuring 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.

Note The **shutdown/no shutdown** port state is independent of the **block/no block** port state.

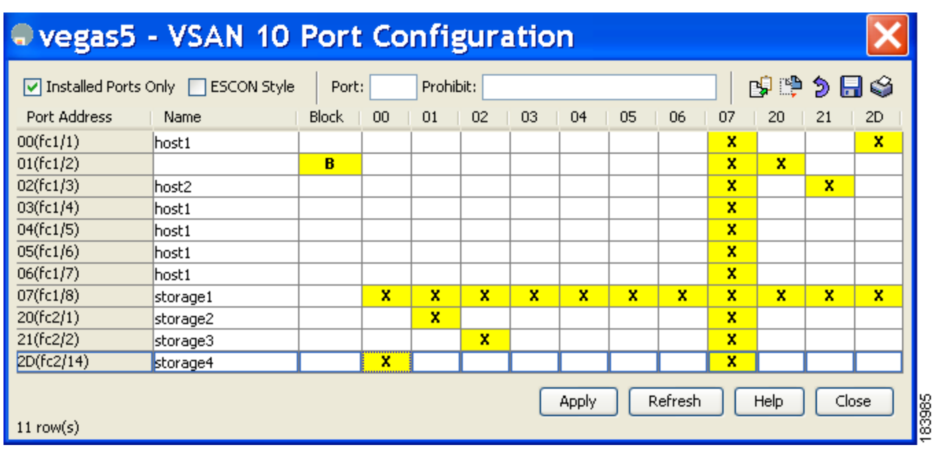
To block or unblock port addresses in a VSAN using Device Manager, follow these steps:

Step 1 Choose **FICON** > **VSANs**.

Step 2 Select a VSAN ID and click **Port Configuration**.

You see the FICON Port Configuration dialog box for the selected VSAN (see Figure 28-14).

Figure 28-14 FICON Port Configuration Dialog Box



Step 3 Check the **Blocked** check box for the port that you want to block.

Step 4 Click **Apply** to save the changes.

Viewing ESCON Style Ports

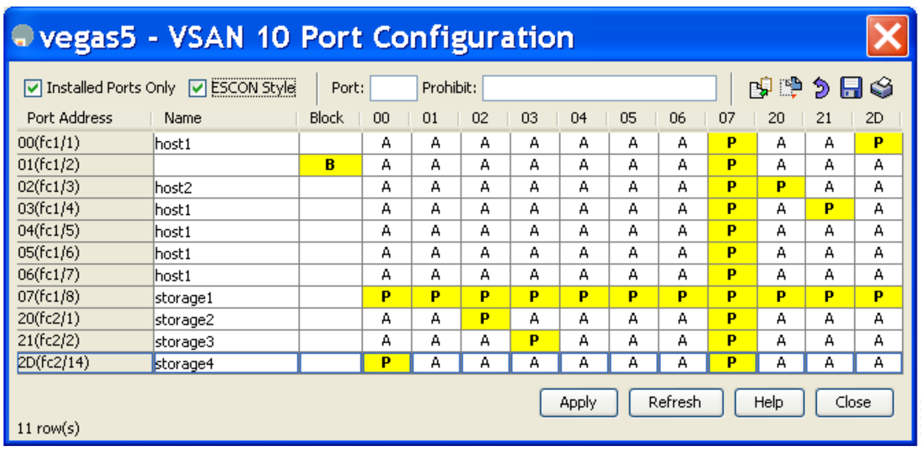
To view the available and prohibited ESCON style ports using Device Manager, follow these steps:

Step 1 Check the ESCON Style check box to see the available and prohibited ESCON style ports.

In Figure 28-15, A stands for available and P stands for prohibited.

When the port address is highlighted red, it represents the E/TE port or multiple interfaces.

Figure 28-15 ESCON Style



Port Address	Name	Block	00	01	02	03	04	05	06	07	20	21	2D
00(fc1/1)	host1		A	A	A	A	A	A	A	P	A	A	P
01(fc1/2)		B	A	A	A	A	A	A	A	P	A	A	A
02(fc1/3)	host2		A	A	A	A	A	A	A	P	P	A	A
03(fc1/4)	host1		A	A	A	A	A	A	A	P	A	P	A
04(fc1/5)	host1		A	A	A	A	A	A	A	P	A	A	A
05(fc1/6)	host1		A	A	A	A	A	A	A	P	A	A	A
06(fc1/7)	host1		A	A	A	A	A	A	A	P	A	A	A
07(fc1/8)	storage1		P	P	P	P	P	P	P	P	P	P	P
20(fc2/1)	storage2		A	A	P	A	A	A	A	P	A	A	A
21(fc2/2)	storage3		A	A	A	P	A	A	A	P	A	A	A
2D(fc2/14)	storage4		P	A	A	A	A	A	A	P	A	A	A

183982

Step 2 Click **Apply** to save the changes.

Port Prohibiting

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

Tip You cannot prohibit a PortChannel or FCIP interface.

Unimplemented ports are always prohibited. In addition, 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 or in TE mode.

Configuring Port Prohibiting

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

Step 1 Choose **FICON** > **VSANs**.

Step 2 Select a VASAN ID and click **Port Configuration**.

You see the FICON Port Configuration dialog box (see Figure 28-14).

Step 3 Set the port prohibit configuration for the selected FICON VSANs.

Step 4 Click **Apply** to save these changes.

Assigning a Port Address Name

Note To view the latest FICON information, you must click the **Refresh** button. See the "Automatically Saving the Running Configuration" section on page 28-23.

To assign a port address name in Device Manager, follow these steps:

Step 1 Choose **FICON** > **VSANs**.

Step 2 Select a VSAN ID and click **Port Configuration**.

You see the FICON Port Configuration dialog box (see Figure 28-14).

Step 3 Enter the Port Configuration information.

Step 4 Click **Apply** to save the configuration information.

About RLIR

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

When an LIR is detected in FICON-enabled switches in the Cisco MDS 9000 Family from a RLIR Extended Link Service (ELS), the switch 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 it to the members of the ERL.

The Nx ports interested in receiving the RLIR ELS send the 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 data is written to persistent storage when you **copy** the running configuration to the startup configuration.

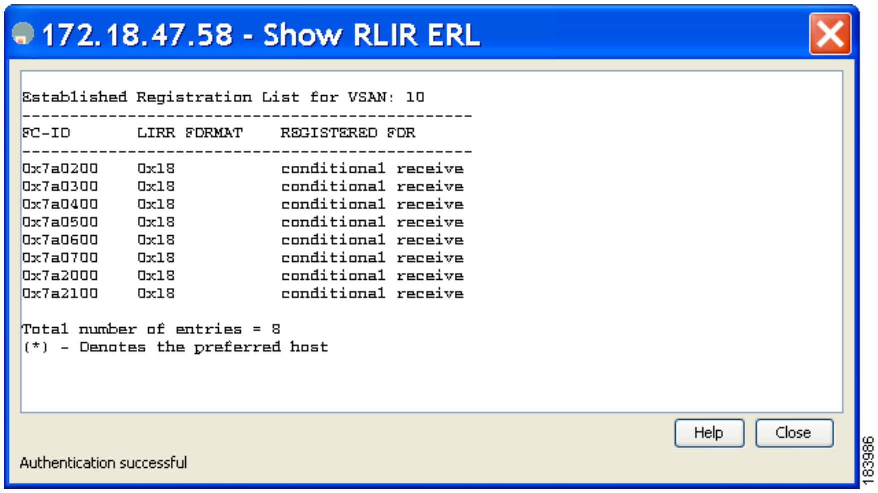
Displaying RLIR Information

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

Step 1 Choose **FICON > RLIR ERL**.

You see the Show RLIR ERL dialog box (see Figure 28-16).

Figure 28-16 Show RLIR ELR Dialog Box



Step 2 Click **Close** to close the 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 on 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, static domain ID configuration, and fabric binding configuration.

See the Chapter 12, "Initial Configuration," for details on the normal configuration files used by Cisco MDS switches.

This section includes the following topics:

About 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 Saved Configuration Files to the Running Configuration

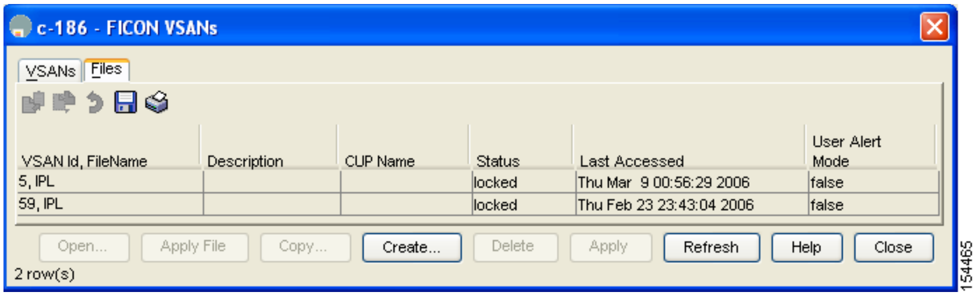
To apply the saved configuration files to the running configuration using Device Manager, follow these steps:

Step 1 Choose **FICON** > **VSANs**.

Step 2 Click the **Files** tab.

You see the FICON Files dialog box (see Figure 28-17).

Figure 28-17 FICON VSANs Dialog Box



Step 3 Highlight the file you want to apply and click **Apply File** to apply the configuration to the running 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.

Note To view the latest FICON information, you must click the **Refresh** button. See the "Automatically Saving the Running Configuration" section on page 28-23.

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

Step 1 Choose **FICON > VSANs**.

Step 2 Click the **Files** tab.

You see the FICON VSANs dialog box (see Figure 28-17).

Step 3 Select a VSAN ID and then click **Open** to edit the FICON configuration file.

Step 4 Select a VSAN ID and then click **Delete** to delete the FICON configuration file.

Step 5 Click **Apply** to apply the changed FICON configuration file.

Displaying FICON Configuration Files

To open and view configuration files in Fabric Manager, follow these steps:

Step 1 Choose **FICON > VSAN**.

You see the FICON configuration table in the Information pane.

Step 2 Click the **Files** tab.

Step 3 Select the file you want to open.

Step 4 Click **Open**.

Copying FICON Configuration Files

To copy an existing FICON configuration file using Device Manager, follow these steps:

Step 1 Choose **FICON** > **VSANs**.

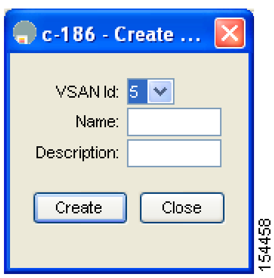
Step 2 Click the **Files** tab.

You see the FICON VSANs dialog box (see Figure 28-17).

Step 3 Click **Create** to create a FICON configuration file.

You see the Create FICON VSANs Files dialog box shown in Figure 28-18.

Figure 28-18 Create FICON VSANs Files Dialog Box in Device Manager



a. Select a VSAN ID for the FICON VSAN you want to configure.

b. Enter the file name and the description.

c. Click **Create** to create the file.

Step 4 Click **Copy** to copy the file to a new file.

Step 5 Click Apply to apply the FICON configuration file.

Port Swapping

The FICON port swapping 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 nonexistent 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.

- If you swap a port in a module that has unlimited oversubscription ratios enabled with a port in a module that has limited oversubscription ratios, then you may experience a degradation in bandwidth.

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.

Note To view the latest FICON information, you must click the **Refresh** button. See the "Automatically Saving the Running Configuration" section on page 28-23.

This section includes the following topics:

About Port Swapping

Be sure to follow these guidelines when using the FICON port swapping 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.
- Before performing a port swap, the Cisco SAN-OS software performs a compatibility check to verify the extended BB_credits configuration.
- If ports have default values (for some incompatible parameters), then a port swap operation is allowed and the ports retain their default values.
- Port tracking information is not included in port swapping. This information must be configured separately (see Chapter 57, "Configuring Port Tracking").

Note The 32-port module guidelines also apply for port swapping configurations .

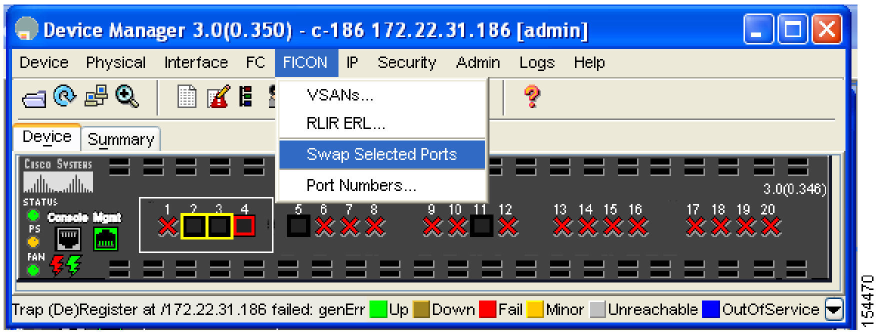
Swapping Ports

To swap ports using Device Manager, follow these steps:

Step 1 Select two Fibre Channel ports by holding down the **CTRL** key and clicking them.

Step 2 Choose **FICON** > **Swap Selected Ports** (see Figure 28-19).

Figure 28-19 FICON Swap Selected Ports



FICON Tape Acceleration

The sequential nature of tape devices causes each I/O operation to the tape device over an FCIP link to incur the latency of the FCIP link. Throughput drastically decreases as the round-trip time through the FCIP link increases, leading to longer backup windows. Also, after each I/O operation, the tape device is idle until the next I/O arrives. Starting and stopping of the tape head reduces the lifespan of the tape, except when I/O operations are directed to a virtual tape.

Cisco MDS SAN-OS software provides acceleration for the following FICON tape write operations:

- The link between mainframe and native tape drives (both IBM and Sun/STK)
- The back-end link between the VSM (Virtual Storage Management) and tape drive (Sun/STK)

FICON tape acceleration over FCIP provides the following advantages:

- Efficiently utilizes the tape device by decreasing idle time
- More sustained throughput as latency increases
- Similar to FCP tape acceleration, and does not conflict with it

Note FICON tape read acceleration over FCIP is not supported.

Figure 28-20 through Figure 28-23 show supported configurations:

Figure 28-20 Host Directly Accessing IBM/STK (StorageTek) Library

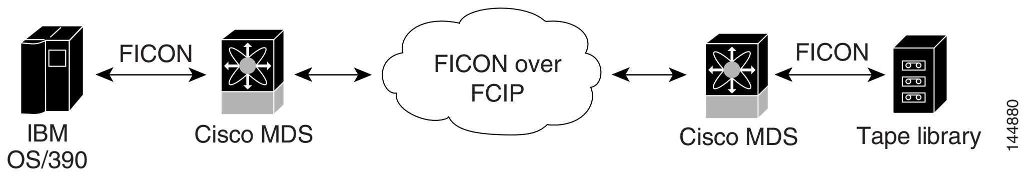


Figure 28-21 Host Accessing Standalone IBM-VTS (Virtual Tape Server) /STK-VSM (Virtual Shared Memory)

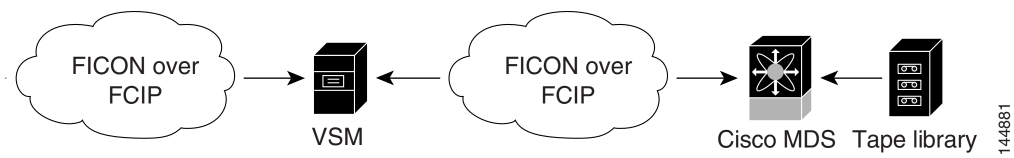


Figure 28-22 Host Accessing Peer-to-Peer VTS (Virtual Tape Server)

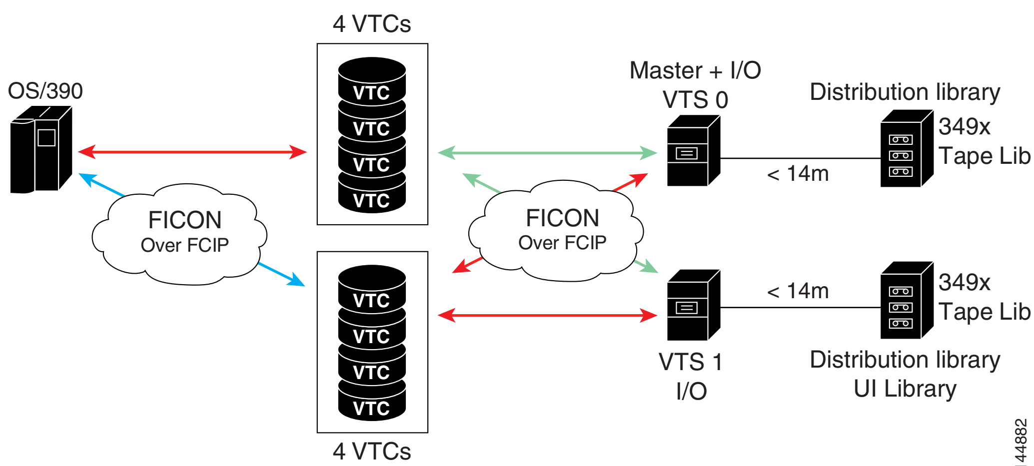
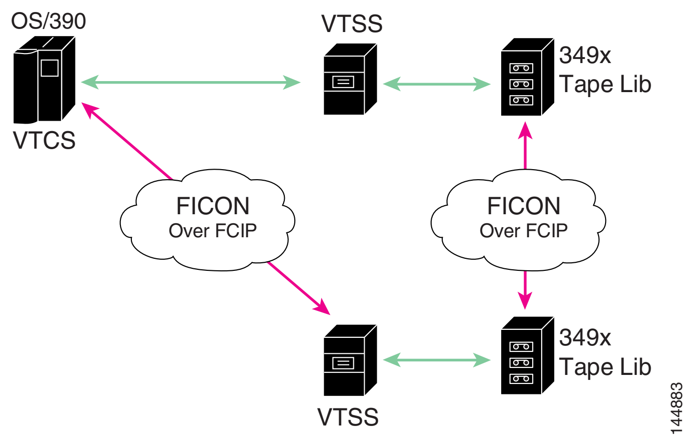


Figure 28-23 Host Accessing Peer-to-Peer VTS (Virtual Tape Server)



Note For information about FCIP tape acceleration, see "FCIP Tape Acceleration" section on page 48-32.

Configuring FICON Tape Acceleration

FICON tape acceleration has the following configuration considerations:

- In addition to the normal FICON configuration, FICON tape acceleration must be enabled on both ends of the FCIP interface. If only one end has FICON tape acceleration enabled, acceleration does not occur.
- FICON tape acceleration is enabled on a per VSAN basis.
- FICON tape acceleration cannot function if multiple ISLs are present in the same VSAN (PortChannels or FSPF load balanced).
- You can enable both Fibre Channel write acceleration and FICON tape acceleration on the same FCIP interface.
- Enabling or disabling FICON tape acceleration disrupts traffic on the FCIP interface.

To configure FICON tape acceleration over FCIP in Fabric Manager, follow these steps:

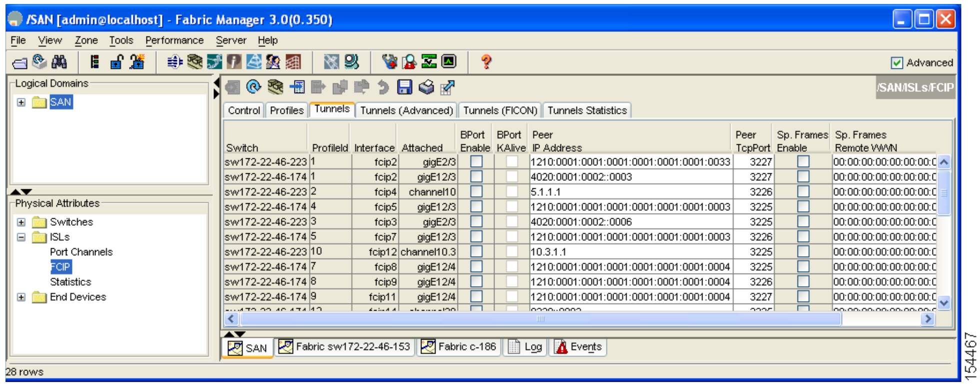
Step 1 Expand **ISL** and then select **FCIP** in the Physical Attributes pane.

Step 2 Click the **Tunnels** tab in the Information pane.

You see a list of available switches (Figure 28-24).

Send documentation comments to mdsfeedback-doc@cisco.com

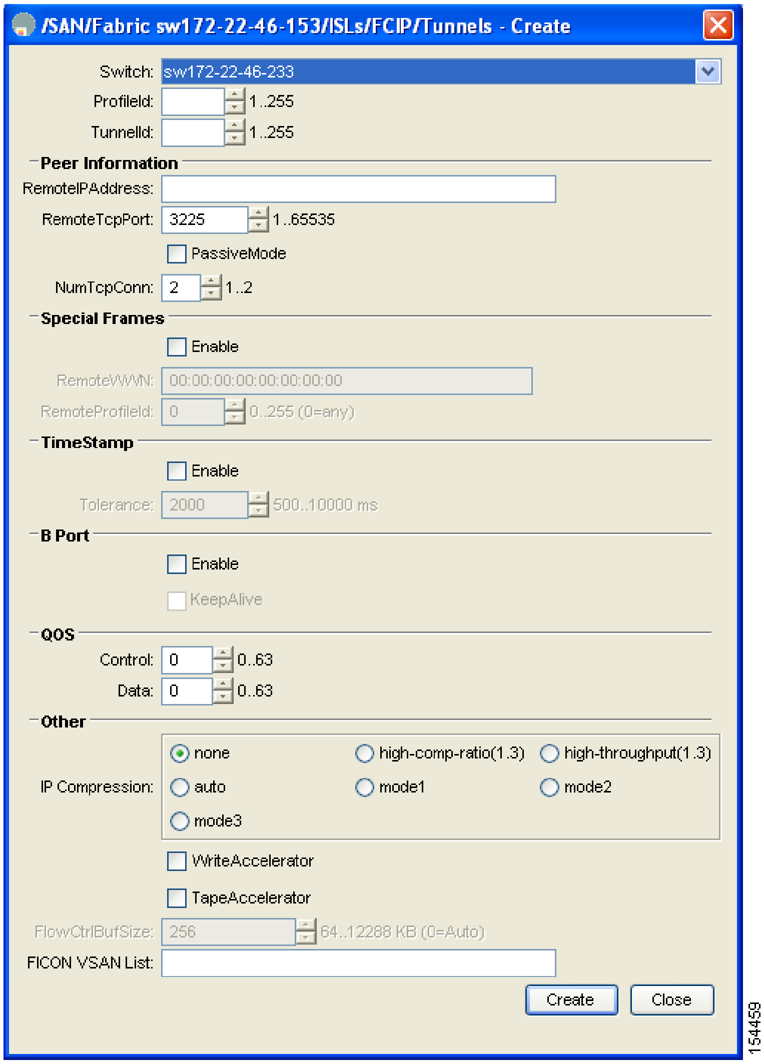
Figure 28-24 FCIP Tunnels Tab in Fabric Manager



Step 3 Click the **Create Row** icon to create an FCIP tunnel.

You see the Create FCIP Tunnel dialog box shown in Figure 28-25.

Figure 28-25 Create FCIP Tunnel Dialog Box



Step 4 Configure the tunnel with the options shown in Figure 28-25.

Step 5 Check the **TapeAccelerator** check box to enable FICON tape acceleration over this FCIP tunnel.

Step 6 Click **Create**.

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.

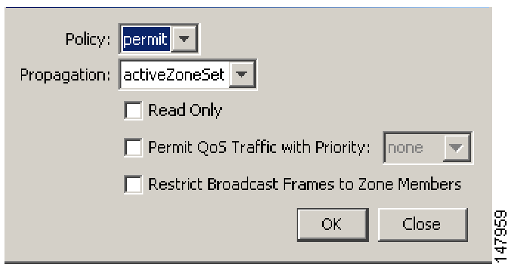
Note The CUP specification is proprietary to IBM.

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.

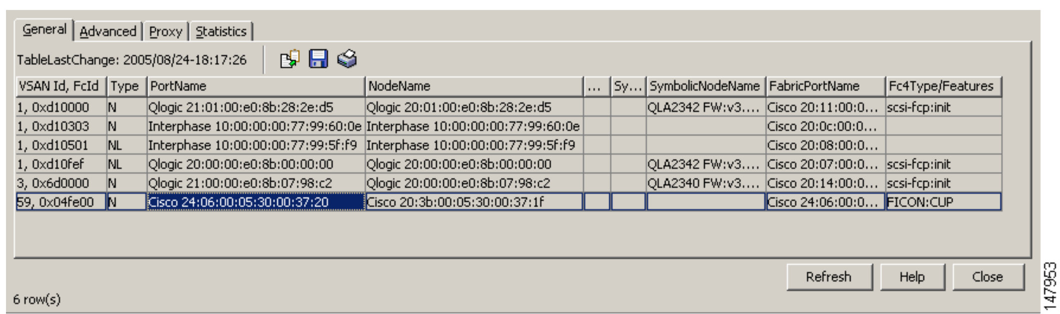
Step 1 In Fabric Manager, choose **Zone > Edit Full Zoneset,** and then choose **Edit > Edit Default Zone Attributes** to set the default zone to permit for the required VSAN. (See Figure 28-26.)

Figure 28-26 Setting the Default Zone Policy



Step 2 In Device Manager, choose **FC > Name Server...** for the required VSAN and obtain the FICON:CUP WWN. See Figure 28-27.

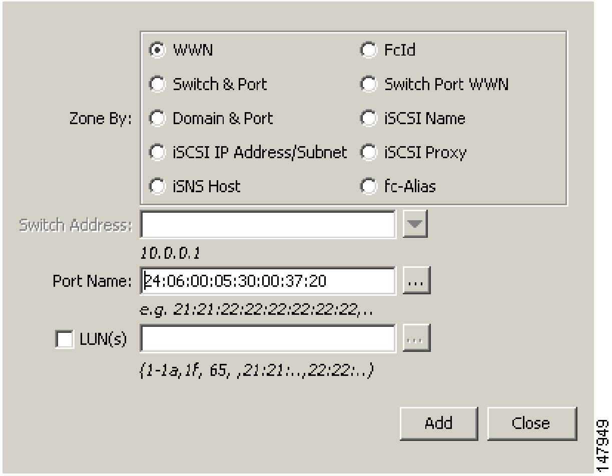
Figure 28-27 Finding pWWN for FICON:CUP



> **Note** If more than one `FICON:CUP WWN` exists in this fabric, be sure to add all the `FICON:CUP` pWWNs to the required zone.

Step 3 In Fabric Manager, choose **Zone > Edit Full Zoneset** and add the FICON:CUP pWWN to the zone database. (See Figure 28-28.)

Figure 28-28 Adding FICON:CUP WWN to Zone



Calculating FICON Flow Load Balance

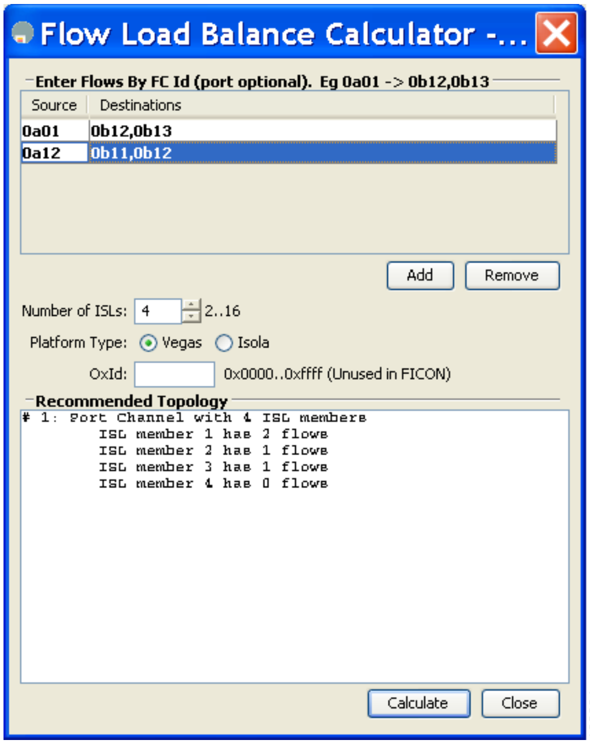
The FICON Flow Load Balance Calculator allows you to get the best load balancing configuration for your FICON flows. The calculator does not rely on any switch or flow discovery in the fabric. It is available from the Fabric Manager Tools menu.

To use the FICON Flow Load Balance Calculator from Fabric Manager follow these steps:

Step 1 Choose **Tools > Other > Flow Load Balance Calculator**.

You see the Flow Load Balance Calculator (see Figure 28-29).

Figure 28-29 Flow Load Balance Calculator



Step 2 Click **Add** to enter the source and destination(s) flows.

Step 3 Enter source and destination using 2 byte hex (by domain and area IDs).You can copy and paste these IDs, and then edit them if required.

Step 4 Enter (or select) the number of ISLs between the two switches (for example, between domain ID 0a and 0b).

Step 5 Select a row to remove it and click **Remove**.

Step 6 Select the module for which you are calculating the load balance.

Step 7 Click **Calculate** to show the recommended topology.

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

Displaying FICON Information

This section includes the following topics:

- Receiving FICON Alerts, page 28-41
- Displaying FICON Port Address Information, page 28-41
- Displaying IPL File Information, page 28-41
- Viewing the History Buffer, page 28-41

Receiving FICON Alerts

To receive an alert to indicate any changes in the FICON configuration using Device Manager, follow these steps:

Step 1 Choose **FICON** > **VSANs**.

You see the FICON VSANs dialog box.

Step 2 Check the **User Alert Mode** check box to receive an alert when the FICON configuration changes.

Step 3 Click **Apply** to apply this change.

Displaying FICON Port Address Information

To display FICON port address information using Device Manager, follow these steps:

Step 1 Choose **FICON** > **VSANs**.

You see the FICON VSANs dialog box.

Step 2 Select a VSAN ID and click **Port Configuration**.

You see the FICON Port Configuration dialog box.

Step 3 Click **Close** to close the dialog box.

Displaying IPL File Information

To display the IPL file information using Device Manager, follow these steps:

Step 1 Select **VSANs** from the FICON menu.

Step 2 Click the **Files** tab.

You see the FICON VSANs dialog box.

Step 3 Select the file that you want to view and click **Open**.

Viewing the History Buffer

In the directory history buffer, 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.

To view the directory history buffer using Device Manager, follow these steps:

Step 1 Choose **FICON > VSANs**.

You see the FICON VSANs dialog box.

Step 2 Click the Director History button.

You see the history buffer dialog box.

Step 3 Click **Close** to close the dialog box.

Default Settings

Table 28-3 lists the default settings for FICON features.

Table 28-3 Default FICON Settings

Parameters	Default
FICON feature	Disabled.
Port numbers	Same as port addresses.
FC ID last byte value	0 (zero).
EBCDIC format option	US-Canada.
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.
Prohibited ports	Ports 90–253 and 255 for the Cisco MDS 9200 Series switches. Ports 250–253 and 255 for the Cisco MDS 9500 Series switches.