Redpaper

Jon Tate

Cisco FICON Basic Implementation

In this IBM® Redpaper we discuss the basic steps to configuring a switch for FICON® in both switched point-to-point and cascaded configurations. We use Fabric Manager (FM) and Device Manager (DM) to perform all configuration steps.

Important: Although this paper shows the screen capture flow from a Fabric Manager/Device Manager 3.0(3) installation, the flow equally applies to the latest release of FM/DM 3.2.(1).

We discuss some basic FICON/mainframe steps that you will need to perform. It is not our intent to show any of the steps on the mainframe, but we highlight the considerations.

Hardware configuration definition

An I/O configuration defines the hardware resources that are available to the operating system and the connections between these resources, which include:

- Channels
- ESCON/FICON Directors (switches)
- Control units
- Devices

You must define an I/O configuration to the operating system (software) and the channel subsystem (hardware). The Hardware Configuration Definition (HCD) element of z/OS® combines hardware and software I/O configuration under a single interactive user interface. HCD also performs validation checking, which helps to eliminate errors before you attempt to use the I/O configuration.

The output of HCD is an I/O definition file (IODF). An IODF is used to define multiple hardware and software configurations to the z/OS operating system. When you activate an IODF, HCD defines the I/O configuration to the channel subsystem, the operating system, or both. With the HCD activate function or the MVS™ ACTIVATE operator command, you can make changes to the current configuration without having to perform an initial program load (IPL) on the software or power-on reset (POR) of the hardware. Making changes while the system is running is known as *dynamic configuration* or *dynamic reconfiguration*.

You select your I/O configuration when you:

- POR
- IPL
- Activate a dynamic configuration change

IPL and activation require that you identify the IODF that contains the definition of your configuration. A data set called an I/O configuration data set (IOCDS) is used at POR. An IOCDS can be created from a configuration definition in an IODF. The IOCDS contains the configuration for a specific processor, and the IODF contains configuration data for multiple processors.

Important: We recommend that you complete the FICON configuration on the switches before attempting to bring any CHPIDs or Control Units online. Switch configuration cannot be finished until HCD configuration is complete.

Figure 1 shows an example topology and associated statements.

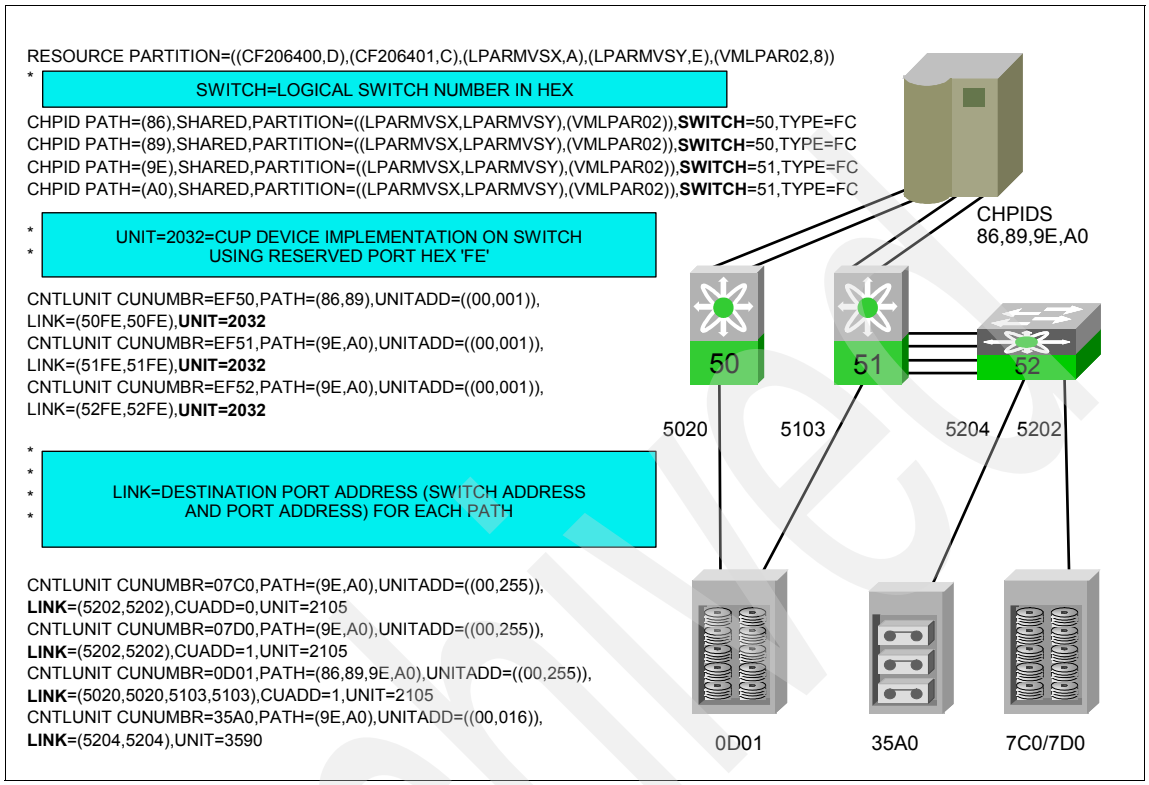


Figure 1 FICON environment IOCP definitions

Note: There is no change to the IODEVICE or ID statements to support SAN.

You must be familiar with the HCD definition process before attempting to code any of the statements shown in Figure 1, so we do not cover this process here.

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 each switch. We show how to accomplish this in later sections.

FICON port numbering on the MDS switches

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, as shown in Figure 2.

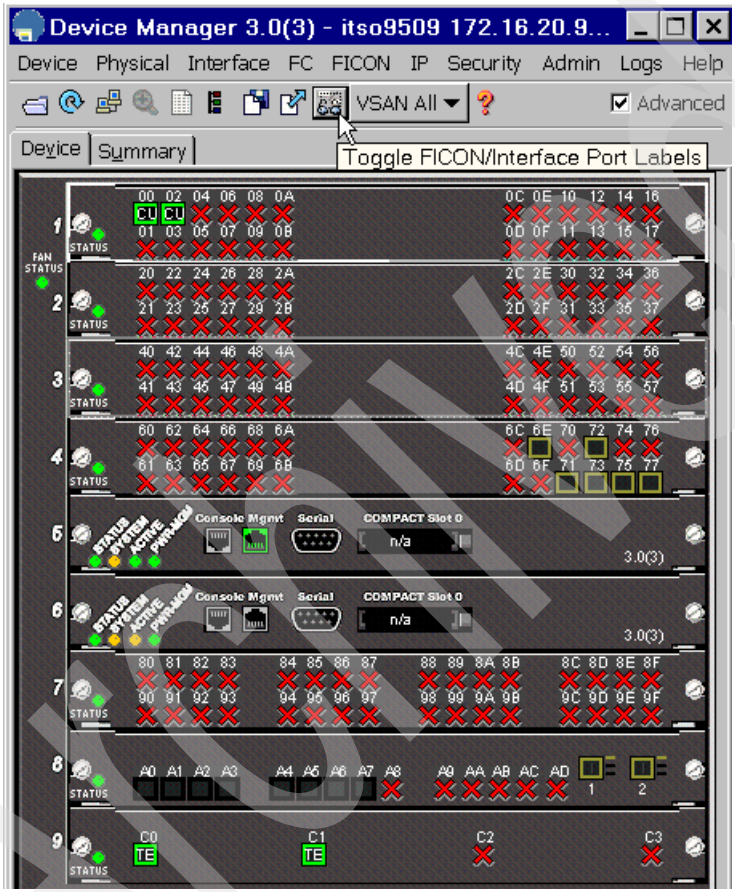


Figure 2 Toggle FICON port numbers in Device Manager

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. On all Cisco MDS 9000 Family switches, 32 port numbers are assigned to each slot—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: You can set the preference in Device Manager to always display FICON port numbers instead of the default interface numbers by selecting **Device** → **Preferences** → **Label Physical Ports View With**, then select **FICON** and click **Apply.**

FICON port number assignment

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'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.

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

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 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.
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 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			
Cisco MDS 9513 Director	Slot 1	0 through 15	224 through 249	250 through 253 and port 255	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 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			

Figure 3 Default FICON port numbering

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.

FCIDs are 3 bytes in length. The first byte is the static domain ID of the switch, in hexadecimal, which matches the switch parameter on the CHPID macro in the IOCDS. The second byte of the FCID is the switch FICON port number (port address). The last byte of the FCID defaults to 0. FICON requires the last byte of the fabric address to be the same for all allocated FCIDs. The value of the last byte can be changed if required, but only when the FICON VSAN is in the offline state.

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 of the ports are flagged to switch from dynamic to static FC IDs and back again. Figure 4 shows the static FC ID allocation for FICON.

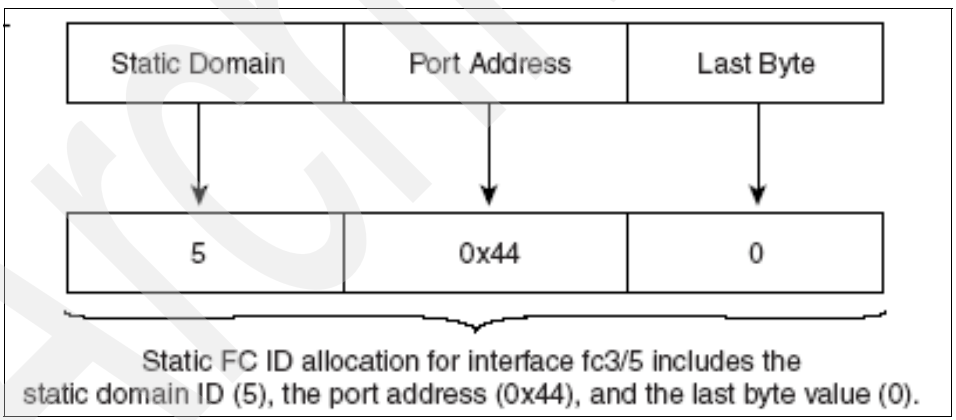


Figure 4 Static FC ID allocation

Port addresses

By default, port numbers are the same as port addresses. You can swap the port addresses, as described in “Using DM to swap ports” on page 62.

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. See Figure 3 on page 6.

Reserved FICON port numbering scheme

A range of 255 port numbers are available to assign to the ports on a switch. Figure 3 on page 6 shows that you can have more than 255 physical ports on a switch and the excess ports do not have port numbers in the default numbering scheme. When you have more than 255 physical ports on your switch, you can assign unimplemented port numbers to the ports, or 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 FICON VSAN can have a maximum of 250 port numbers.

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

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.
- 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.

- 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.

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.

Assigning FICON port numbers to slots

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

1. Select **FICON** → **Port Numbers** to display the FICON port numbers (Figure 5).

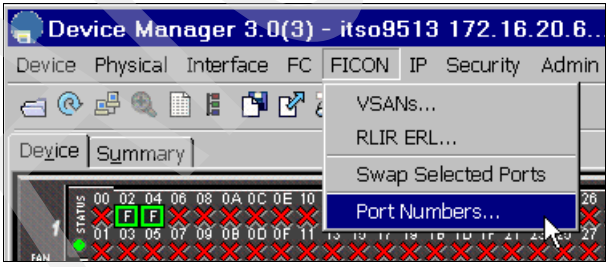


Figure 5 FICON port numbers

2. Enter the chassis slot port numbers in the Reserved Port Numbers field (if so desired), click **Apply**, click **Close** (Figure 6).

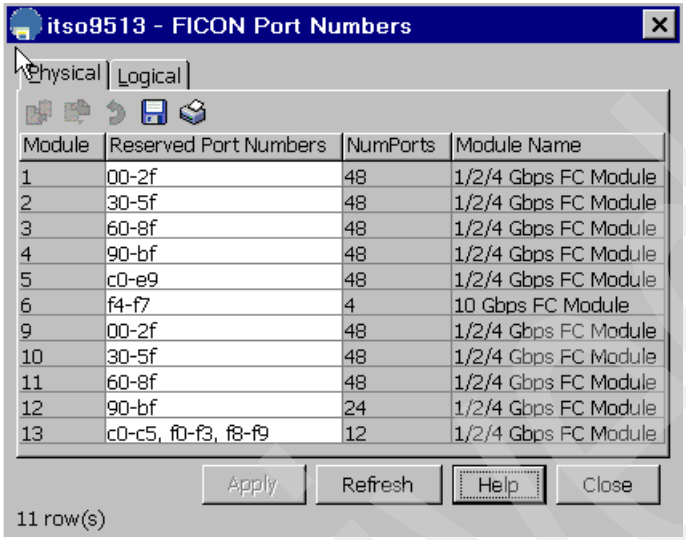


Figure 6 Reserving FICON port numbers

Note: The reserved port numbers can be configured per module. Most times, these reserved port numbers are configured to be contiguous.

Port numbers for FCIP and PortChannel interfaces

FCIP and PortChannels cannot be used in a FICON-enabled VSAN unless they are explicitly bound to a port number. You can use the default port numbers if they are available or if you reserve port numbers from the pool of port numbers that are not reserved for Fibre Channel interfaces.

Reserving FICON port numbers for FCIP and PortChannel

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:

1. Click **FICON** → **Port Numbers** to display the FICON port numbers as shown in Figure 7. Click the **Logical** tab to see the reserved port numbers for the slot.

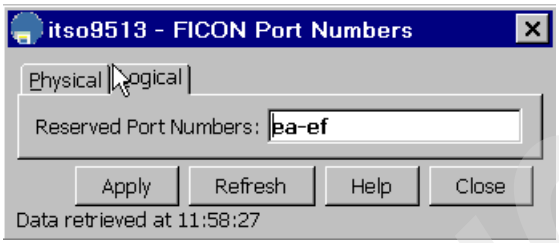


Figure 7 Reserving port numbers

2. 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.
3. After you have selected the ports to reserve, click **Apply** and **Close** to complete the operation.

Cisco MDS 9000 Mainframe Package license

To configure the FICON feature on the Cisco MDS switches, the Cisco MDS 9000 Mainframe Package license must be installed first. This license contains the following features:

- FICON protocol and CUP management
- FICON VSAN and intermixing
- Switch cascading
- Fabric binding

Attention: *Grace period* is the amount of time an application can continue functioning without a license. The grace period is set to 120 days from the first occurrence of using any licensed feature without a license. The grace period starts with the first checkout and is counted only for the days when that feature is used. If you do not use this feature, the grace period stops incrementing.

To obtain new or updated license key files, follow these steps:

1. Collect the host ID of the switch, also referred to as the switch serial number.
2. Obtain your Claim Certificate or the Proof of Purchase document.
3. Locate the Product Authorization Key (PAK) from the Claim Certificate or Proof of Purchase document.
4. Locate the URL from the Claim Certificate or Proof of Purchase document.
5. Access the specified URL that applies to your switch and enter the switch serial number and the PAK.

The license key file is sent to you by e-mail. The license key file is digitally signed to authorize use only on the switch for which it was requested. The requested features are also enabled when the SAN-OS software on the specified switch access the license key file.

The switch serial number can be obtained by selecting **Physical** → **Inventory** from the Device Manager tool bar as shown in Figure 8.

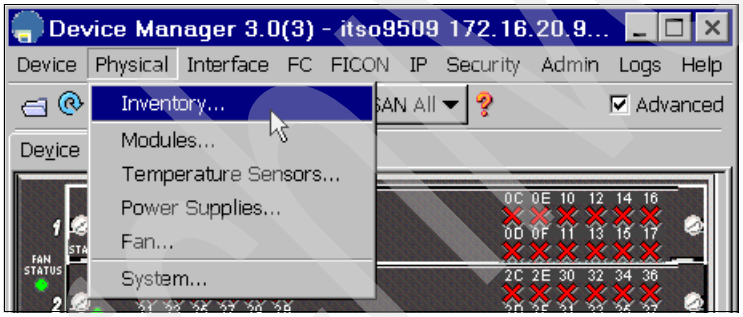
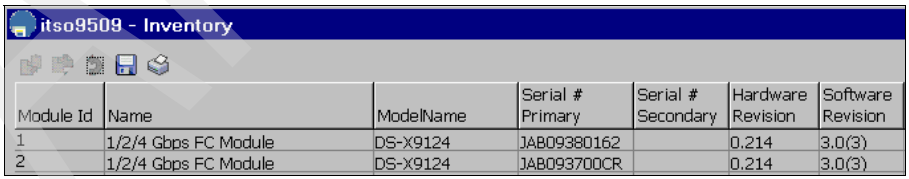


Figure 8 Identifying the switch serial number

This displays the model, serial number, and chassis hardware revision level information as shown in Figure 9.



Module Id	Name	ModelName	Serial # Primary	Serial # Secondary	Hardware Revision	Software Revision
1	1/2/4 Gbps FC Module	DS-X9124	JAB09380162		0.214	3.0(3)
2	1/2/4 Gbps FC Module	DS-X9124	JAB093700CR		0.214	3.0(3)

Figure 9 Switch serial number

After you have received your digitally signed license key (or keys) you can install them on the switch. The license files can be copied to the switch bootflash beforehand, or they can be copied during the install process.

You can also use the Licenses display in FM to verify that the mainframe licenses have been installed. Open Licenses by selecting the **Physical attributes** tab in FM, open the **Switches** folder, and select **Licenses**. Figure 10 shows the installed licenses.

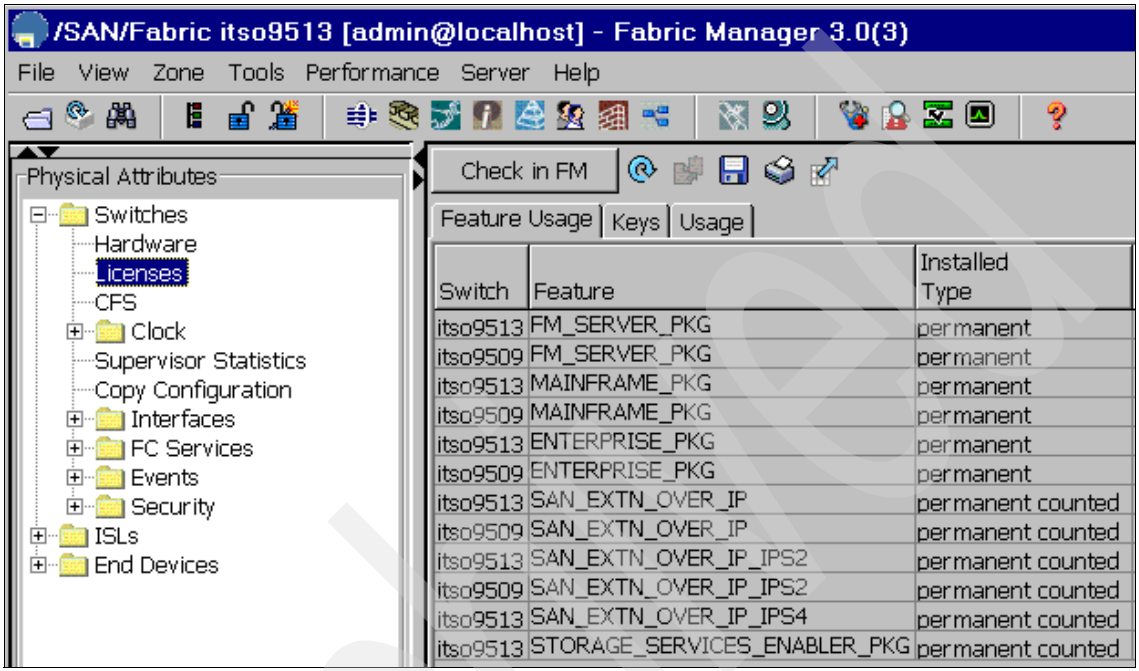


Figure 10 License verification panel

FICON VSAN configuration and requirements

One of the advantages of using the Cisco MDS switches in mixed FCP (open systems) and FICON environments is the ability to separate FICON and FCP traffic into separate VSANs. This is considered best practice. The capability exists, if desired, to mix FCP and FICON traffic into a single VSAN and use zoning to separate the two, but this is *not* the recommended design.

Using separate VSANs provides the following functionality:

- Isolation is improved.
- VSAN based roles for administrative access can be created.
- In-order delivery can be set per VSAN.
- Load balancing behavior can be set per VSAN.
- Default zoning behavior can be set per VSAN.
- Persistent FCIDs can be set per VSAN.

- Domain ID allocation (static or dynamic) behavior can be set per VSAN.
- Fibre Channel timers can be set per VSAN.

This is not an all-inclusive list; it is an overview of how using the VSAN feature enables you to implement FCP and FICON over the same physical topology without sacrificing specific features as a result of FCP or FICON specific fabric/VSAN requirements.

FICON VSAN prerequisites

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

- Set the default zone to **permit** if you are not using the zoning feature.
- Enable in-order delivery on the VSAN.
- Enable (and configure, if required) 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 control unit port (CUP) (area FE) to the zone, if you are using zoning.

All of these requirements must be met to enable the FICON feature.

Next we show the creation of FICON VSAN 2. We again use Fabric Manager to create the cascaded FICON VSAN (VSAN 2) between the 9509 and 9513. We then repeat the process using FM to create the point-to-point FICON VSAN 3 that will reside on the 9513.

At this point we connect the interswitch links between the 9509 and the 9513 as shown in Figure 11 on page 15. This enables us to manage both the 9509 and 9513 switches in the FICON cascaded fabric concurrently.

There are several ways to bring ports online, but perhaps the most intuitive way is to use Device Manager:

1. We loaded DM for the 9506, and have clicked on interface FC9/2 and FC9/1 by holding the CTRL key to highlight both interfaces.

2. We then right-clicked and selected **Enable** from the context menu (Figure 11).

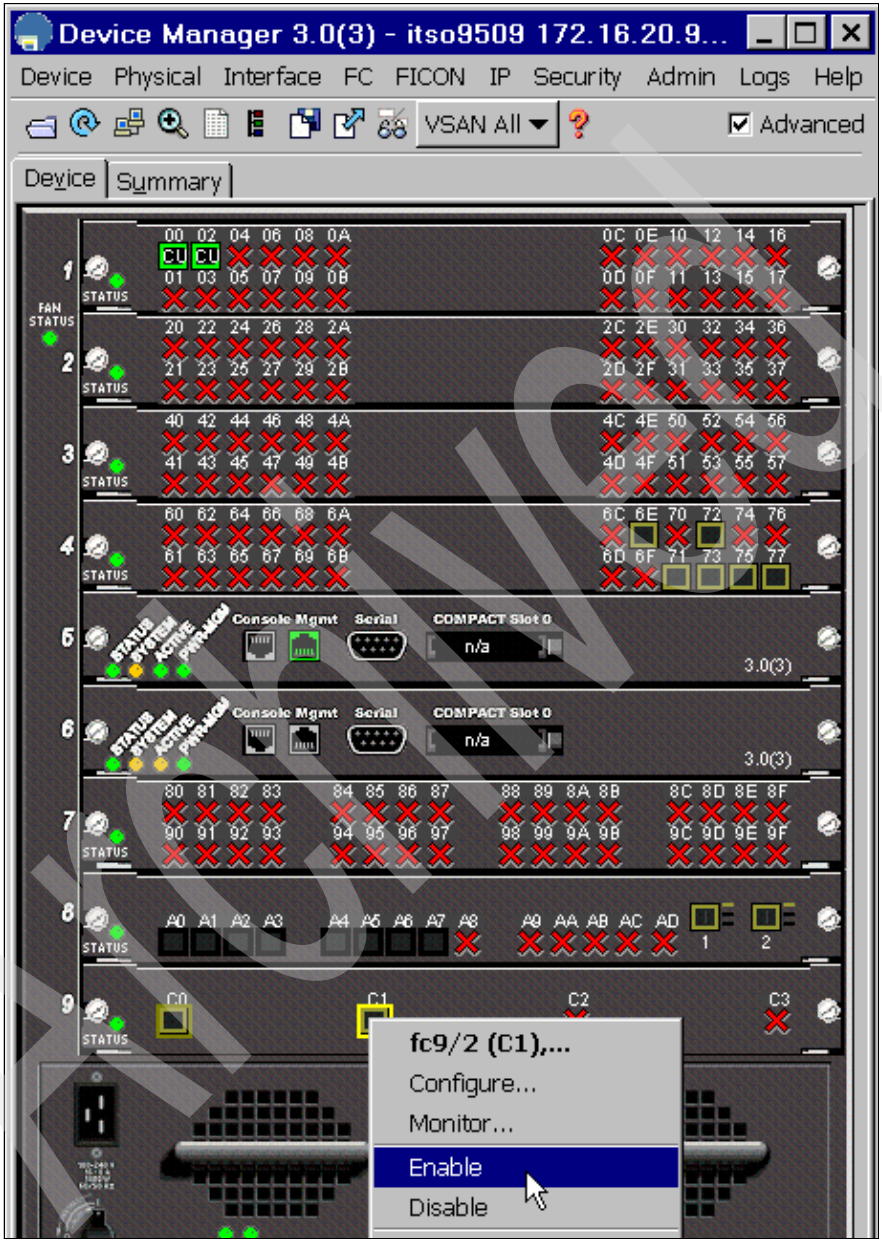


Figure 11 Enable E_Ports in Device Manager on the 9509

3. Repeat these steps in DM for interfaces FC6/1 and FC6/2 on the 9513 as shown in Figure 12.

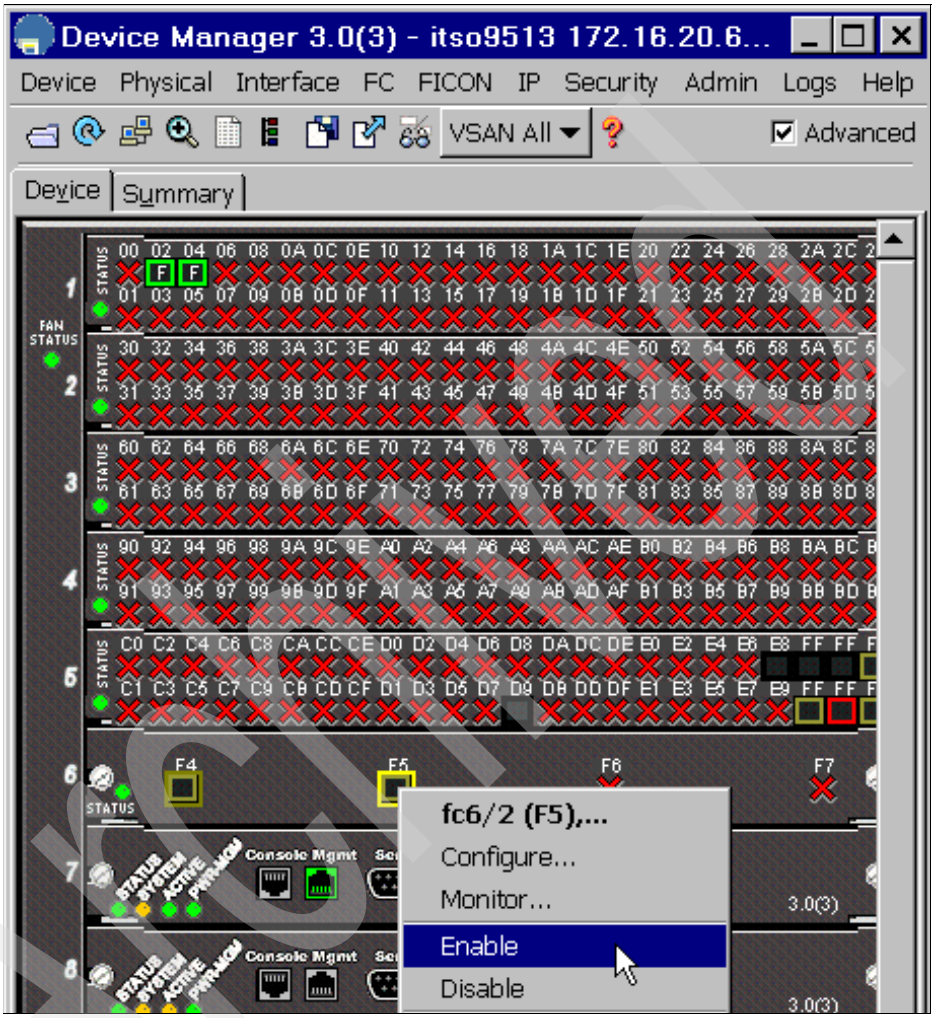


Figure 12 Enable E_Ports on 9513

If we refresh the DM Device view window, it will show a TE indication on the port. This means that the ISLs are up and trunking as shown in Figure 13.

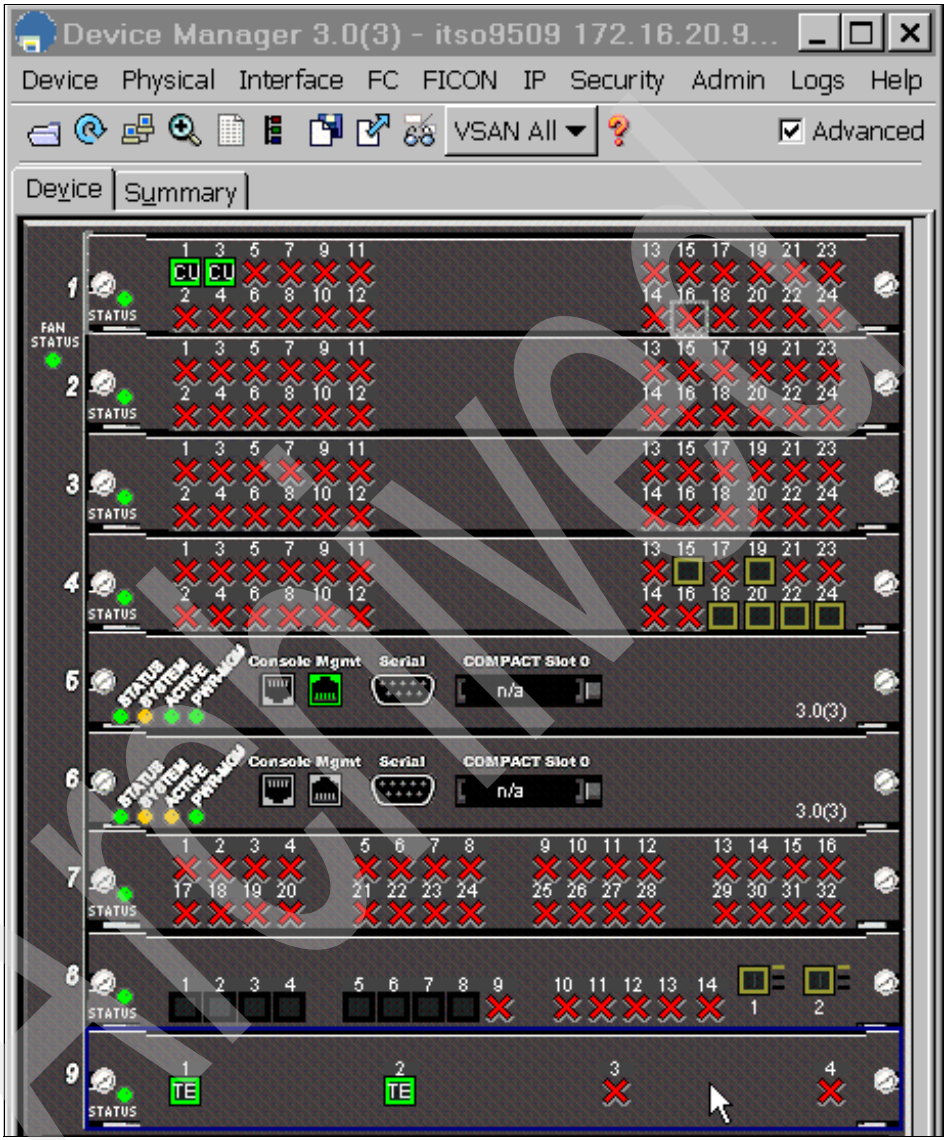


Figure 13 Verify ISL links are up

To begin configuring cascaded FICON VSAN 2:

1. We log on to FM using the FM server located at IP address `172.16.20.60` (Figure 14).

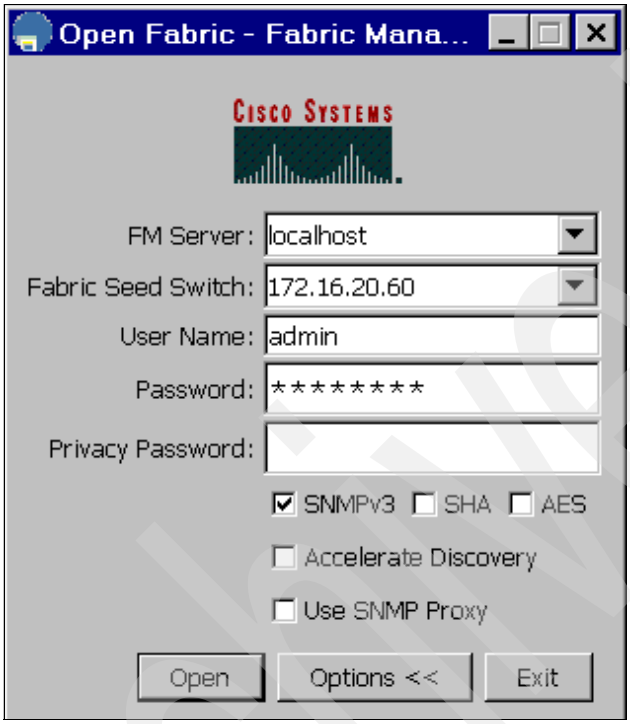


Figure 14 Logging in to FM server

2. Select the **Create VSAN** wizard (Figure 15).

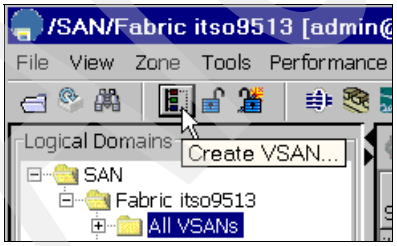


Figure 15 Create VSAN wizard

This opens another panel as shown in Figure 16.

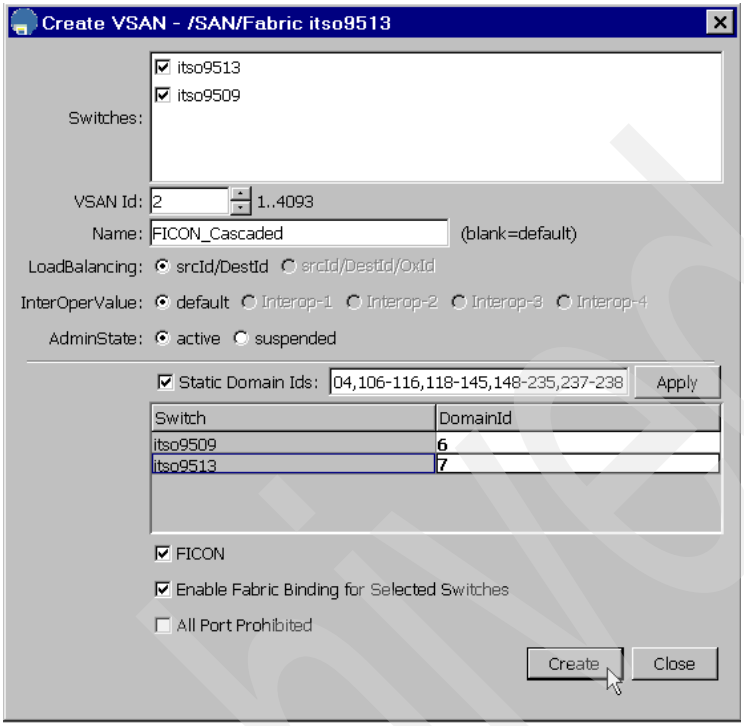


Figure 16 VSAN creation panel

Note the items that are selected in this panel:

- Switches: Both itso9509 and itso9513; VSAN 2 will be created on each
- VSAN ID: 2
- Name: FICON_Cascaded
- LoadBalancing: Source ID / Destination ID (FICON requirement)
- InteropValue: left to default (required)
- Admin state: active
- FICON feature: enabled
- Fabric Binding enabled for this VSAN (required)
- Static domain ID: selected, assigned, and matches what is configured on the mainframe in HCD

When the FICON feature in Cisco MDS switches is enabled, this occurs automatically:

- The IPL configuration file is created (as discussed in “FICON configuration files” on page 54).
- The in-order delivery, source-destination ID load balancing, fabric binding, and static (insistent) domain ID features are enabled for this VSAN and cannot be disabled.
- The default zoning behavior is changed to permit.

We can verify that FICON VSAN 2 was created on each switch with the correct attributes by selecting the **Logical Domains** tab in FM, opening the **FICON_Cascaded(2)** folder, and selecting **VSAN Attributes** (Figure 17).

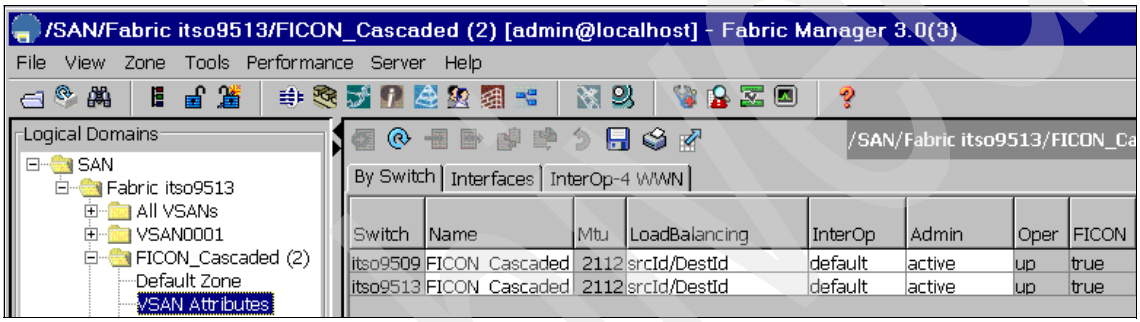


Figure 17 VSAN verification panel one

The default zone behavior (permit is required) can be verified by opening the folder for the created VSAN (FICON_Cascaded in this case), selecting **Default Zone**, then selecting the **Policies** tab as shown in Figure 18.

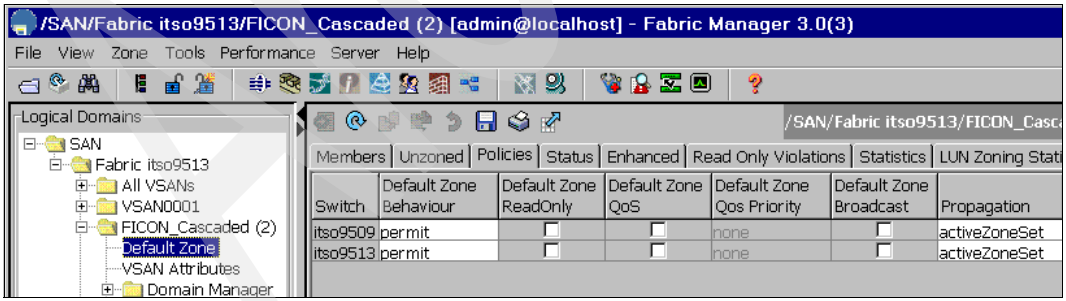


Figure 18 Default zone policy verification

Tip: Using descriptive names for your VSANs helps you identify them more easily in FM and prevent confusion and mistakes.

With cascaded FICON VSAN 2 created, we proceed with the configuration of point-to-point FICON VSAN 3 on the 9513 using the stand-alone version of FM:

1. Log on to Fabric Manager.
2. Select the **Create** VSAN Wizard icon as shown in Figure 19.

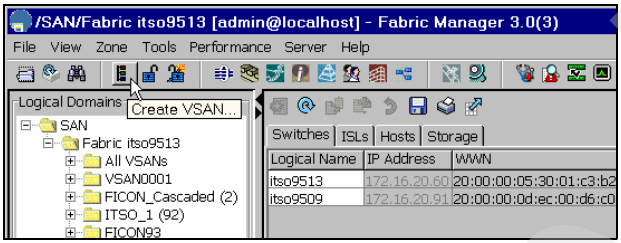


Figure 19 VSAN Create Wizard

This opens the **VSAN Attributes/Create** panel (Figure 20 on page 22).

Note the items that are selected in this panel.

- Switch: only itso9513 is selected
- VSAN ID: 3
- Name: FICON_PT_PT
- Source ID / Destination ID (FICON requirement)
- Interop value: left to default (required)
- Admin state: active
- FICON feature: enabled
- Fabric Binding: enabled (required)
- Static domain ID: 5
  (Static domain ID is selected, assigned, and matches what is configured on the mainframe in HCD.)

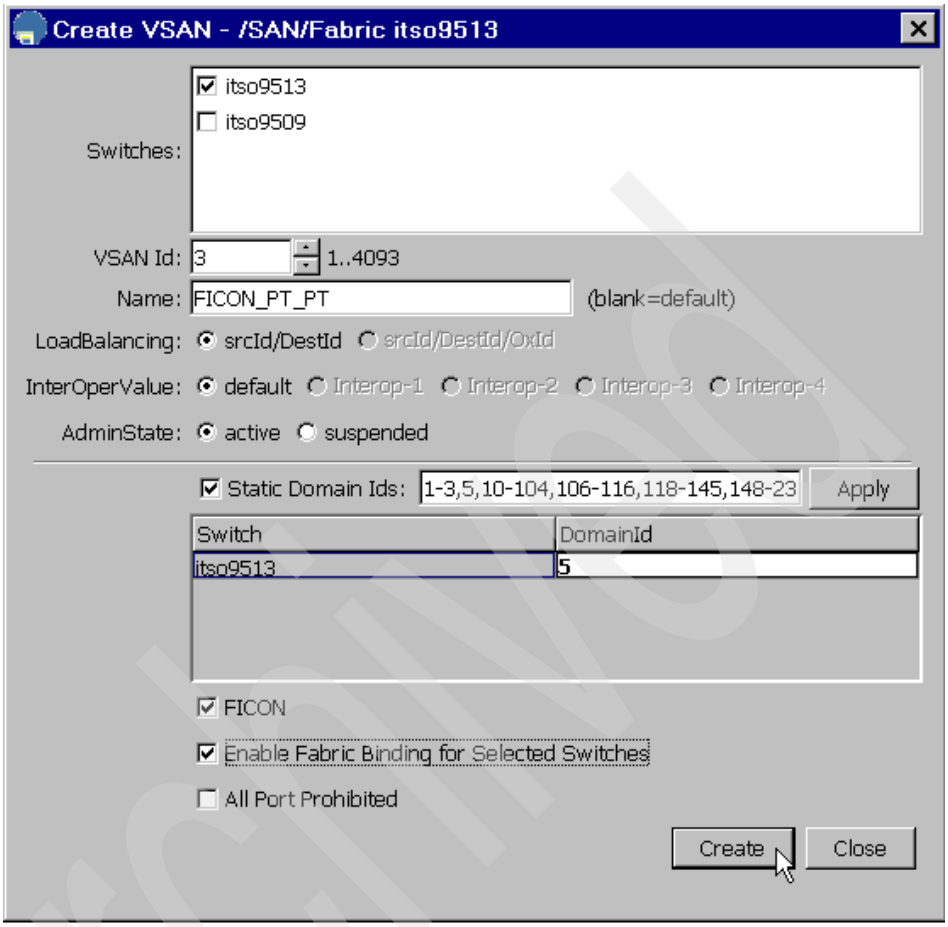


Figure 20 FICON point-to-point VSAN creation

We can verify that FICON VSAN 2 was created on the 9513 with the correct attributes by selecting the **Logical Domains** tab in FM, opening the **FICON_PT_PT** folder, and selecting **VSAN Attributes** as shown in Figure 21.

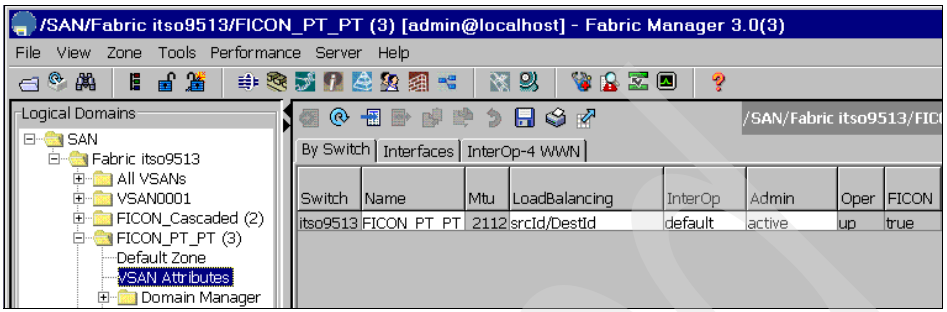


Figure 21 FICON point-to-point VSAN verification

The default zone behavior (permit required) can be verified by opening the folder for the created VSAN (FICON_PT_PT) but in this case by selecting **Default Zone** then the **Policies** tab.

The setting for in-order delivery can be verified by opening the desired VSAN folder (FICON_Cascaded in this case), selecting **VSAN Attributes**, then the **By Switch** tab as shown in Figure 22.

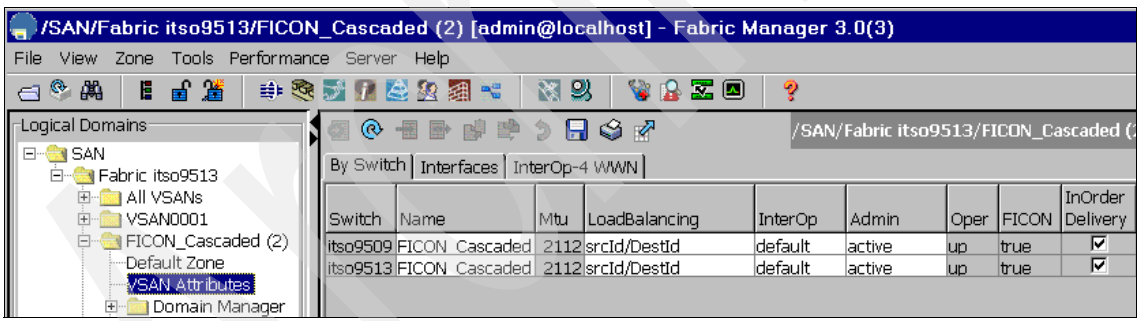


Figure 22 In-order delivery verification

FICON load balancing

FICON uses a load-balancing algorithm based on source and destination ID, so some additional planning is necessary when planning how ISLs, both FC and FCIP, will be designed. An automated tool in FM has been developed to aid in this exercise: the FICON Flow Load Balance Calculator (Figure 23).

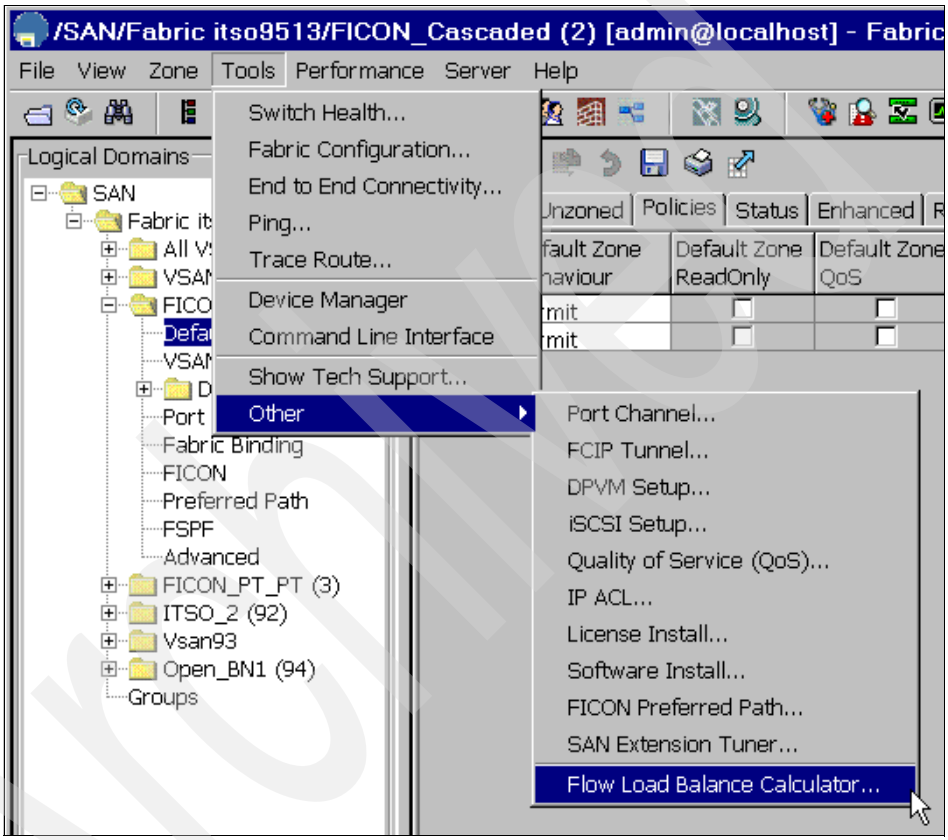


Figure 23 FM FICON Flow Load Balance Calculator

Figure 24 on page 25 shows the calculator. To determine the proper ISL configuration:

1. We clicked **Add** twice.
2. We entered the Source and Destinations flows from **Source** (FCIDS 0x**0602**00 and 0x**0604**00) to the **Destinations** (FCID 0x**6902**00).
3. We selected **2** for the **Number of ISLs** to be used (in this case the ISLs were FCIP links) and clicked **Calculate**.

The Recommended Topology appears as shown in Figure 24.

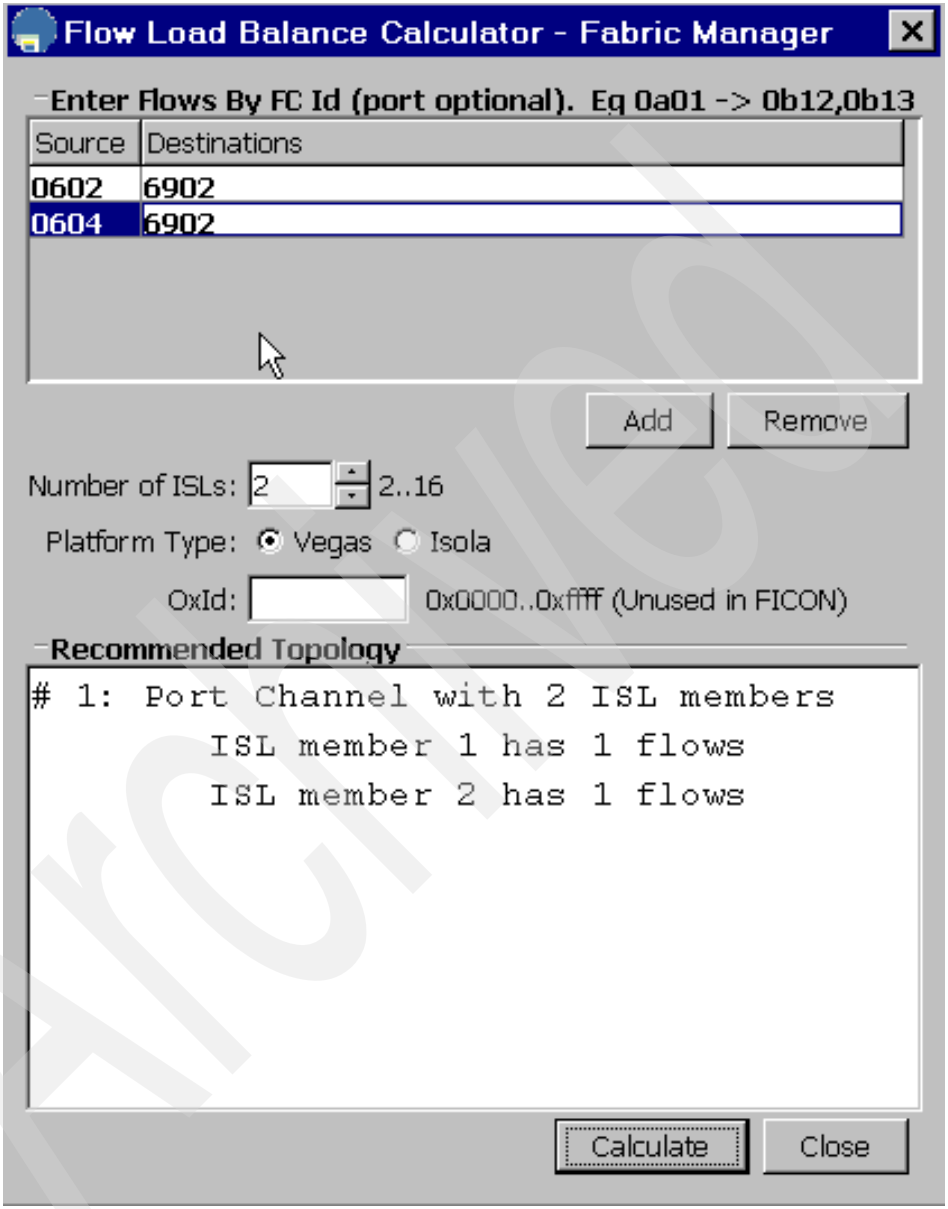


Figure 24 FM FICON Flow Load Balance Calculator

Note: The Platform Type `Vegas` refers to Generation 1 (1 and 2 MBs) linecards. The `Isola` type refers to Generation 2 (1,2, and 4 MBs) linecards.

Static domain ID configuration

As mentioned previously, static (insistent) domain IDs are a requirement for FICON. The use of static domain IDs is required because this information is statically coded in the IOCDS **CHPID** and **CNTLUNIT** macros, and is part of the fabric binding database. MDS switches have a concept of a running and configured domain ID. When you change the domain ID and make it static, you must disruptively restart this VSAN in order for the newly configured domain ID to take effect.

Note: This is done automatically as part of the FM FICON VSAN create wizard.

Fabric binding configuration

Fabric binding is a security feature that enables explicit control over which switches can be part of a fabric by manually defining the authorized switches in a fabric binding database. This prevents non-authorized switches from joining the fabric either accidentally or intentionally. Each FICON switch that is allowed to connect to the fabric must be added to the fabric binding database of every other FICON switch in the fabric. Activating fabric binding is a prerequisite for enabling FICON on a VSAN.

In FICON cascaded topology the fabric binding database contains the switch World Wide Name (sWWN) and domain ID of all switches authorized to join the fabric. Fabric binding authorization is enforced per VSAN, as each VSAN is a logical fabric. In a FICON point-to-point topology fabric binding is still required but the fabric binding database is empty because defining the local sWWN and domain ID in the fabric binding database is not required.

There are two fabric binding databases:

- *Configuration database:* Contains all manually configured sWWNs and domain IDs of those switches that are authorized to join the fabric.
- *Active database:* Contains the entries that are being enforced in the fabric.

To start enforcing a newly created or modified configuration database, an activation sequence must be performed. The activation replaces the active database with the configured database. This activation will fail if the configured database does not match the current state of the fabric (for example, if a switch is in the fabric but not defined in the database, or if a switch is in the fabric but has a different domain ID than is defined in the configuration database). Alternatively the force option could be used to activate the new fabric binding configuration, which will isolate the switch in question.

Attention: It is very easy to make a mistake in the configured fabric binding database by using the force option and causing isolation to occur in the fabric. The force option must be used with discretion and care.

Next, we proceed with the verification of the fabric binding database for both the point-to-point VSAN 3 and the cascaded VSAN 2.

To verify that fabric binding is enabled, we open the folder of the VSAN we want to examine by selecting **Fabric Binding**, and examining the Status column as shown in Figure 25 and Figure 26.

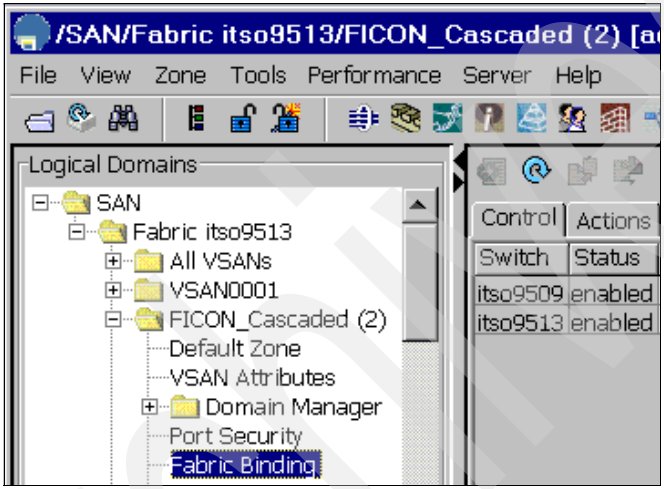


Figure 25 Fabric binding status of VSAN 2

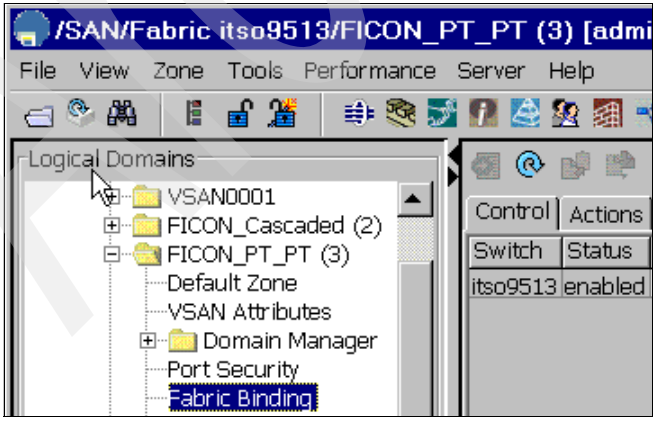


Figure 26 Fabric binding status of VSAN 3

These displays show that fabric binding is enabled, and it was done as part of the FICON VSAN creation process. The next step is to configure the fabric binding database for VSAN 2, verify it, and activate it.

Note: This is can be done automatically by the FM FICON VSAN create wizard.

Figure 27 shows the currently configured database. As an example of how to remove entries, we delete the entries by pressing the CTRL key and clicking each entry. When the entries are highlighted, either right-click and select **Delete Row** from the context menu, or click the **Delete Row** icon.

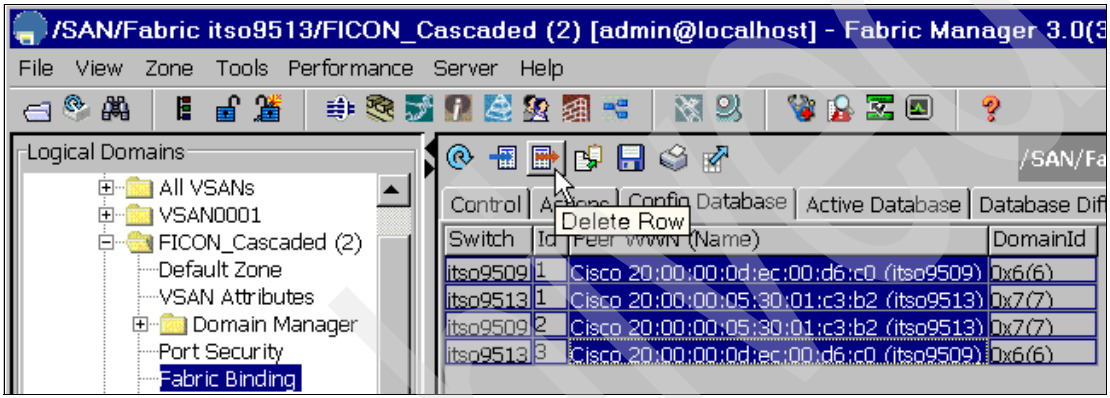


Figure 27 Current Fabric Binding database for VSAN 10

After the entries are deleted, create the new fabric binding entries with the updated domain IDs:

1. Click the **Create Row** icon at the top of the pane as shown in Figure 28.

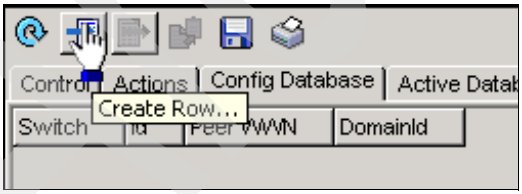


Figure 28 Create new fabric binding entries

2. This opens another window where you can select the sWWNs to add to the fabric binding configuration database. Figure 29 shows adding the 9509 to the fabric binding database of both switches.

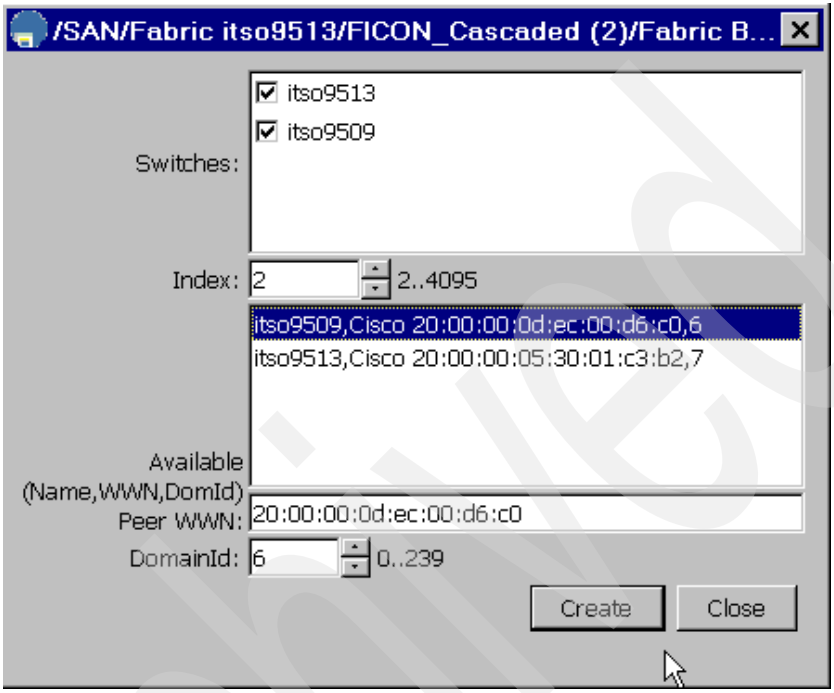


Figure 29 Creation of the fabric binding entry for the 9513 on both switches

3. Figure 30 shows adding the 9513 to the fabric binding database of both switches.

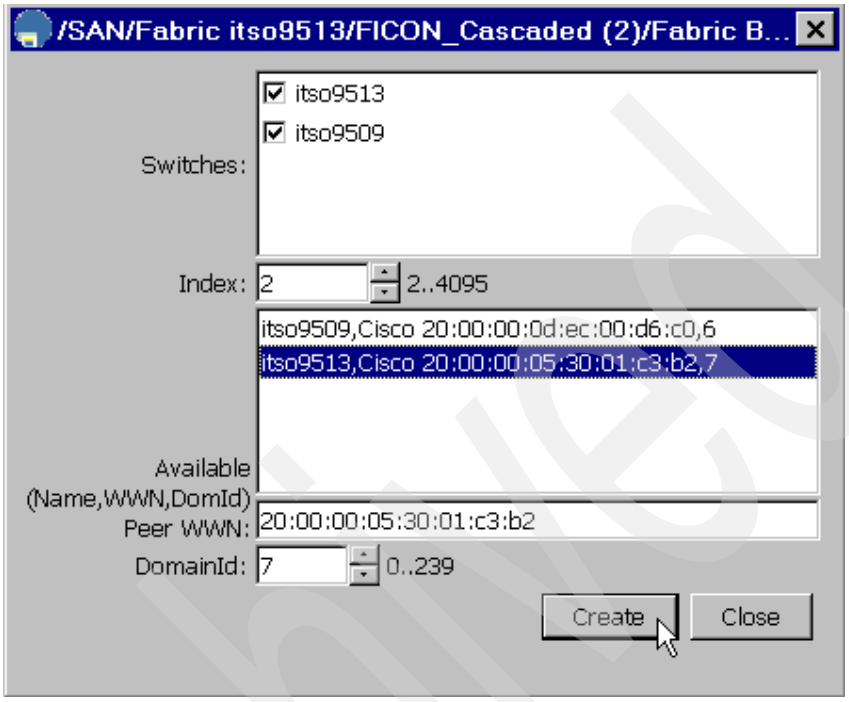


Figure 30 Creation of the fabric binding entry for the 9506 on both switches

4. Verify the newly configured fabric binding database to confirm its accuracy by selecting the **Config Database** tab (Figure 31).

Control | Actions | Config Database | Active Database | Database Differences

Switch	Id	Peer WWN (Name)	DomainId
itso9509	1	Cisco 20:00:00:0d:ec:00:d6:c0 (itso9509)	0x6(6)
itso9513	1	Cisco 20:00:00:05:30:01:c3:b2 (itso9513)	0x7(7)
itso9513	2	Cisco 20:00:00:0d:ec:00:d6:c0 (itso9509)	0x6(6)
itso9509	2	Cisco 20:00:00:05:30:01:c3:b2 (itso9513)	0x7(7)

Figure 31 New fabric binding entries

5. Activate the newly defined configuration database: Click the **Actions** tab, click in the Action column for each switch and select **activate** from the pull-down selection list. Click the **Apply Changes** icon (Figure 32).

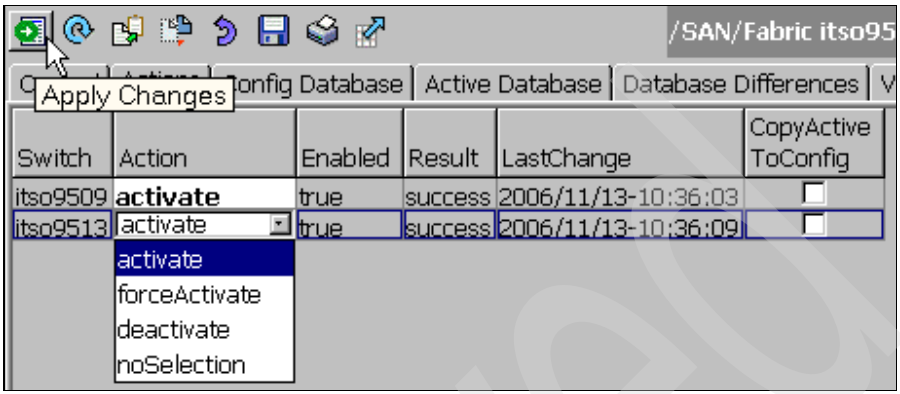


Figure 32 Activate new fabric binding database

If correct, the active fabric binding database should appear as in Figure 33.

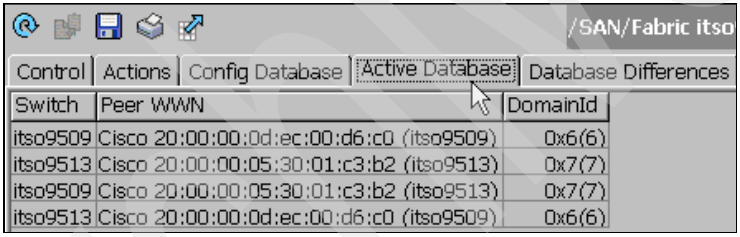


Figure 33 Current active fabric binding database

PortChannel configuration

PortChannels refer to the aggregation of multiple physical interfaces into one logical interface to provide higher aggregated bandwidth, load balancing, and link redundancy. PortChannels should be built using interfaces across multiple switching modules so that a failure in one module does not bring down the PortChannel link.

In summary, PortChannels provide increased reliability and performance by:

- Combining multiple ISLs into a single logical link.
- Aggregating bandwidth by distributing traffic among all functional links in the PortChannel.

- Providing high availability. If one physical link fails, traffic previously carried on this link is switched to the remaining links. If a link goes down in a PortChannel, the upper protocol is not aware of it. To the upper protocol, the link is still there, although the bandwidth is diminished. The routing tables are not affected by link failure. PortChannels may contain up to 16 physical links and may span multiple modules for added high availability.

We will create our PortChannel configuration by using the PortChannel Wizard inside FM, but in order to use this wizard, ISLs between the switch must be currently up and active. Remember that this was done prior to the creation of the FICON VSANs discussed in “FICON VSAN configuration and requirements” on page 13. Refer to that for details about how to activate the ISLs.

1. After verifying that both ISLs have come online, select the PortChannel wizard icon as shown in Figure 34.

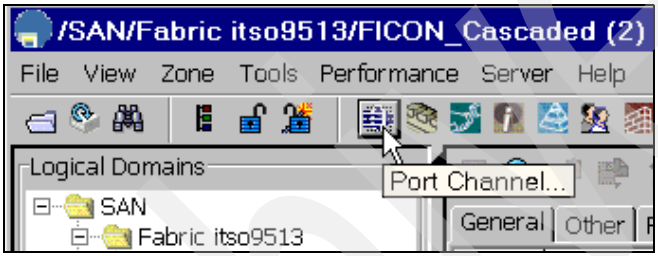


Figure 34 PortChannel Wizard in FM

2. This opens the PortChannel Wizard series of panels. In the first (Figure 35), we select the switches we want to create the PortChannel between (itso9509 and itso9513). Select **Create New** and click **Next**.

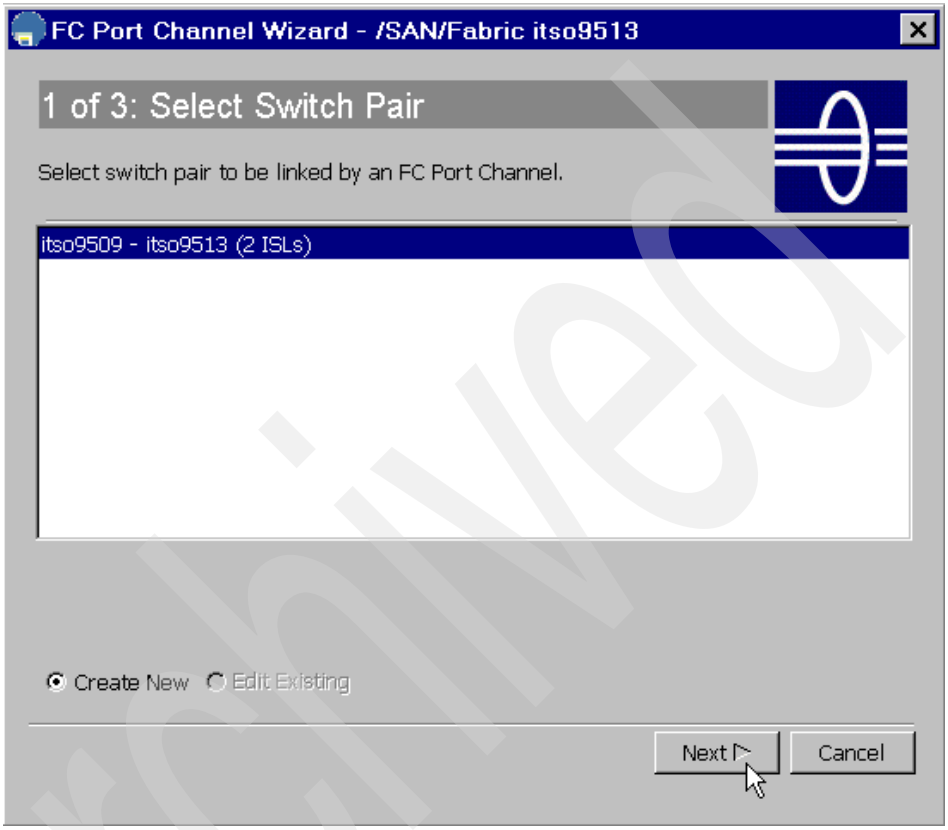


Figure 35 PortChannel panel 1 of 3

3. In the next panel (Figure 36), select the ISLs to bundle into the PortChannel. It is best practice to select links from multiple modules for high availability reasons.

   In our case we did not have this option. We selected ISLs that were connected to ports 9/1 and 9/2 on the 9509, and ports 6/1 and 6/2 on the 9513. We then used the right arrow icon to move the ISLs from the Available column to the Selected column.

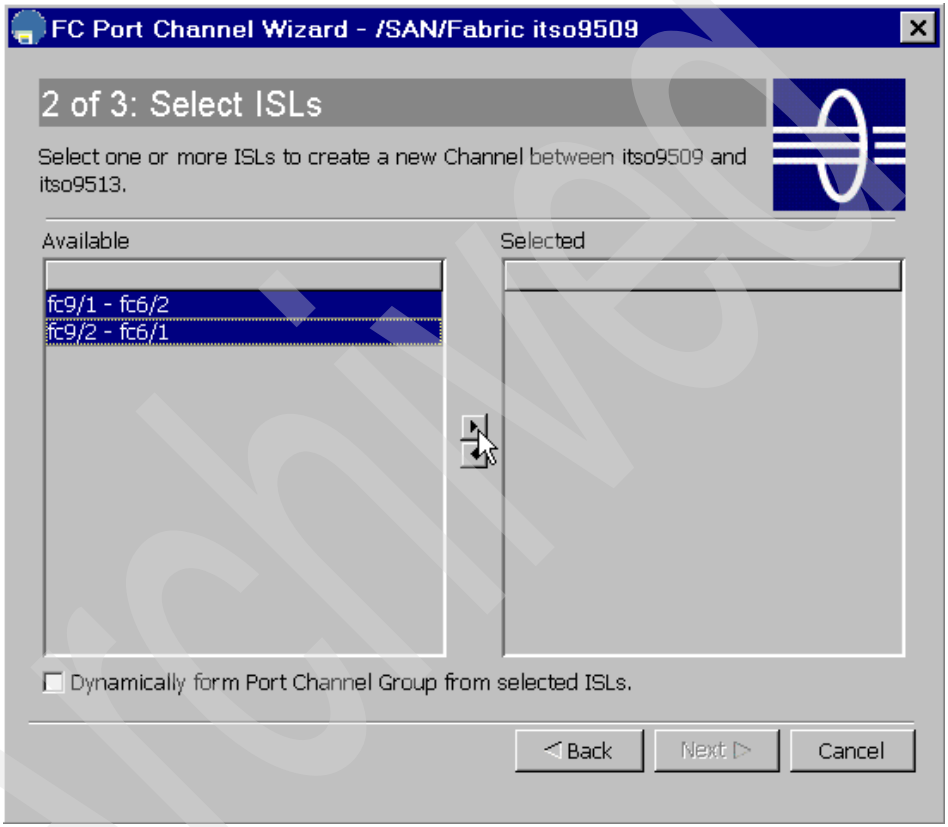


Figure 36 PortChannel ISL selection panel

4. The box to Dynamically form Port Channel Group from selected ISLs is not selected because we want to designate the FICON Port address ourselves. To proceed with the configuration of the PortChannel, click **Next** (Figure 37).

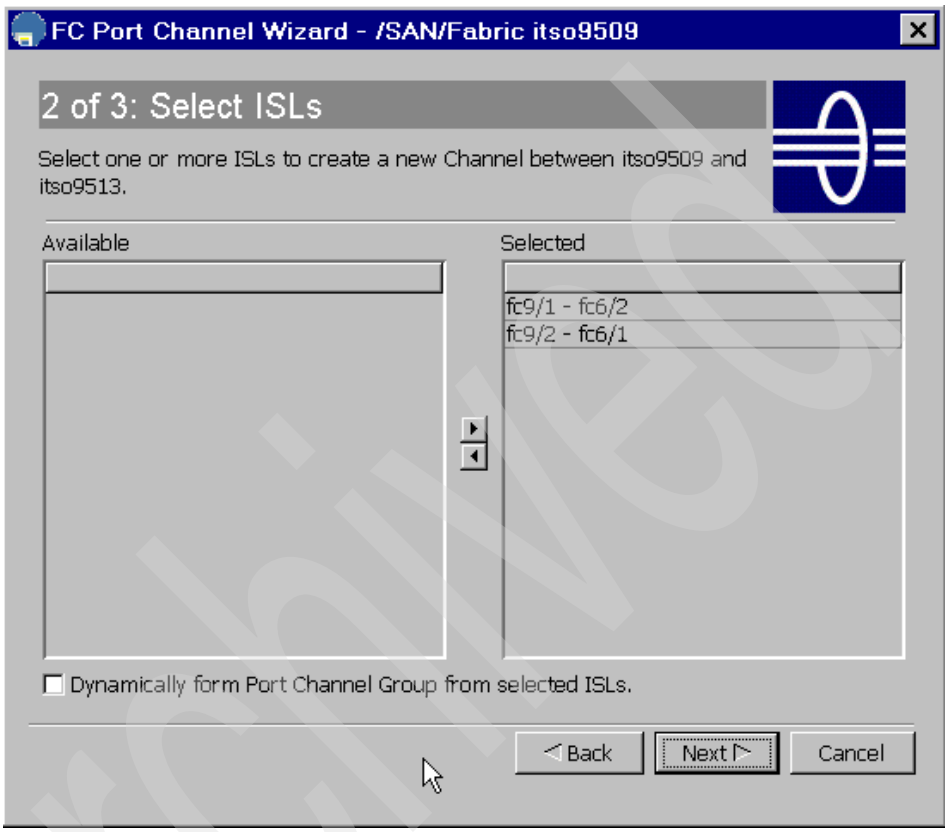


Figure 37 PortChannel ISL selection panel 2

5. Set the attributes of the PortChannel in panel 3 of the PortChannel wizard (Figure 40 on page 38). The following attributes can be set:
   - Channel ID number
   - Description of the PortChannel

     The wizard will put in a default description of the destination if one is not entered. The configuration in both switches is updated with this description.
   - FICON Port Address

   To get the next available FICON port address, click the **...** box shown in Figure 38.

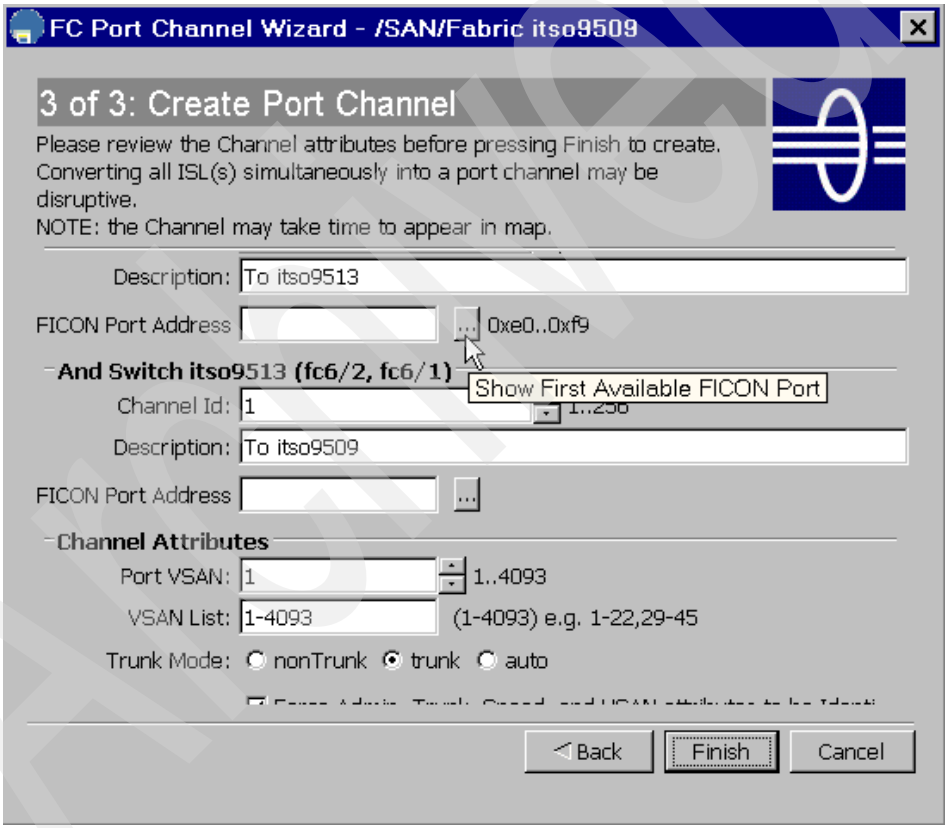


Figure 38 Show first available FICON port

6. This opens the window shown in Figure 39. We enter the value 0xe0 into the field and repeat the process for the next switch.

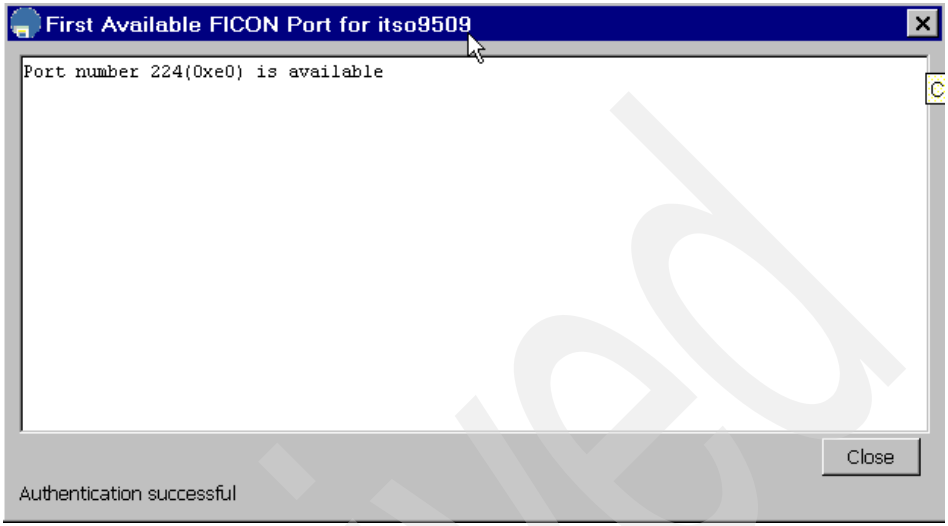


Figure 39 First available FICON port

7. It is recommended that you leave the **Force Admin, Trunk, Speed, and VSAN attributes to be identical** box selected (Figure 40). This helps eliminate configuration errors.

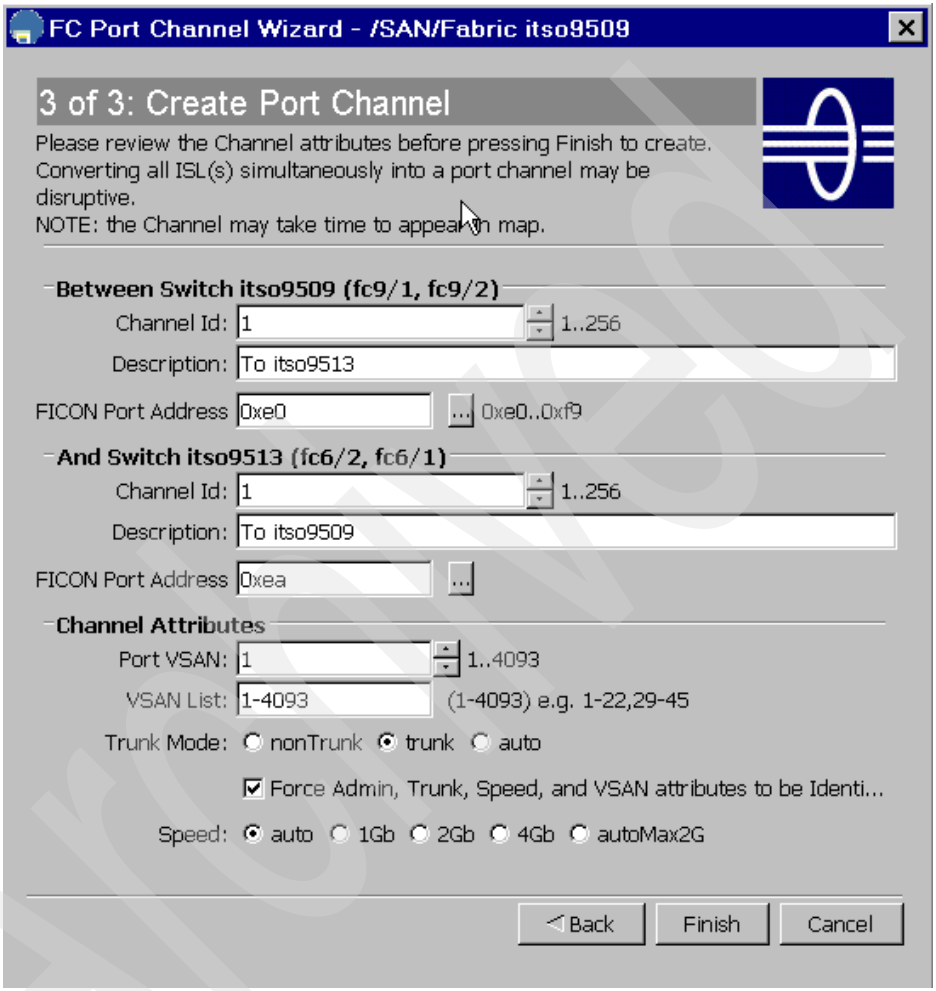


Figure 40 PortChannel wizard panel 3

The error message in Figure 41 warns that moving ISLs into PortChannels is a disruptive operation.

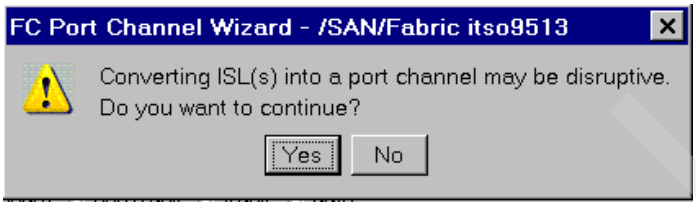


Figure 41 PortChannel creation warning message

8. In DM, to verify the PortChannel operation, select the **Interface** → **Port Channels** on the 9513 (Figure 42).

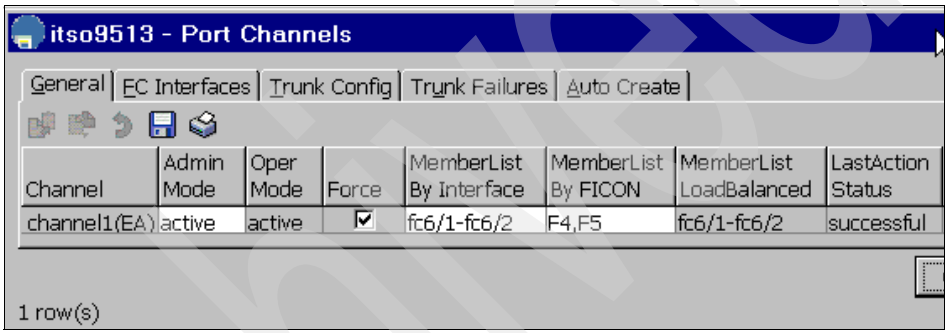


Figure 42 9513 Port Channel verification

9. We did the same on the 9509 as shown in Figure 43.

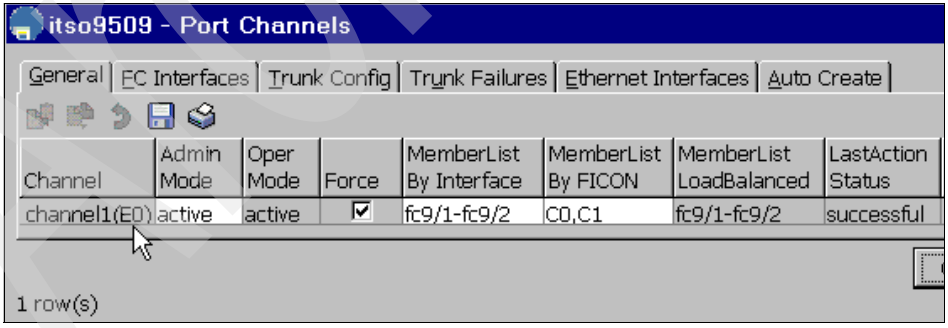


Figure 43 9509 verification

10. If at any point you need to take down (known as “admin down”) and then bring back up (known as “admin up”) the logical PortChannel interface to cause a reinitialization to occur, this can be done in FM by selecting the **Physical Attributes** tab, open the **Switches** → **Interfaces** folders, and select **FC Logical**.

    From the **General** tab (Figure 44), Admin **down** the PortChannel in question and click **Apply**. To Admin up the PortChannel, select **up** and **Apply** the changes.

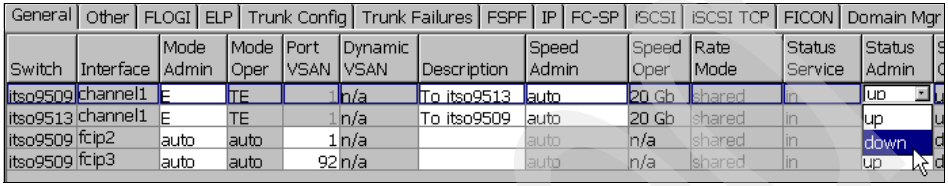


Figure 44 Causing reinitialization

It will take a while for FM to display the changes so we use the CLI command **`sho int port-channel`** on both the 9509 and the 9513 to verify that all is well, as shown in Example 1 and Example 2 on page 41.

Example 1 9509 display

```
itso9509# sho int port-channel 1
port-channel 1 is trunking
    Port description is To itso9513
    Hardware is Fibre Channel
    Port WWN is 24:01:00:0d:ec:00:d6:c0
    Admin port mode is E, trunk mode is on
    snmp traps are enabled
    Port mode is TE
    Port vsan is 1
    Speed is 20 Gbps
    Trunk vsans (admin allowed and active) (1-2,92-94)
    Trunk vsans (up)                       (1-2,92-94)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()
    5 minutes input rate 13608 bits/sec, 1701 bytes/sec, 21 frames/sec
    5 minutes output rate 12808 bits/sec, 1601 bytes/sec, 19 frames/sec
      6670 frames input, 502336 bytes
        0 discards, 0 errors
        0 CRC,  0 unknown class
        0 too long, 0 too short
      5927 frames output, 461048 bytes
        0 discards, 0 errors
```

```
      0 input OLS, 2 LRR, 0 NOS, 0 loop inits
      3 output OLS, 2 LRR, 0 NOS, 0 loop inits
--More--
```

Example 2 9513 display

```
   itso9513# sho int port-channel 1
   port-channel 1 is trunking
       Port description is To itso9509
       Hardware is Fibre Channel
       Port WWN is 24:01:00:05:30:01:c3:b2
       Admin port mode is E, trunk mode is on
       snmp traps are enabled
       Port mode is TE
       Port vsan is 1
       Speed is 20 Gbps
       Trunk vsans (admin allowed and active) (1-2,92-94)
       Trunk vsans (up)                       (1-2,92-94)
       Trunk vsans (isolated)                 ()
       Trunk vsans (initializing)             ()
       5 minutes input rate 2440 bits/sec, 305 bytes/sec, 1 frames/sec
       5 minutes output rate 808 bits/sec, 101 bytes/sec, 1 frames/sec
         6517 frames input, 599860 bytes
           0 discards, 0 errors
           0 CRC,  0 unknown class
           0 too long, 0 too short
         7205 frames output, 542860 bytes
           0 discards, 0 errors
         2 input OLS, 2 LRR, 2 NOS, 0 loop inits
         2 output OLS, 2 LRR, 0 NOS, 0 loop inits
   --More--
```

To use FM to display the ISL/PortChannel operation, hover the cursor on the ISL between itso9509 and itso9513 in the SAN fabric map as shown in Figure 45.

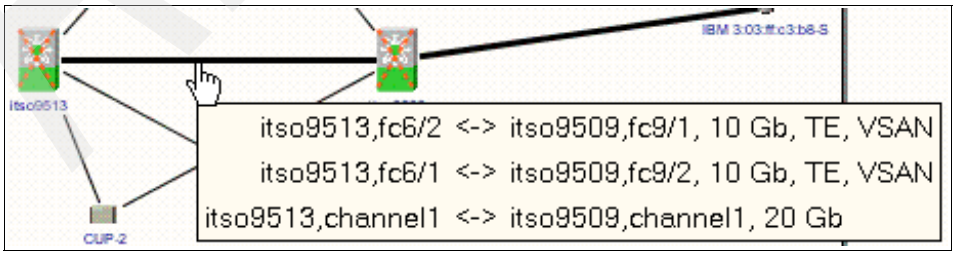


Figure 45 FM ISL display

Moving ports to the FICON VSAN

The last FICON switch configuration step moves all of the required ports for the channels and control units into the correct FICON VSANs and enables the ports. Remember that FICON VSAN 5 was defined on the 122 switch, and FICON VSAN 10 was on the 81 and 49 switches. We perform this operation once for *each* fabric.

Previously we used Device Manager to enable the ISL ports; for this section we use Fabric Manager to configure and enable ports.

1. Click the **Physical Attributes** tab in FM.
2. Open **Switches** → **Interfaces** folder, and select **FC Physical** as shown in Figure 46.
3. Click the **General** tab in the right information pane above the FM map to display the panel shown in Figure 46. Sort on any column by clicking it once.

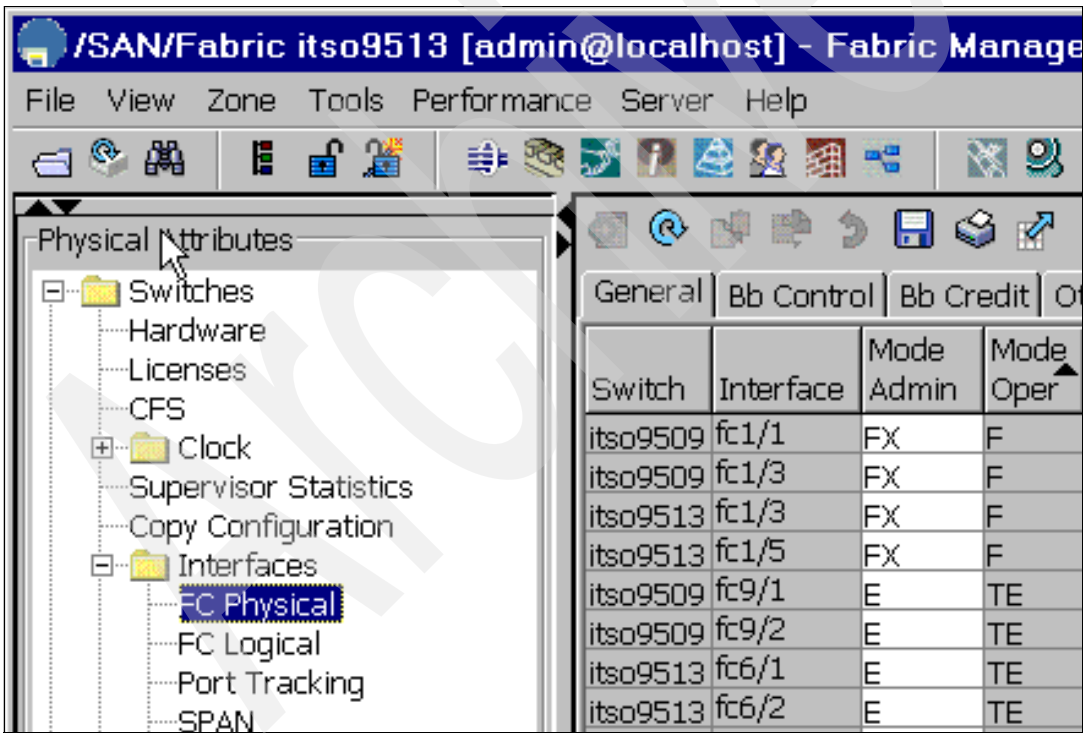


Figure 46 General tab of FM physical interface display

4. Place the ports you are using into the VSAN you want them in (in our case we change from VSAN 92 to VSAN 2), set them to **Admin Up** status (if not up already) as shown in Figure 47 on page 43 and Figure 48, and apply the changes.

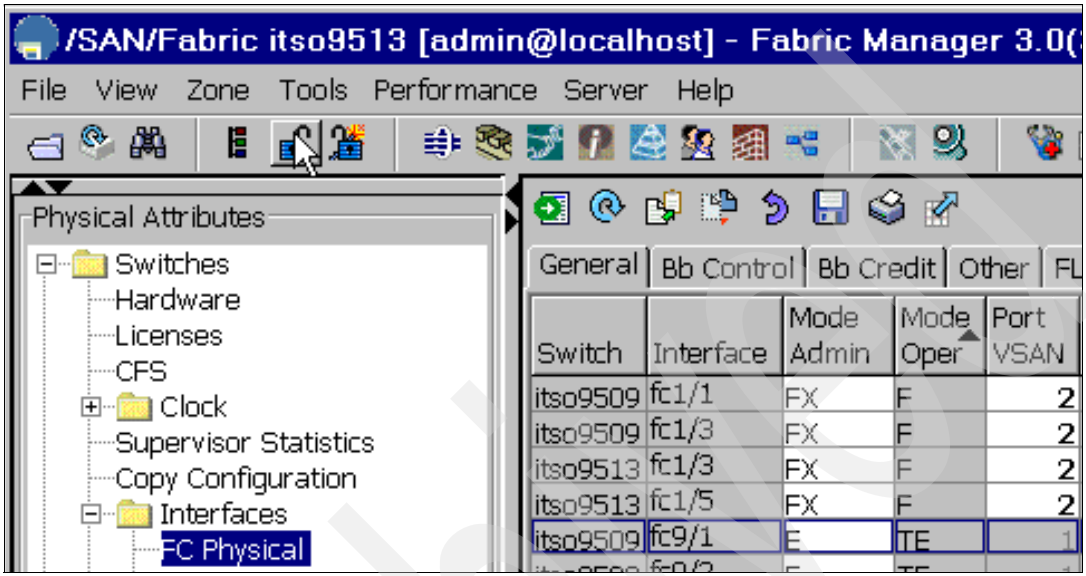


Figure 47 Ports on the 9509 that we want to change

5. Click **Apply Changes** (Figure 48).

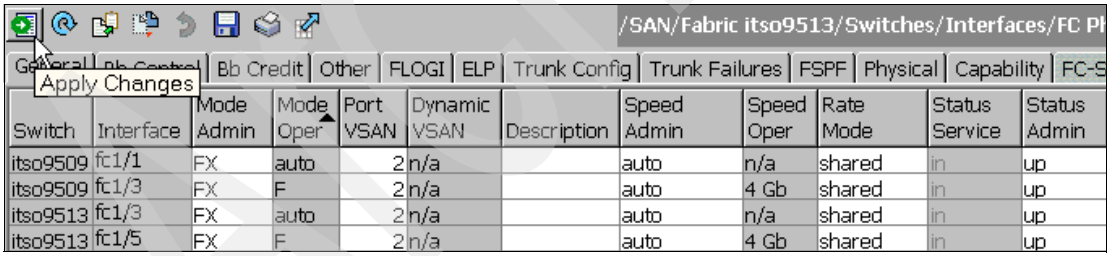


Figure 48 Ports on the 9513 we want to change

This process must be repeated for switch.

CUP 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.

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.

1. To start the process to set the default zone to `permit`, select **Zone** → **Edit Local Full Zone Database** (Figure 49).

Note: There is no need to explicitly zone the CUP devices. Setting the default zone to permit should be sufficient. We show the process in case you have a need to explicitly zone it.

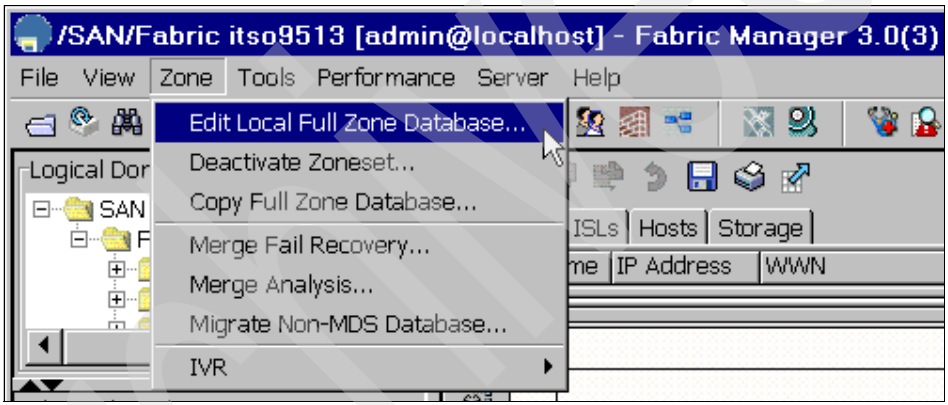


Figure 49 Edit Local Full Zone Database

2. In Edit Local Full Zone Database Edit, select **Edit** → **Edit Default Zone Attributes** (Figure 50).

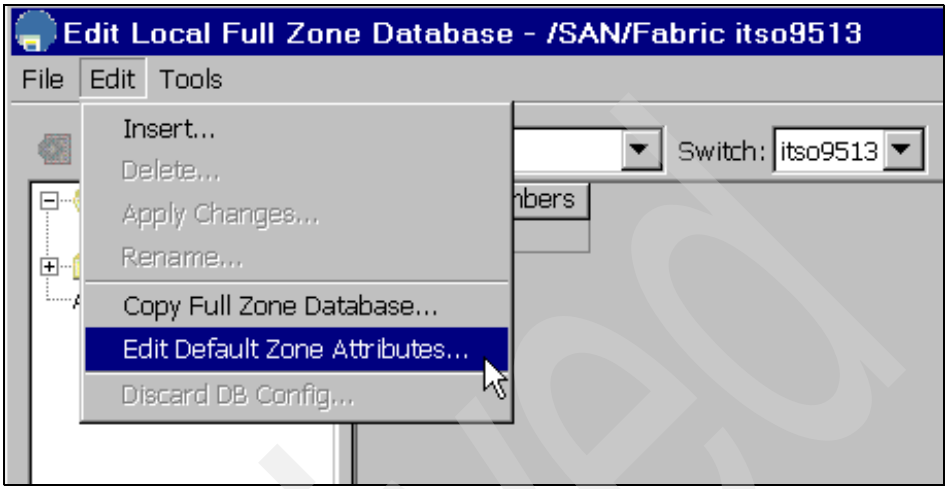


Figure 50 Edit Default Zone Attributes

3. Set the policy to `permit` if it is not already set and click **OK** (Figure 51).

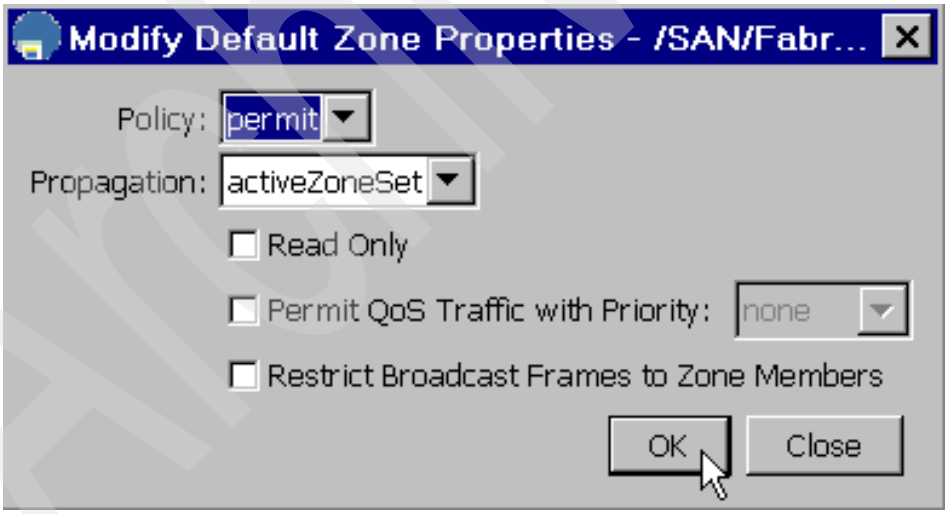


Figure 51 Modifying properties

4. In Figure 52, from **Device Manager** → **FC** → **Name Server** for our VSAN (93 in this case) we obtain the FICON:CUP WWN.

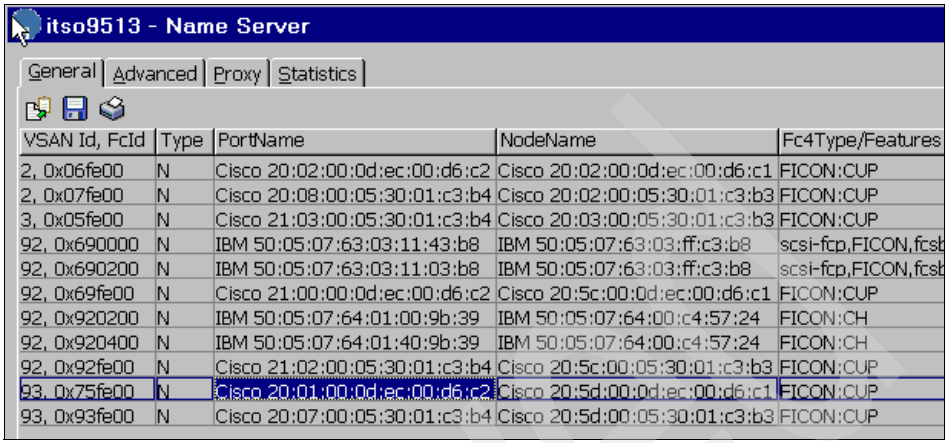


Figure 52 Name Server

5. Edit the zone database for the FICON93 VSAN (Figure 53).

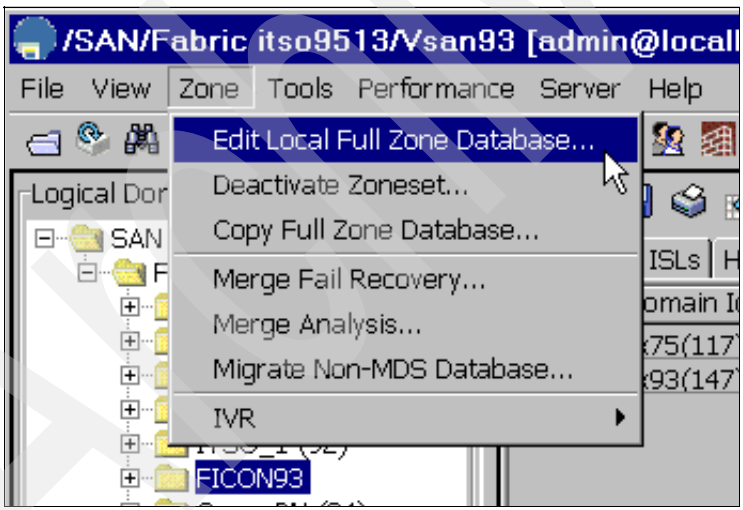


Figure 53 FICON93

Figure 54 shows the zone after we have dragged and dropped itso9509 into the zone (that we identified in Figure 52 on page 46).

Important: If more than one FICON:CUP exists in this fabric, make sure to add all the FICON:CUP WWNs to the required zone.

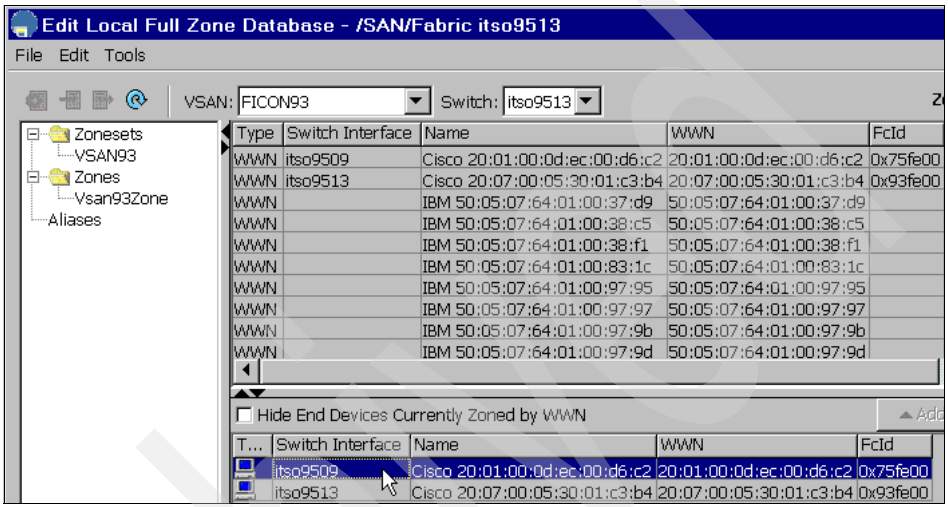


Figure 54 itso9509 dragged and dropped

Bringing CHPIDs, devices and CUP online

After configuring the switches in both fabrics for FICON, you can start to bring the host ports (CHPIDS), the devices, and the CUP devices online. Figure 55 shows that the channel ports are online in Device Manager for the 9513.

Figure 55 DM device view indicating channels online

Figure 56 shows that the CUs are online.

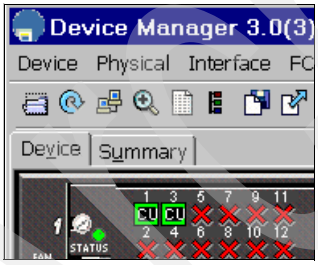


Figure 56 CUs online

Traditional open systems zoning can be done, but it is unnecessary because open systems and FICON traffic can be separated by VSAN. In our case we are not using zoning, so we will not show zoning.

Figure 57 is a display of the switches that are part of the FICON cascaded VSAN.

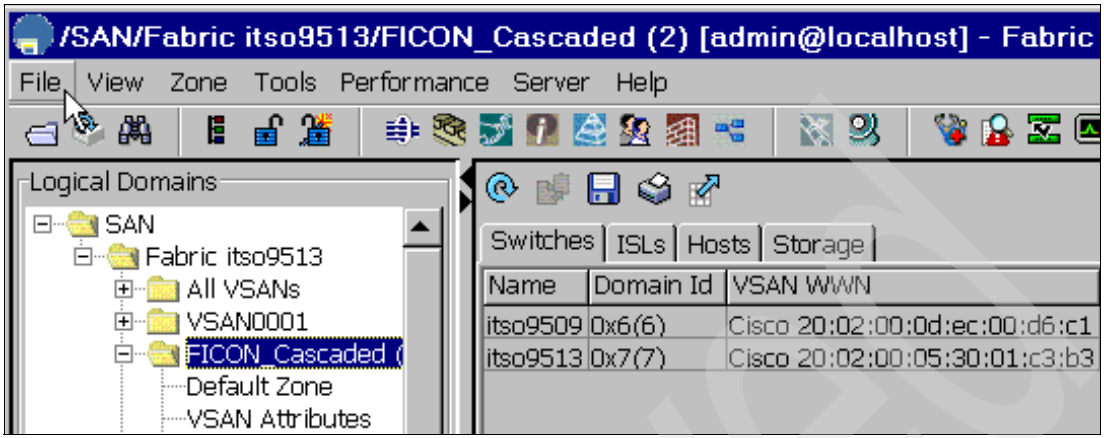


Figure 57 FM display of the switches in FICON VSAN 2

Figure 58 shows summary information of the PortChannel defined between the 9509 and the 9513.

Figure 58 FM display of the PortChannel in VSAN 2

DM is used to manage an individual switch and FM is used to manage the fabric. Figure 59 shows how to select the FICON Interface information.

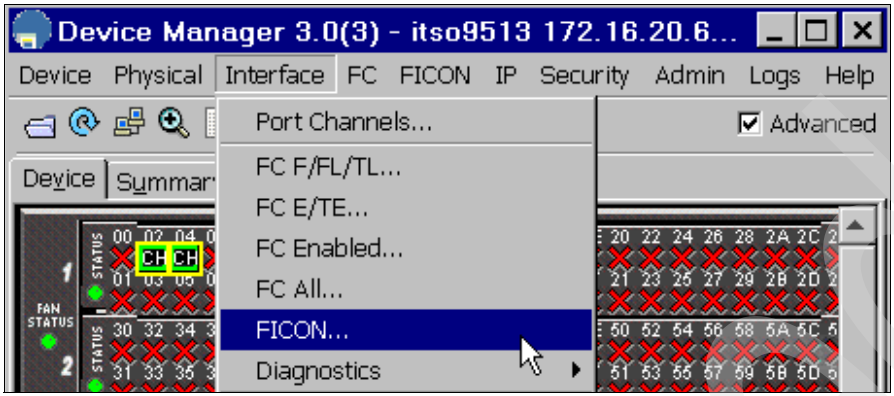


Figure 59 DM display showing both CH and CU ports online

Next, we look at the FICON interface information for this 9513.

Figure 60 shows the operational settings of the FICON ports.

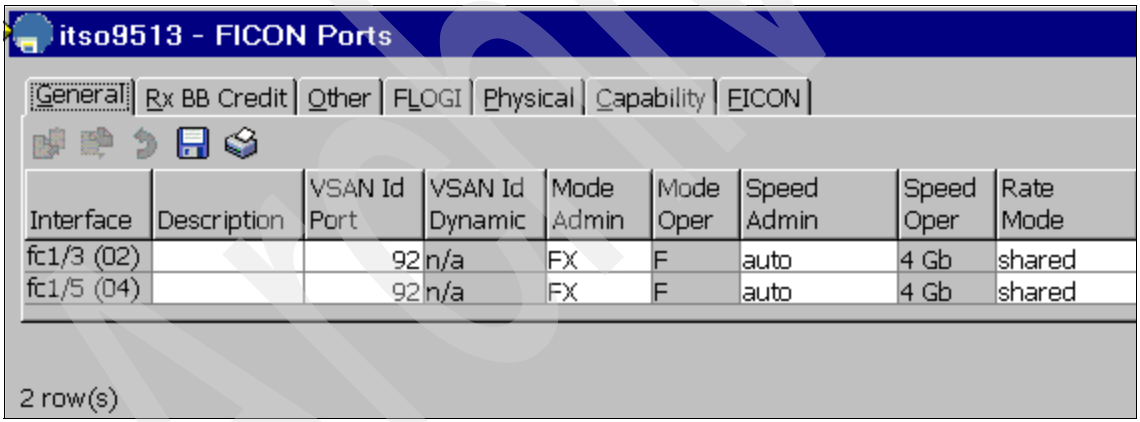


Figure 60 DM display of FICON general information

Figure 61 on page 51 displays the buffer-to-buffer (BB) credit information for the channel and control unit ports on the 9513.

The current RX BB Credit tab shows the amount of frames the device can send to the switch without waiting for an R_RDY from the switch to replenish the BB credit. The TX value is the amount of frames the switch can send to the device without waiting for an R_RDY from the device. The amount of RX BB Credit can be modified, based on the mode in which the port is operating. If the port is

operating as an F_Port, the AdminFx value can be modified. If the port is operating as an E_Port or TE_Port, the AdminISL value can be modified. To globally change the value regardless of the mode in which the port is operating, the Admin value can be modified.

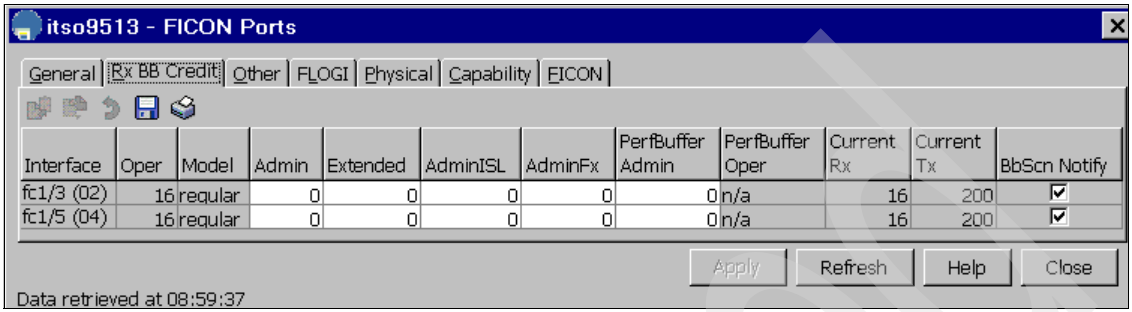


Figure 61 DM display of FICON BB credit information

Figure 62 provides the Mtu and WWN (Fabric World Wide Name [fWWN]) information for each interface. The Fabric WWN is the World Wide Name of the switch port itself.

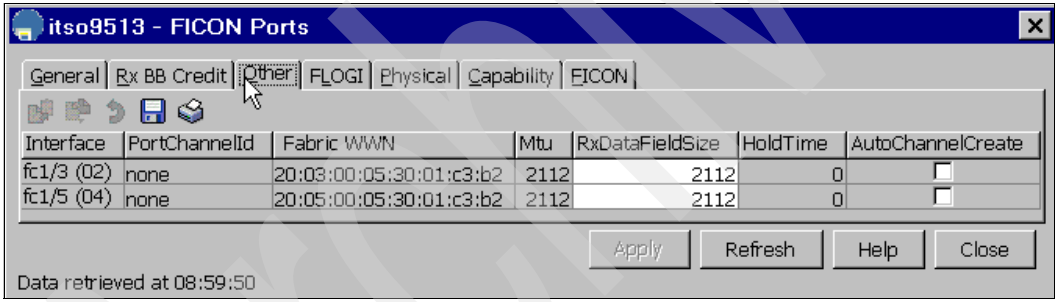


Figure 62 DM display FICON port information

Figure 63 shows the FICON-specific FLOGI information for just this switch. This includes the negotiated buffer-to-buffer credits and class of service (CoS) capability.

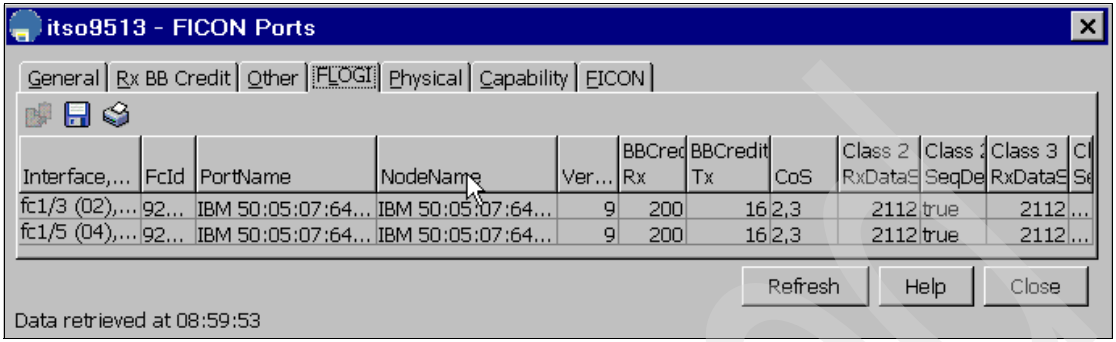


Figure 63 DM display of FICON FLOGI database for the 9506

Figure 64 displays the port physical information.

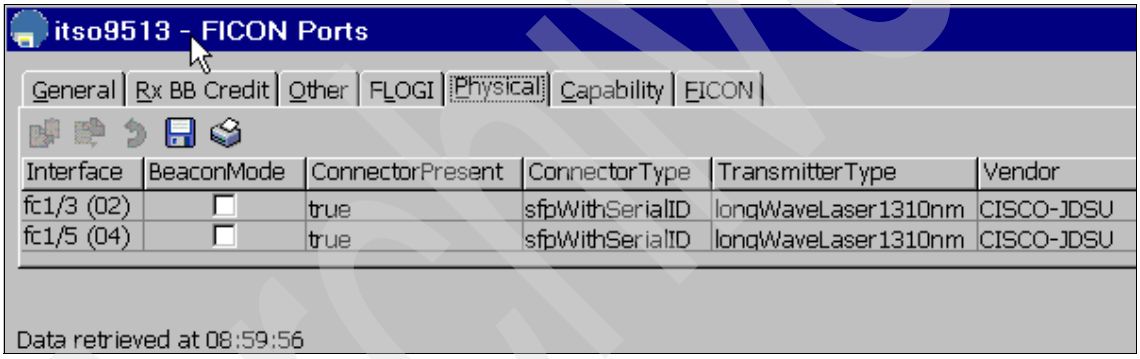


Figure 64 DM display of physical port attributes for the FICON ports

Figure 65 indicates the Fibre Channel attributes that the switch port is capable of supporting. For example, from this display we can discern that the switch can support either class F, 2, or 3 types of service for connections to this port.

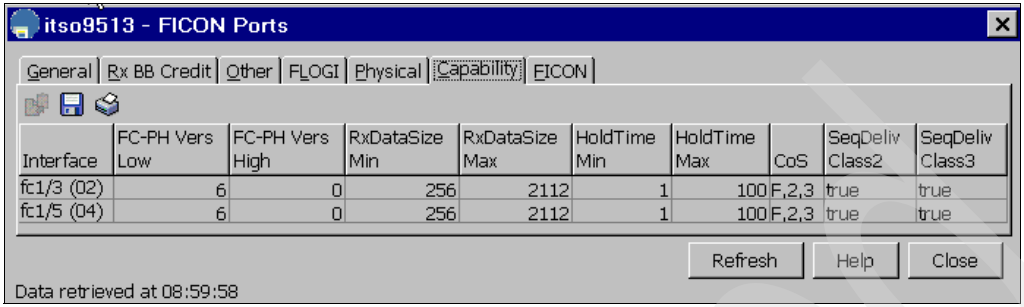


Figure 65 DM display of capability for the FICON ports

Figure 66 displays the Request Node Identification Data (RNID) for the attached device.

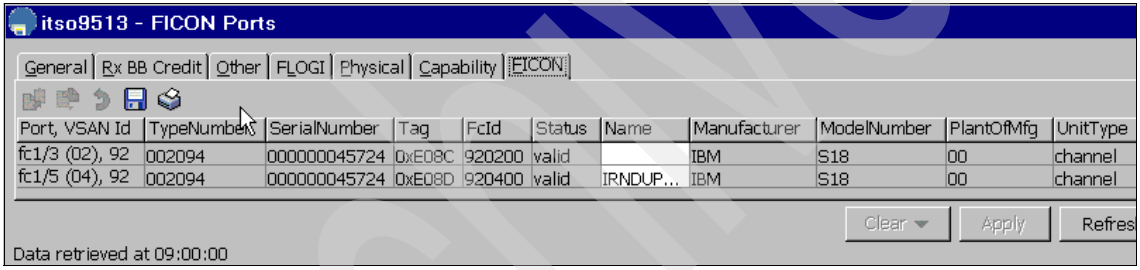


Figure 66 DM display of FICON RNID information

Select **FC** → **Name Server** (Figure 67) to display the global name server.

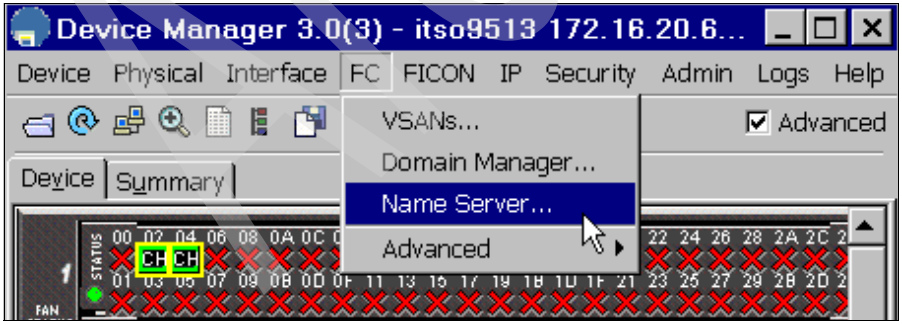
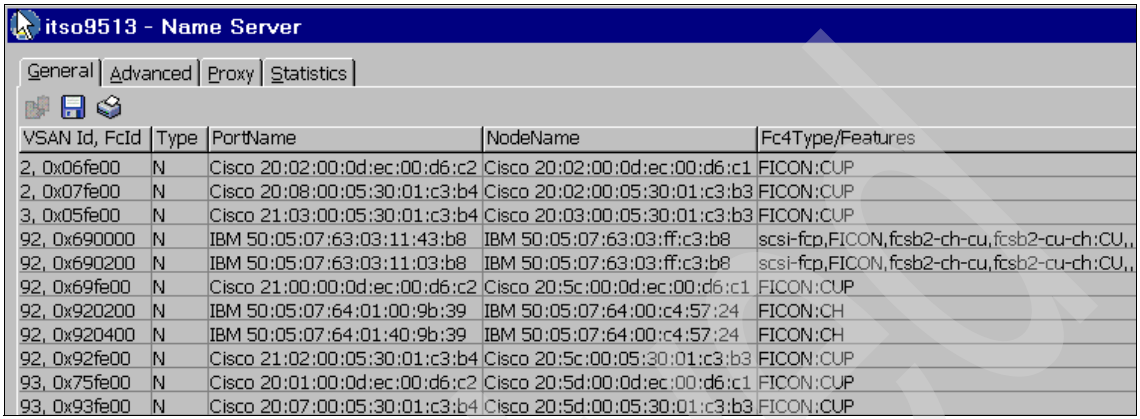


Figure 67 Path to DM display of name server information

Figure 68 show the global name server information. There are several interesting pieces of information in this display. For example, notice that the devices with FcID 0x690000 and 0x690200 have registered for both FICON (fcsb2) and Open Systems (scsi-fcp) support in the FC4Type/Features column.



VSAN Id, FcId	Type	PortName	NodeName	Fc4Type/Features
2, 0x06fe00	N	Cisco 20:02:00:0d:ec:00:d6:c2	Cisco 20:02:00:0d:ec:00:d6:c1	FICON:CUP
2, 0x07fe00	N	Cisco 20:08:00:05:30:01:c3:b4	Cisco 20:02:00:05:30:01:c3:b3	FICON:CUP
3, 0x05fe00	N	Cisco 21:03:00:05:30:01:c3:b4	Cisco 20:03:00:05:30:01:c3:b3	FICON:CUP
92, 0x690000	N	IBM 50:05:07:63:03:11:43:b8	IBM 50:05:07:63:03:ff:c3:b8	scsi-fcp,FICON,fcsb2-ch-cu,fcsb2-cu-ch:CU,,
92, 0x690200	N	IBM 50:05:07:63:03:11:03:b8	IBM 50:05:07:63:03:ff:c3:b8	scsi-fcp,FICON,fcsb2-ch-cu,fcsb2-cu-ch:CU,,
92, 0x69fe00	N	Cisco 21:00:00:0d:ec:00:d6:c2	Cisco 20:5c:00:0d:ec:00:d6:c1	FICON:CUP
92, 0x920200	N	IBM 50:05:07:64:01:00:9b:39	IBM 50:05:07:64:00:c4:57:24	FICON:CH
92, 0x920400	N	IBM 50:05:07:64:01:40:9b:39	IBM 50:05:07:64:00:c4:57:24	FICON:CH
92, 0x92fe00	N	Cisco 21:02:00:05:30:01:c3:b4	Cisco 20:5c:00:05:30:01:c3:b3	FICON:CUP
93, 0x75fe00	N	Cisco 20:01:00:0d:ec:00:d6:c2	Cisco 20:5d:00:0d:ec:00:d6:c1	FICON:CUP
93, 0x93fe00	N	Cisco 20:07:00:05:30:01:c3:b4	Cisco 20:5d:00:05:30:01:c3:b3	FICON:CUP

Figure 68 DM display of name server information

FICON configuration files

When the FICON feature on a VSAN is enabled, an *IPL file* is created automatically with a default configuration. The IPL file contains port configuration information about each FICON port with regard to what other FICON ports are allowed to communicate with this port (*prohibit* function), whether this port is completely isolated from other FICON ports (*block* function), and the description or name of this FICON port. This information is not stored in the startup-config or running-config of the switch as other configuration information is. This file was designed to work specifically with the CUP feature, but it can also be managed from the CLI, FM and DM as shown in Figure 69 on page 55.

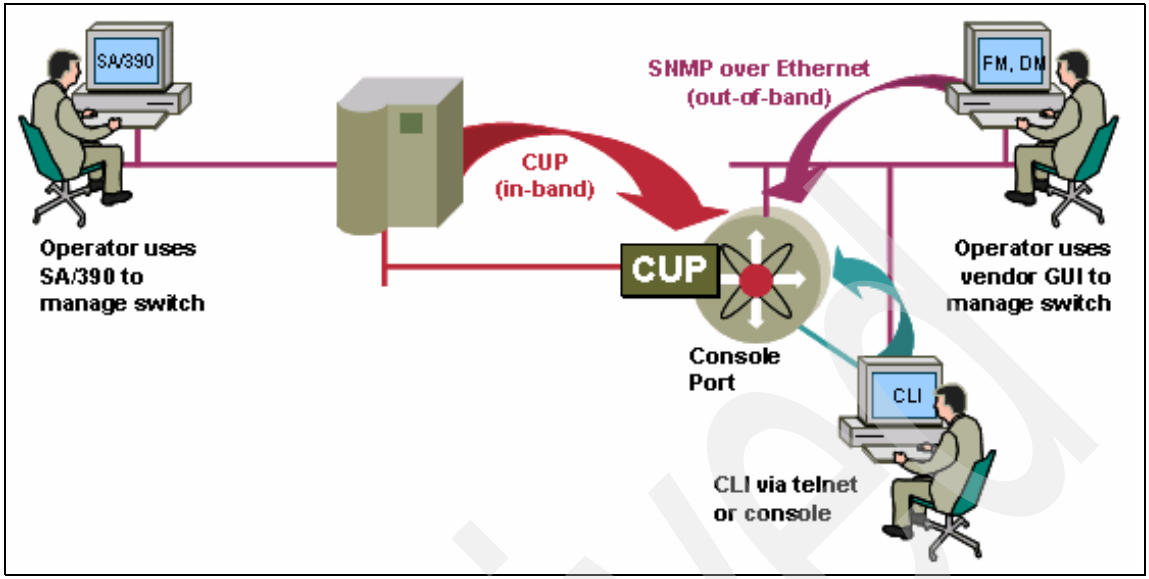


Figure 69 Managing FICON configuration files

You can save up to 16 FICON configuration files on each FICON VSAN. The files are in EBCDIC format and are saved in persistent storage, so they will survive a reload of the switch. FICON configuration files are maintained for each FICON VSAN and the names need only be unique per FICON VSAN instance. For example, you can have a configuration file called `test` for both FICON VSAN 5 and 10. In addition to the port configuration attributes we described earlier, the following additional information is also stored in the FICON configuration file:

- Configure automatic saving of the FICON configuration
- FICON configuration for code page on this VSAN
- Configuration of the last byte of the FCID
- Enable host SA/390 control of the FICON VSAN
- Enable SNMP (FM/DM) control of this FICON VSAN

These additional configuration settings can be viewed and modified using FM by opening the FICON VSAN that you want to view or modify, and selecting **FICON** from the list (Figure 70 on page 56).

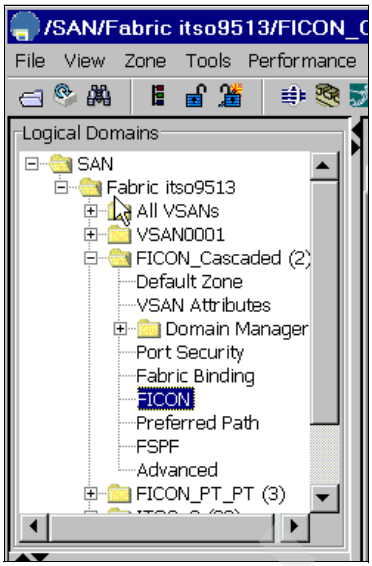


Figure 70 Viewing FICON IPL file

Four tabs are available. Figure 71 shows the information displayed on the Control tab.

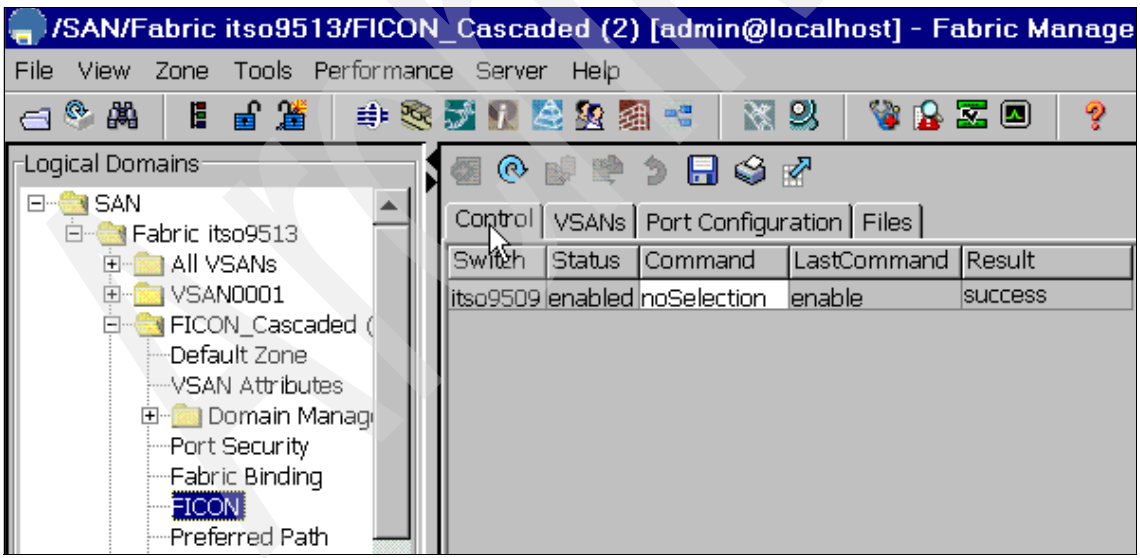


Figure 71 Control tab

Figure 72 and Figure 73 show the parameters on the VSAN tab.

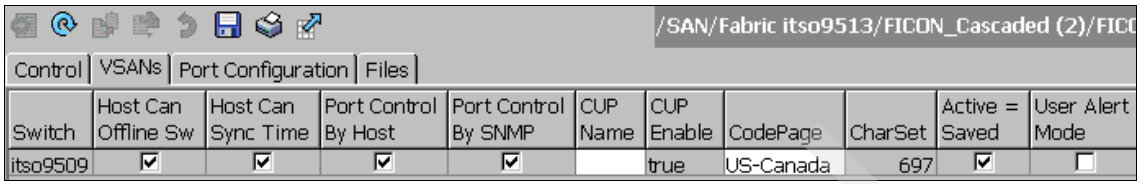


Figure 72 VSAN attributes

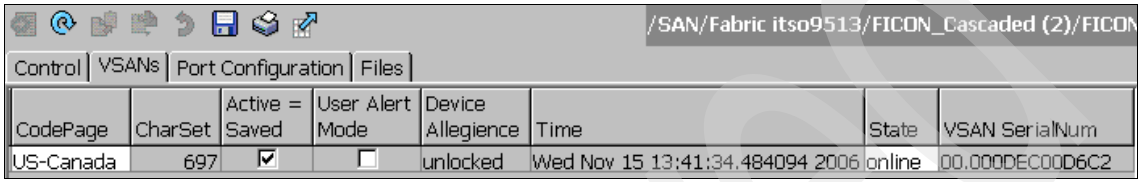


Figure 73 VSAN attributes continued

You can toggle any of the IPL file attributes on or off, then select the **Apply Changes** icon to make changes to the active configuration. These changes are also saved into the IPL file immediately based on the default Active=Saved feature.

Active=Saved If this feature is off, changes are written *only* when you copy the switch's running configuration to the startup configuration. All other FICON configuration information that is not contained in the IPL file is saved only after the running configuration has been copied to the startup configuration.

Port Control By Host If enabled, the SA/390 administrator can block, prohibit, or name ports. If not, the port configuration can be viewed but not modified.

Host Can Offline Sw If enabled, the SA/390 administrator user can take the VSAN offline and cause all ports in this VSAN to transmit the OLS primitive sequence.

Host Can Sync Time If enabled, the SA/390 administrator can sync the host and switch time for troubleshooting purposes.

Tip: Setting the switch time zone can be done with the CLI **`clock timezone`** configuration command.

Port Control By SNMP The switch can also be configured to permit or deny an SNMP (FM/DM) user from modifying IPL file attributes. If the SNMP check box is toggled off, an FM/DM user cannot change any port attributes or any other setting that is stored in the FICON config files. FM/DM users could still view the status of the FICON VSAN.

Note: When the SNMP box is unchecked, it can be re-enabled only via the CLI.

Device Allegiance Refers to the mechanism whereby the IPL file is locked in order to avoid concurrent updates from multiple sources. Remember, this file can be modified via SNMP, SA/390, and the CLI. This panel indicates whether the file is locked or unlocked and, if locked, which device has the lock.

CodePage The FICON CodePage can also be modified here if necessary.

Using DM to prohibit and block ports

As mentioned previously, SNMP (DM) can be used to manage FICON configuration files, and as such can be used to prohibit, block, and swap ports. Before you make any changes to the FICON IPL configuration file, first make a backup copy of this file:

1. Select **FICON** → **VSANs** (Figure 74).

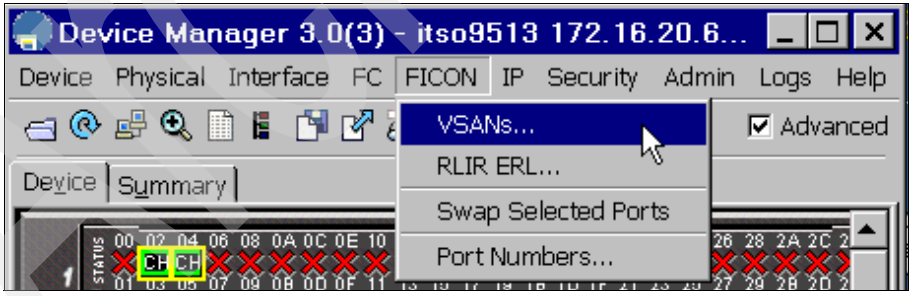


Figure 74 Accessing FICON configuration files

2. Click the **Files** tab (Figure 75).

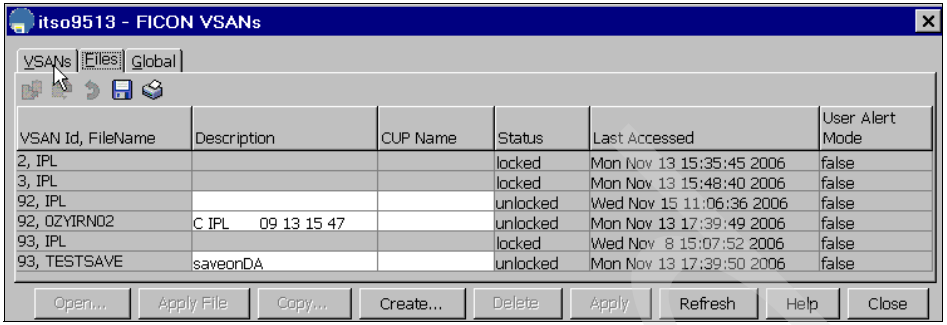


Figure 75 Accessing FICON configuration files panel 2

You *might* see only one configuration file, the IPL file, and if the Active=Saved feature is enabled this file will be locked and it cannot be opened.

3. To make a copy of this file for backup purposes, select the IPL file you want to copy, select **Copy**, enter the name of the new file, and click **OK** (Figure 76).

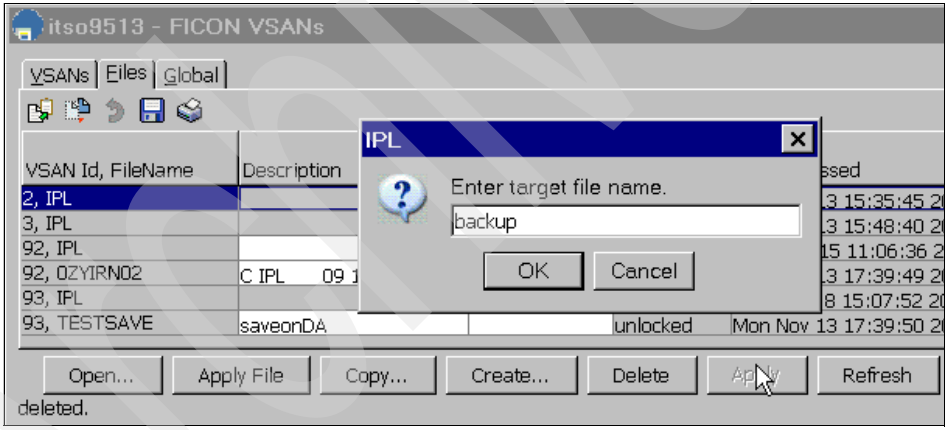


Figure 76 Creating a copy of the IPL configuration file

This create the new file (called `backup` in our example) shown in Figure 77.

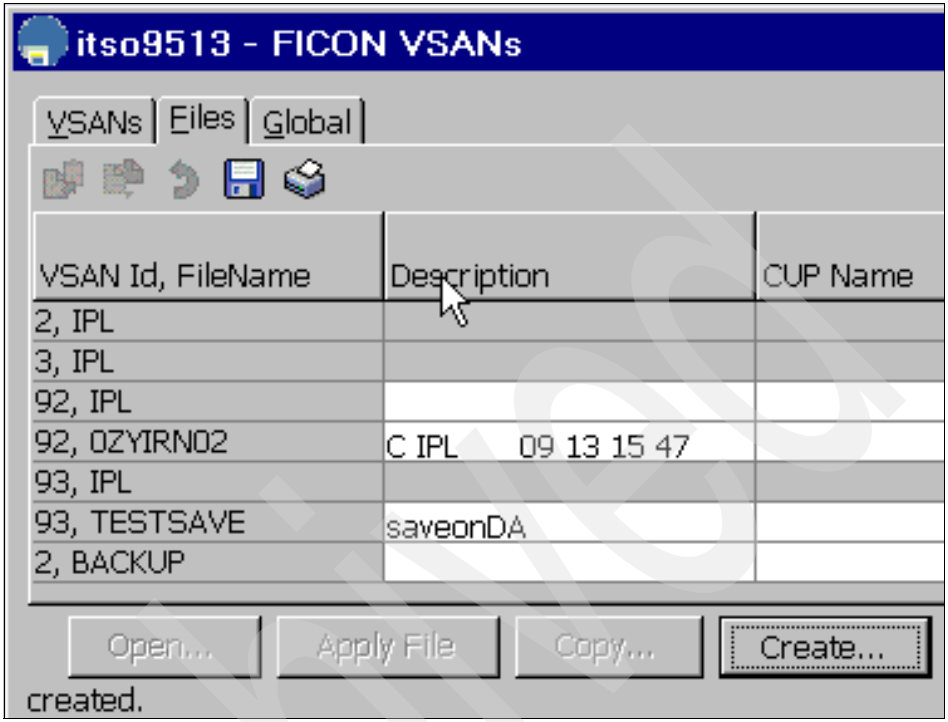


Figure 77 Newly created backup FICON configuration file

With a backup of the configuration file created (`2, BACKUP`), we can make changes directly to the IPL file. Select the FICON VSAN to modify, then click **Port Configuration** (Figure 78).

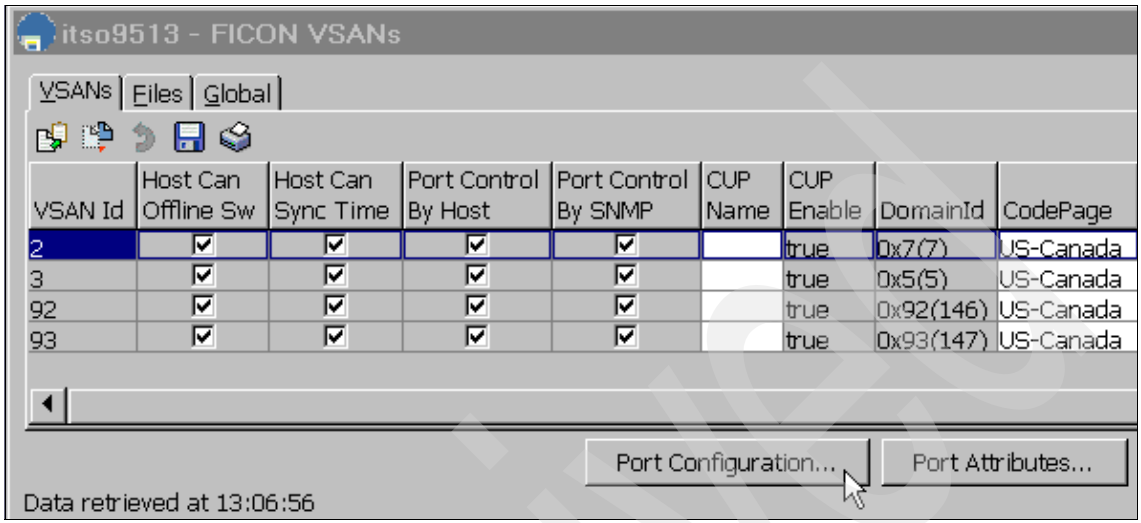


Figure 78 Modifying IPL port attributes

At this point blocking and prohibiting ports is intuitive and can be accomplished by simply toggling on and off the column boxes for the desired ports. The example in Figure 79 shows port 2 blocked from all communication, port 1 prevented from communicating with port 3, and the name `Production` assigned to port 4. If the cursor is moved over a row and column, the intersecting port addresses are displayed (01/03). Clicking once in the port enters a red `X` and automatically selects the corresponding row/port (03/01).

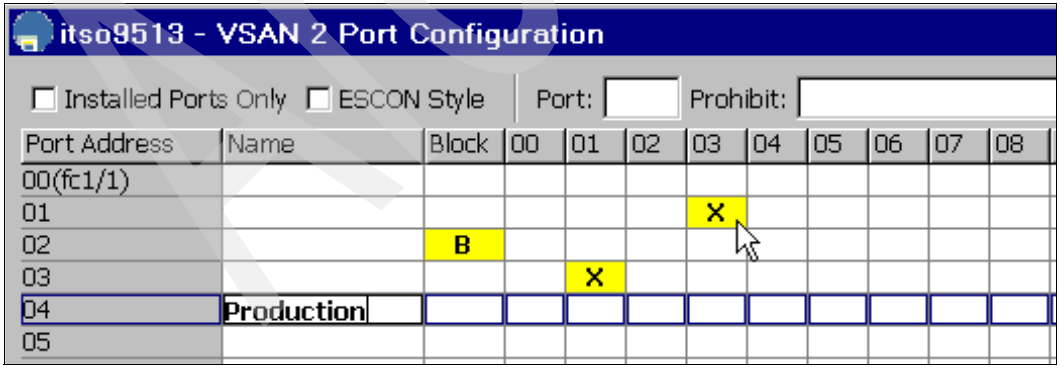


Figure 79 Prohibiting, blocking, and naming FICON ports

Tip: To view the available and prohibited ESCON® style ports, select the ESCON Style box.

Finally, apply the changes. Verify the changes by reopening the VSAN 2 Port Configuration panel as shown in Figure 80.

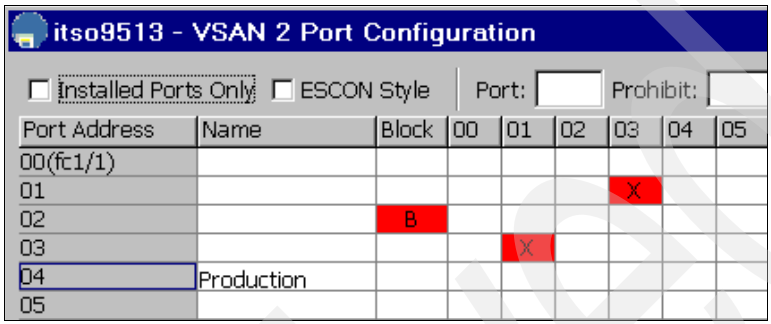


Figure 80 Verifying FICON port attribute changes

Using DM to swap ports

If there is a problem with a particular port, a feature called *port swap* can be used to move the FICON port address of one interface to a different Fibre Channel interface that resides in the same switch. This temporarily circumvents the need to make HCD changes on the host. Remember that the port number of FICON CUs is defined in the LINK parameter on the CNTLUNIT macro in IOCDS. Our goal is to swap the FICON port address for the CU on interface FC1/3 with interface FC1/5. Both the source and destination ports must be FICON ports (that is, both ports must be members of the FICON VSAN).

First, verify the current port addresses of the interfaces by selecting **FICON** → **VSANs**. Select **VSAN 92**, click **Port Attributes**, and click the **FICON** tab (Figure 81). Notice the FCIDs 920200 and 920400.

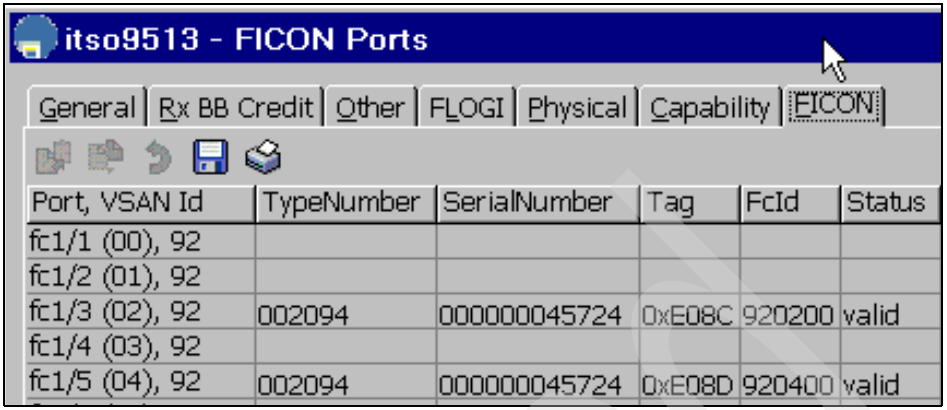


Figure 81 Viewing FICON port attributes

At this point the physical cabling swap for interfaces fc1/3 and fc1/5 (ports 02 and 04 in our display) is complete. We now port swap interfaces fc1/3 (02) with fc1/5(04) in DM:

1. Click fc1/3 (02), hold down the CTRL key and click fc1/5(04).
2. Select **FICON** → **Swap Selected Ports** (Figure 82).

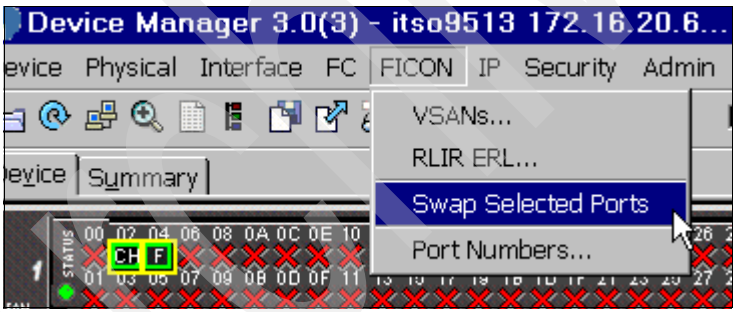


Figure 82 Swapping selected ports

3. At the advisory that this might be disruptive (Figure 83), click **Yes**.

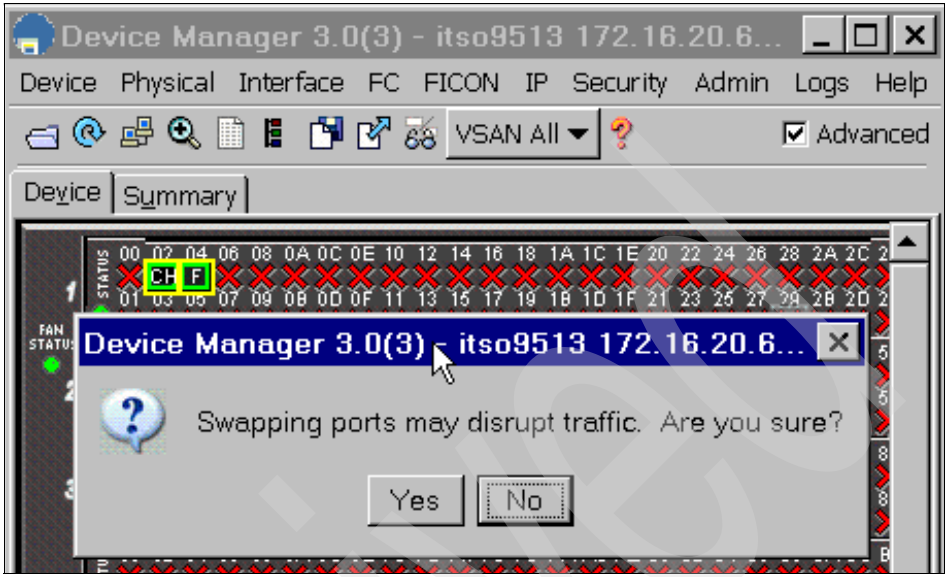


Figure 83 Warning message

4. Click **OK** to the swap success message (Figure 84).

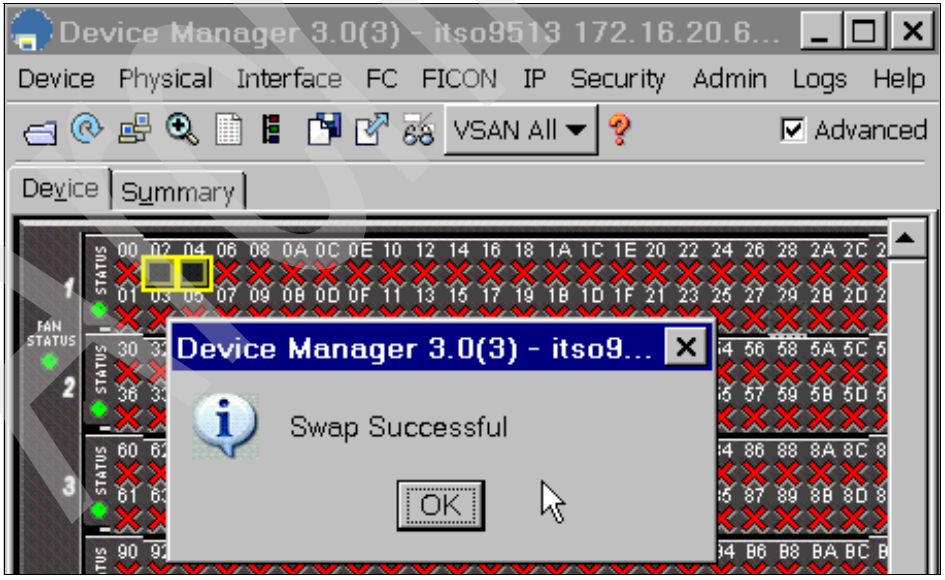


Figure 84 Port swap successful message

5. When prompted to enable the ports (Figure 85), we selected **Yes** because we have already moved the required cables.

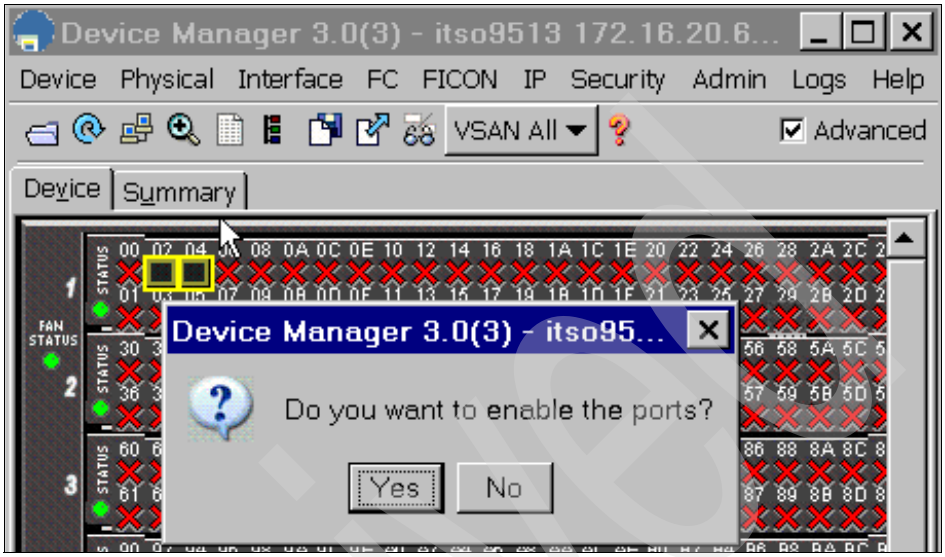
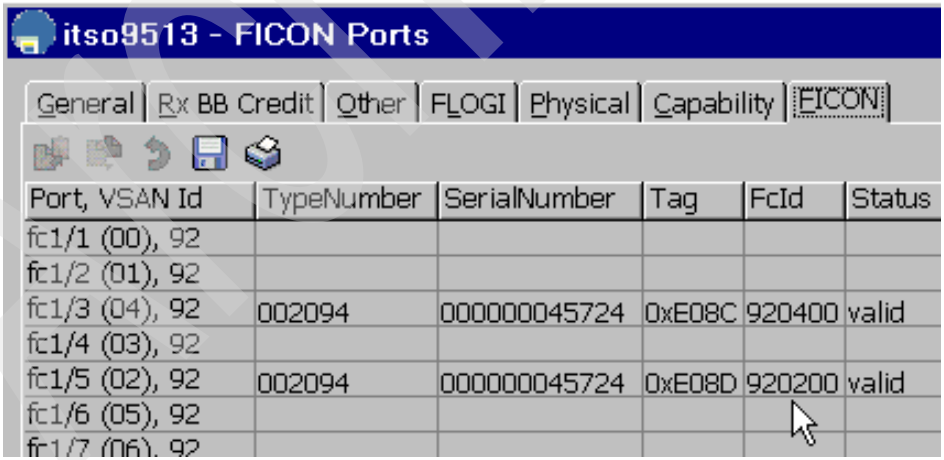


Figure 85 Port swap enable ports message

We can verify that the port address was swapped as shown in Figure 86. Notice how the FCIDs have changed when compared to Figure 81 on page 63.



Port, VSAN Id	TypeNumber	SerialNumber	Tag	FcId	Status
fc1/1 (00), 92					
fc1/2 (01), 92					
fc1/3 (04), 92	002094	000000045724	0xE08C	920400	valid
fc1/4 (03), 92					
fc1/5 (02), 92	002094	000000045724	0xE08D	920200	valid
fc1/6 (05), 92					
fc1/7 (06), 92					

Figure 86 FICON port attribute display after the port swap

This completes our FICON basic configuration.

The team that wrote this paper

This paper was produced at the International Technical Support Organization, Austin Center.

Jon Tate is a Project Manager for IBM System Storage™ SAN Solutions at the International Technical Support Organization, Austin Center. Before joining the ITSO in 1999, he worked in the IBM Technical Support Center, providing Level 2 support for IBM storage products. Jon has 22 years of experience in storage software and management, services, and support. He is both an IBM Certified IT Specialist and an IBM SAN Certified Specialist, and is also the UK Chairman of the Storage Networking Industry Association (SNIA).

Thanks to the following people for their contributions to this project:

Tom Cady
Emma Jacobs
Leslie Parham
Deanna Polm
Sangam Racherla
Bill Trimble
Sokkieng Wang
International Technical Support Organization

Marci Nagel
IBM Storage Systems Group

Brent Anderson
John McKibben
Paul Raytick
Cisco Systems

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

This document REDP-4392-00 was created or updated on April 17, 2008.

Send us your comments in one of the following ways:
- Use the online **Contact us** review Redbooks form found at:
  ibm.com/redbooks
- Send your comments in an e-mail to:
  redbook@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099, 2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

Redbooks (logo) ®	FICON®	OS/390®
z/OS®	IBM®	System Storage™
ESCON®	MVS™	

Other company, product, or service names may be trademarks or service marks of others.