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

Contents

FICON Overview

The Cisco MDS 9000 Family supports the Fibre Channel, FICON, iSCSI, and FCIP capabilities within a single, high-availability platform. Fibre Channel 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. The Cisco SAN-OS FICON feature supports high-availability, scalability, and SAN extension technologies including VSANs, IVR, FCIP, and PortChannels.

Note: When you create 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.

You can implement FICON on 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

Note: The FICON feature is not supported on Cisco MDS 9120, 9124 or 9140 switches, the 32-port Fibre Channel switching module, Cisco Fabric Switch for HP c-Class BladeSystem or Cisco Fabric Switch for IBM BladeCenter.

Refer to the Cisco MDS 9000 Family configuration guides for details about configuring FICON at one of the following websites:

- *Cisco MDS 9000 Family Fabric Manager Configuration Guide, Release 3.x* at http://www.cisco.com/en/US/products/ps5989/products_configuration_guide_chapter09186a0080662d7a.html
- *Cisco MDS 9000 Family CLI Configuration Guide, Release 3.x* at http://www.cisco.com/en/US/products/ps5989/products_configuration_guide_chapter09186a0080664d07.html

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

The following guidelines apply to FICON port numbers:

- Supervisor modules do not have port number assignments.
- Chassis-wide unique port numbers should be reserved for trunking expansion (TE) ports since TE ports appear in multiple VSANs.
- Each PortChannel must be explicitly associated with a FICON port number.
- For individual ports in a PortChannel, the configuration of the port corresponding to the PortChannel is applied and not that of the individual 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 online.

Note: When you assign, change, or release a port number, the port goes offline and then back online as a result of the change.

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).

Table 16-1 lists the default port number assignments for the Cisco MDS 9000 Family of switches and directors

Table 16-1 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

The first 4, 12, 16, or 24 port numbers are used in 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.

Cisco MDS 9222i Series

Slot 1

0 through 31

64 through 89

90 through 253 and port 255

Slot 2

32 through 63

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

Supervisor modules are not allocated port numbers.

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 are used in 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 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

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 model, 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

112through 127

Slot 11

128 through 143

Slot 12

144 through 159

Slot 13

160 through 175

Note: You can use the **ficon slot assign port**-*numbers* CLI command to use any excess ports by assigning numbers to the slots. Before you assign numbers to the slots however, we recommend that you review the default port number assignments for Cisco MDS 9000 switches shown in Table 16-1.

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

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 16-1 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 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** CLI command.

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

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 modify these FICON configuration files. 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 immediately after FICON is enabled in a VSAN.

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.

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

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

- Block
- Prohibit mask
- Port address name

Note: You cannot prohibit a PortChannel or an FCIP interface.

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.

Note: You can not directly assign a FICON port number to an interface. You assign a range of port numbers to the module.

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.

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

Fabric Binding

The fabric binding feature ensures that ISLs are enabled only between specified switches in the fabric binding configuration. Fabric binding is configured on a per-VSAN basis.

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

To enforce fabric binding, configure the switch world wide name (sWWN) to specify the xE port connection for each switch. Fabric binding policies are enforced on every activation and also when the port tries to come up. In a FICON VSAN, the fabric binding feature requires that all sWWNs are connected to a switch and that their persistent domain IDs are part of the fabric binding active database. In a Fibre Channel VSAN, only the sWWN is required; the domain ID is optional.

Use the **show wwn switch** CLI command to determine the sWWN to use for fabric binding.

The fabric binding feature must be enabled in each switch in the fabric that participates in the fabric binding.

FICON Configuration Requirements

Use the following best practices for implementing FICON for Cisco SAN-OS products:

- Use static domain IDs for all switches in the FICON fabric.
- Do not enable persistent FC IDs for the FICON-enabled VSAN.
- Enable in-order delivery for the FICON-enabled VSAN.
- Enable fabric binding for all FICON switches in the fabric.
- Use the source ID (SID)-destination ID (DID) load balancing scheme for the FICON-enabled VSAN.
- Set the VSAN interop value to default.
- Limit cascaded FICON switches to two switches between the host and storage.
- Use the CLI FICON setup script or the Fabric Manager VSAN Wizard to configure FICON.
- You cannot enable IVR NAT in a FICON VSAN.
- FICON VSANs can only be in the default interop mode.

Initial Troubleshooting Checklist

Begin troubleshooting FICON issues by checking the following issues:

Checklist	Check off
Verify licensing requirements. See *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.	
Verify that you enabled in-order delivery for the FICON-enabled VSAN.	
Verify that you have enabled fabric binding in all switches in the FICON fabric.	
Verify that all switches in the FICON fabric are in the fabric binding database.	
Verify that you have assigned static domain IDs for all switches in the FICON fabric.	
Verify that you have not enabled persistent FC IDs for the FICON-enabled VSAN.	
Verify that the load balancing scheme is SID- DID.	
Verify that the default zone is set to permit if you are not using the zoning feature.	
Verify that the CUP (area FE) is in the correct zone if you are using zoning.	
Verify that conflicting persistent FC IDs do not exist in the switch.	
Verify that the configured domain ID and requested domain ID match.	

Common Troubleshooting Tools in Fabric Manager or Device Manager

Use the following procedures to troubleshoot FICON issues:

- Choose **Fabricxx > VSANyy > FICON** in Fabric Manager to view the FICON configuration.
- Choose **Fabricxx > VSANyy > Fabric Binding** in Fabric Manager to view the fabric binding configuration.
- Choose **FICON > VSANs** in Device Manager, and then highlight the FICON VSAN and click **Director History** to get a history of changes on this FICON VSAN.
- Choose **Tools > Other > Flow Load Balance Calculator** in Fabric Manager to determine the proper ISL configuration for FICON load balancing.
- Choose **Device > Preferences >Label Physical Ports View With** on Device Manager, check **FICON**, and click **Apply** to set the Device Manager display to use FICON port numbers.

Common Troubleshooting Commands in the CLI

Use the following CLI commands to troubleshoot FICON issues:

- **show ficon**
- **show ficon vsan** *vsan-id* **file ficon-file-name**
- **show ficon vsan** *vsan-id* **portaddress**
- **show ficon vsan** *vsan-id* **director-history**
- **show fabric-binding status**
- **show fabric-binding database**
- **show fabric-binding violations**
- **show in-order-guarantee**

Port Swapping

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

Follow these guidelines when using the FICON port swapping feature:

- Port swapping is not supported for logical ports (PortChannels, FCIP links).
- Port swapping is not supported between physical ports that are part of a PortChannel.
- If the two ports involved in a port swap have incompatible configuration options, 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.

Swapping Ports

To swap ports, except the port numbers, using the CLI, follow these steps:

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

> **Note**: The **ficon swap portnumber** command might fail if more than one interface on the MDS switch has the same port number as the *old-port-number* or *new-port-number* specified in the command.

The specified ports are operationally shut down.

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

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

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

To swap physical Fibre Channel ports, including the port numbers, using the CLI, follow these steps:

1. Enter the **ficon swap interface** *old-interface new-interface* command in EXEC mode.

The specified interfaces are operationally shut down.

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

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

> 📝**Note**: If you specify the **ficon swap interface** *old-interface new-interface* **after swap noshut** command, the ports are automatically initialized.

FICON Issues

This section describes common FICON issues.

Cannot Enable FICON

Symptom Cannot enable FICON.
Table 16-2 Cannot Enable FICON

Symptom

Possible Cause

Solution

Cannot enable FICON.

No MAINFRAME_PKG license is installed, and the grace period has ended.

Install the MAINFRAME_PKG license to use FICON features. Refer to the Licensing information at one of the following URLs:

•For Fabric Manager:
http://www.cisco.com/en/US/products/ps5989/products_configuration_guide_chapter09186a0080662c89.html

•For CLI:
http://www.cisco.com/en/US/products/ps5989/products_configuration_guide_chapter09186a0080664c67.html

Switch ISL Isolated

Symptom Switch ISL is isolated
Table 16-3 Switch ISL Isolated

Symptom

Possible Cause

Solution

Switch ISL is isolated.

Switch WWN is not configured in the fabric binding database.

Add the sWWN to the fabric binding database for all switches in the FICON fabric. Choose **Fabricxx > VSANyy > Fabric Binding** in Fabric Manager, click the **Config Database** tab, and click **Create Row**.

Alternatively, use the **fabric-binding database vsan** CLI command to add a switch to the fabric binding database.

Fabric Manager or Device Manager Cannot Configure FICON

Symptom Fabric Manager or Device Manager cannot configure FICON.
Table 16-4 Fabric Manager or Device Manager Cannot Configure FICON

Symptom

Possible Cause

Solution

Fabric Manager or Device Manager cannot configure FICON.

Switch is configured to disallow SNMP control over FICON.

Use the snmp port control CLI command in FICON submode to enable SNMP control for FICON.

Mainframe Cannot Configure FICON

Symptom Mainframe cannot configure FICON.
Table 16-5 Mainframe Cannot Control FICON

Symptom

Possible Cause

Solution

Mainframe cannot configure FICON.

Switch is configured to disallow Host control over FICON.

Enable host control for FICON. Choose **Fabricxx > VSANyy > FICON** in Fabric Manager, click the **VSANs** tab, and check the appropriate host control check boxes. Click **Apply Changes**.

Alternatively, use the **host port control**, **host set-timestamp**, and **host control switch** CLI commands to configure host control for FICON.

CUP is not in the correct zone.

Add the CUP to the same zone as the FICON VSAN in the switch. Choose **Zone > Edit Local Full Zone Database** in Fabric Manager, or use the **member** CLI command in zone submode to add the CUP to the appropriate zone.

Cannot Enable FICON Port

Symptom Cannot enable FICON port.
Table 16-6 Cannot Enable FICON Port

Symptom

Possible Cause

Solution

Cannot enable FICON port.

Port is blocked.

Unblock the port. Choose **FICON > VSANs** in Device Manager, highlight the **VSAN**, and click **Port Configuration**. Then unset the **Block** column, and click **Apply**.

Alternatively, use the **portaddress** CLI command in FICON submode and use the **no block** command.

TE or E port is prohibited.

Change the TE or E port to disable prohibit. Choose **FICON > VSANs** in Device Manager, highlight the **VSAN** and click **Port Configuration**. Then uncheck the port number column and click **Apply**.

Alternatively, use the **portaddress** CLI command in FICON submode and use the **no prohibit** command.

Another port in the same VSAN has the same port number as this port.

Change the port number to resolve the conflict.

Choose **FICON > Port Numbers** in Device Manager. Alternatively, use the **ficon slot** *slot number* **assign** *port-numbers* CLI command to change the port number.

Cannot Configure FCIP or PortChannel for FICON

Symptom Cannot configure FCIP or PortChannel for FICON.
Table 16-7 Cannot Configure FCIP or PortChannel for FICON

Symptom

Possible Cause

Solution

Cannot configure FCIP or PortChannel for FICON.

FICON port numbers are not reserved for logical ports.

Reserve a block of FICON port numbers for logical ports.

Use the **show ficon first-available** *port-number* CLI command to determine which logical ports are available for use with FCIP and or PortChannels.

Choose **FICON > Port Numbers** in Device Manager. Alternatively, use the **ficon logical-port assign** *port-numbers* CLI command.

FCIP fails for FICON

Symptom FCIP fails for FICON.
Table 16-8 FCIP Fails for FICON

Symptom

Possible Cause

Solution

FCIP fails for FICON.

FICON port address is not assigned to the FCIP tunnel.

Assign the FICON port address to FCIP tunnel and restart FCIP tunnel. Use the **show ficon port-numbers interface** CLI command to determine if there is a FICON port number assigned to the logical port. Use the **ficon portnumber** CLI command in FCIP or PortChannel submode.

FICON Tape Acceleration Not Working

Symptom FICON tape acceleration not working.
Table 16-9 FICON Tape Acceleration Not Working

Symptom

Possible Cause

Solution

FICON tape acceleration not working.

FICON tape acceleration is not enabled on both ends of an FCIP link.

Enable FICON tape acceleration on both ends of the FCIP link. Choose **Switches > ISLs > FCIP** in Fabric Manager, then select the **Tunnels (Advanced)** tab and check **Write Accelerator**.You can also use the **ficon-tape-accelerator vsan** CLI command on each FCIP interface.

Back to Main Page: Cisco MDS SAN-OS Troubleshooting Guide