CHAPTER 2

Configuring FCIP

Cisco MDS 9000 Family IP storage (IPS) services extend the reach of Fibre Channel SANs by using open-standard, IP-based technology. The switch can connect separated SAN islands using Fibre Channel over IP (FCIP).

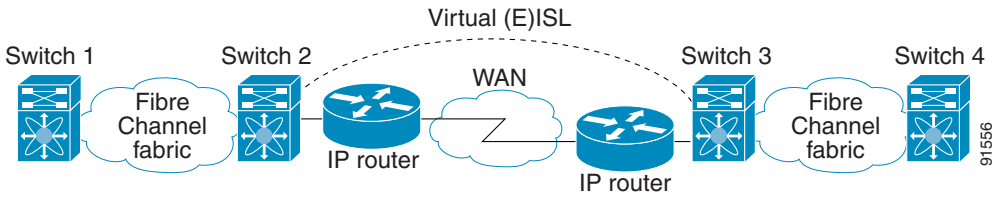
Note FCIP is supported on the MDS 9222i switch, MSM-18/4 module, MDS 9216i switch, MPS-14/2 module, 16-Port Storage Services Node (SSN-16), and IPS modules on MDS 9200 Series directors.

This chapter includes the following topics:

Information About FCIP

The Fibre Channel over IP Protocol (FCIP) is a tunneling protocol that connects geographically distributed Fibre Channel storage area networks (SAN islands) transparently over IP local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs). The switch can connect separated SAN islands using Fibre Channel over IP (FCIP) (see Figure 2-1).

Figure 2-1 Fibre Channel SANs Connected by FCIP



FCIP uses TCP as a network layer transport. The DF bit is set in the TCP header.

Note For more information about FCIP protocols, refer to the IETF standards for IP storage at http://www.ietf.org. Also refer to Fibre Channel standards for switch backbone connection at http://www.t11.org (see FC-BB-2).

This section includes the following topics:

FCIP Concepts

To configure IPS modules or MPS-14/2 modules for FCIP, you should have a basic understanding of the following concepts:

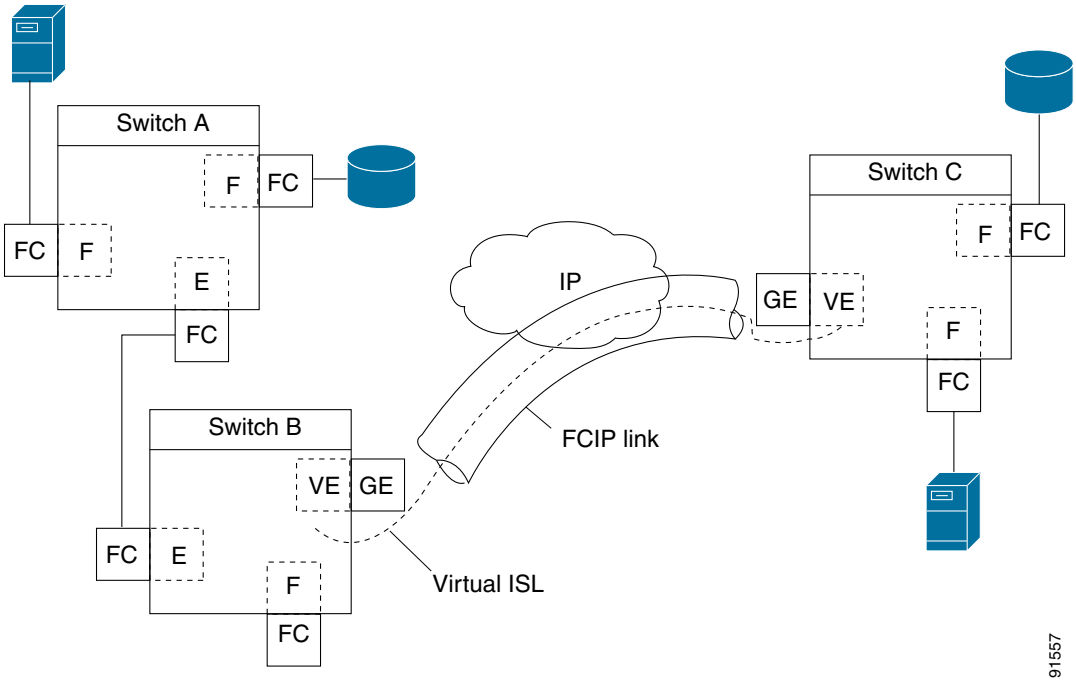
FCIP and VE Ports

Figure 2-2 describes the internal model of FCIP with respect to Fibre Channel Inter-Switch Links (ISLs) and Cisco's extended ISLs (EISLs).

FCIP virtual E (VE) ports behave exactly like standard Fibre Channel E ports, except that the transport in this case is FCIP instead of Fibre Channel. The only requirement is for the other end of the VE port to be another VE port.

A virtual ISL is established over an FCIP link and transports Fibre Channel traffic. Each associated virtual ISL looks like a Fibre Channel ISL with either an E port or a TE port at each end (see Figure 2-2).

Figure 2-2 FCIP Links and Virtual ISLs



See the "Configuring B Ports" section on page 2-28 for more information.

FCIP Links

FCIP links consist of one or more TCP connections between two FCIP link endpoints. Each link carries encapsulated Fibre Channel frames.

When the FCIP link comes up, the VE ports at both ends of the FCIP link create a virtual Fibre Channel (E)ISL and initiate the E port protocol to bring up the (E)ISL.

By default, the FCIP feature on any Cisco MDS 9000 Family switch creates two TCP connections for each FCIP link:

- One connection is used for data frames.
- The other connection is used only for Fibre Channel control frames, that is, switch-to-switch protocol frames (all Class F). This arrangement provides low latency for all control frames.

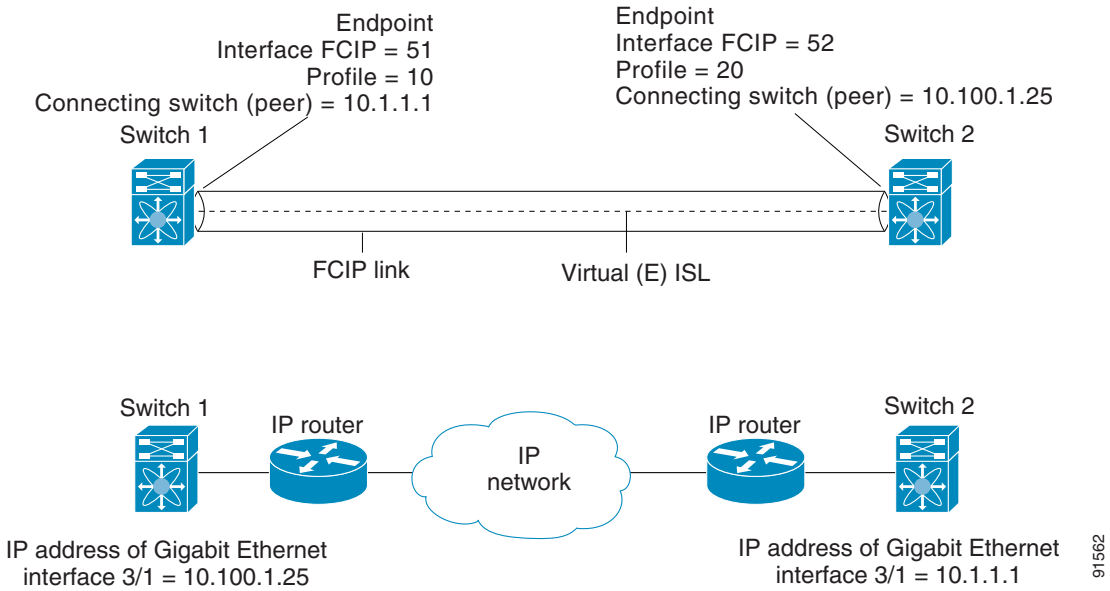
To enable FCIP on the IPS module or MPS-14/2 module, an FCIP profile and FCIP interface (interface FCIP) must be configured.

The FCIP link is established between two peers, the VE port initialization behavior is identical to a normal E port. This behavior is independent of the link being FCIP or pure Fibre Channel, and is based on the E port discovery process (ELP, ESC).

Once the FCIP link is established, the VE port behavior is identical to E port behavior for all inter-switch communication (including domain management, zones, and VSANs). At the Fibre Channel layer, all VE and E port operations are identical.

When two FCIP link endpoints are created, an FCIP link is established between the two IPS modules or MPS-14/2 modules. To create an FCIP link, assign a profile to the FCIP interface and configure the peer information. The peer IP switch information initiates (creates) an FCIP link to that peer switch (see Figure 2-3).

Figure 2-3 Assigning Profiles to Each Gigabit Ethernet Interface



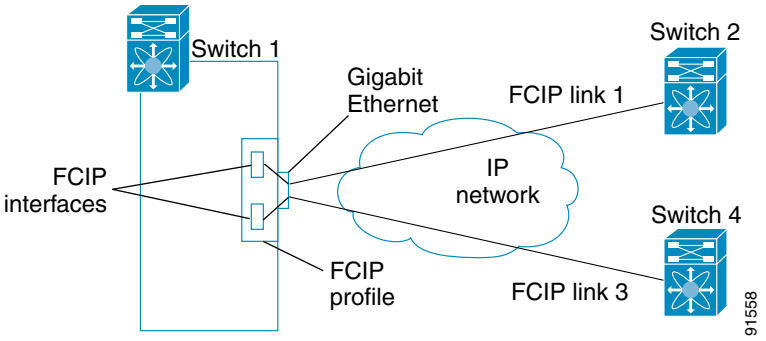
FCIP Profiles

The FCIP profile contains information about the local IP address and TCP parameters. The profile defines the following information:

- The local connection points (IP address and TCP port number)
- The behavior of the underlying TCP connections for all FCIP links that use this profile

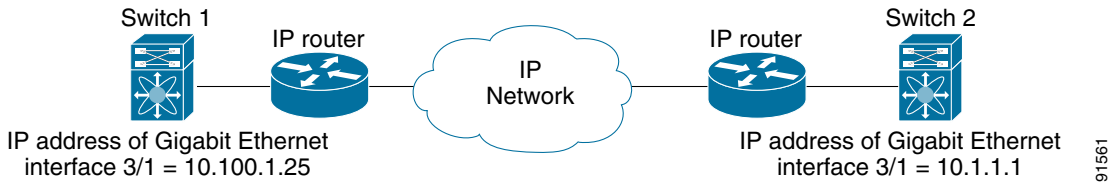
The FCIP profile's local IP address determines the Gigabit Ethernet port where the FCIP links terminate (see Figure 2-4).

Figure 2-4 FCIP Profile and FCIP Links



You must assign a local IP address of a Gigabit Ethernet interface or subinterface to the FCIP profile to create an FCIP profile. You can assign IPv4 or IPv6 addresses to the interfaces. Figure 2-5 shows an example configuration.

Figure 2-5 Assigning Profiles to Each Gigabit Ethernet Interface



FCIP Interfaces

The FCIP interface is the local endpoint of the FCIP link and a VE port interface. All the FCIP and E port parameters are configured in context to the FCIP interface.

The FCIP parameters consist of the following:

- The FCIP profile determines which Gigabit Ethernet port initiates the FCIP links and defines the TCP connection behavior.
- Peer information.
- Number of TCP connections for the FCIP link.
- E port parameters—trunking mode and trunk allowed VSAN list.

FCIP High-Availability Solutions

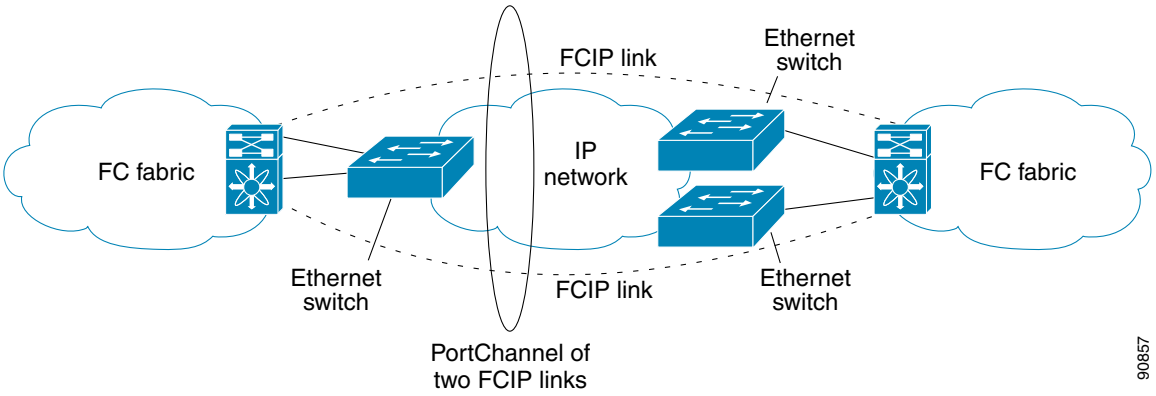
The following high-availability solutions are available for FCIP configurations:

- Fibre Channel PortChannels, page 2-5
- FSPF, page 2-6
- VRRP, page 2-7
- Ethernet PortChannels, page 2-7

Fibre Channel PortChannels

Figure 2-6 provides an example of a PortChannel-based load-balancing configuration. To perform this configuration, you need two IP addresses on each SAN island. This solution addresses link failures.

Figure 2-6 PortChannel-Based Load Balancing



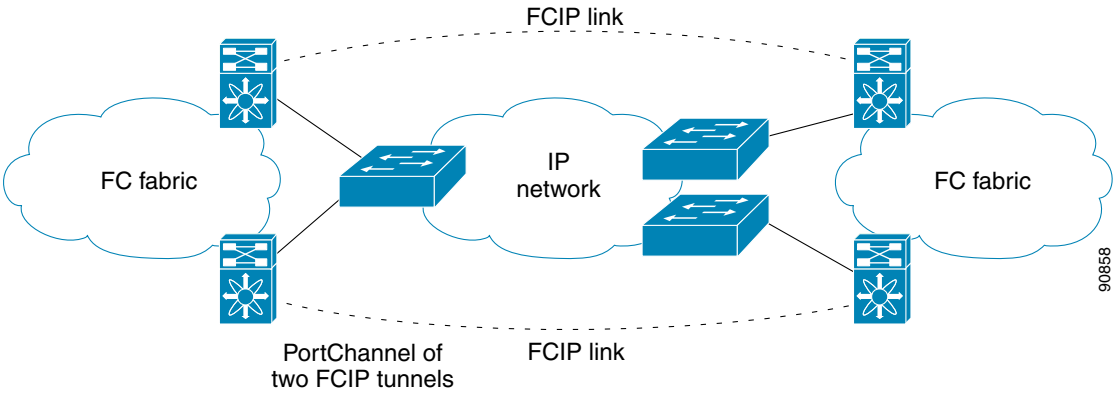
The following characteristics set Fibre Channel PortChannel solutions apart from other solutions:

- The entire bundle is one logical (E)ISL link.
- All FCIP links in the PortChannel should be across the same two switches.
- The Fibre Channel traffic is load balanced across the FCIP links in the PortChannel.

FSPF

Figure 2-7 displays a FPSF-based load balancing configuration example. This configuration requires two IP addresses on each SAN island, and addresses IP and FCIP link failures.

Figure 2-7 FSPF-Based Load Balancing



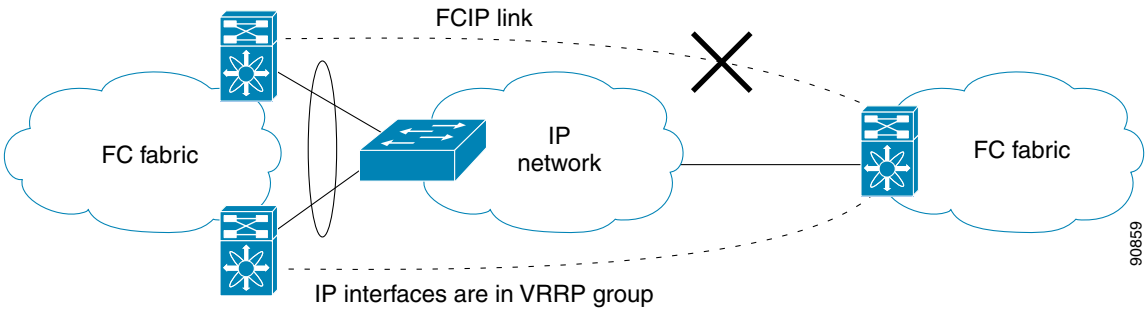
The following characteristics set FSPF solutions apart from other solutions:

- Each FCIP link is a separate (E)ISL.
- The FCIP links can connect to different switches across two SAN islands.
- The Fibre Channel traffic is load balanced across the FCIP link.

VRRP

Figure 2-8 displays a Virtual Router Redundancy Protocol (VRRP)-based high availability FCIP configuration example. This configuration requires at least two physical Gigabit Ethernet ports connected to the Ethernet switch on the island where you need to implement high availability using VRRP.

Figure 2-8 VRRP-Based High Availability



The following characteristics set VRRP solutions apart from other solutions:

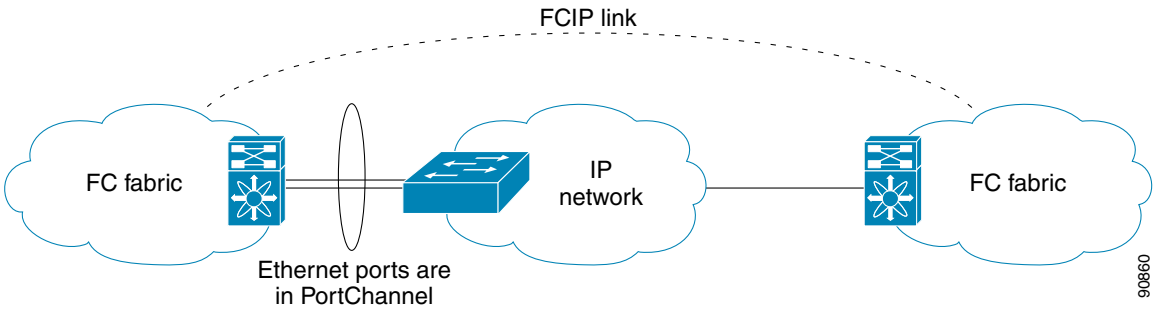
- If the active VRRP port fails, the standby VRRP port takes over the VRRP IP address.
- When the VRRP switchover happens, the FCIP link automatically disconnects and reconnects.
- This configuration has only one FCIP (E)ISL link.

Note Port-fast needs to be enabled in the catalyst/n7k switches where the GigabitEthernet/Mgmt port is connected.

Ethernet PortChannels

Figure 2-9 displays an Ethernet PortChannel-based high-availability FCIP example. This solution addresses the problem caused by individual Gigabit Ethernet link failures.

Figure 2-9 Ethernet PortChannel-Based High Availability



The following characteristics set Ethernet PortChannel solutions apart from other solutions:

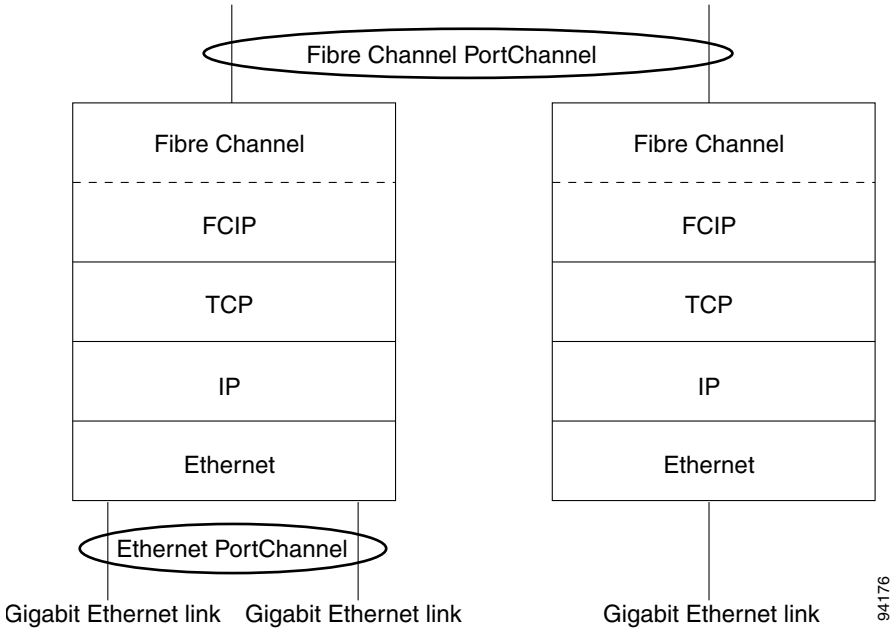
- The Gigabit Ethernet link-level redundancy ensures a transparent failover if one of the Gigabit Ethernet links fails.
- Two Gigabit Ethernet ports in one Ethernet PortChannel appear like one logical Gigabit Ethernet link.
- The FCIP link stays up during the failover.

Ethernet PortChannels and Fibre Channel PortChannels

Ethernet PortChannels offer link redundancy between the Cisco MDS 9000 Family switch's Gigabit Ethernet ports and the connecting Ethernet switch. Fibre Channel PortChannels also offer (E)ISL link redundancy between Fibre Channel switches. FCIP is an (E)ISL link and is only applicable for a Fibre Channel PortChannel. Beneath the FCIP level, an FCIP link can run on top of an Ethernet PortChannel or on one Gigabit Ethernet port. This link is totally transparent to the Fibre Channel layer.

An Ethernet PortChannel restriction only allows two contiguous IPS ports, such as ports 1–2 or 3–4, to be combined in one Ethernet PortChannel (see Chapter 6, "Configuring IP Storage" for more information). This restriction only applies to Ethernet PortChannels. The Fibre Channel PortChannel (to which FCIP link can be a part of) does not have a restriction on which (E)ISL links can be combined in a Fibre Channel PortChannel as long as it passes the compatibility check, The maximum number of Fibre Channel ports that can be put into a Fibre Channel PortChannel is 16 (see Figure 2-10).

Figure 2-10 PortChannels at the Fibre Channel and Ethernet Levels



To configure Fibre Channel PortChannels, see the *Interfaces Configuration Guide, Cisco DCNM for SAN*.

To configure Ethernet PortChannels, see the *High Availability and Redundancy Configuration Guide,Cisco DCNM for SAN*.

FCIP Profile Configuration

A basic FCIP configuration uses the local IP address to configure the FCIP profile. In addition to the local IP address and the local port, you can specify other TCP parameters as part of the FCIP profile configuration.

Peers

All the FCIP and E port parameters are configured in context to the FCIP interface. To create an FCIP link, assign a profile to the FCIP interface and configure the peer information. The peer IP switch information initiates (creates) an FCIP link to that peer switch. The basic FCIP configuration uses the peer's IP address to configure the peer information. You can establish an FCIP link with the peer using the Peer IP address option. This option configures both ends of the FCIP link. Optionally, you can also use the peer TCP port along with the IP address.

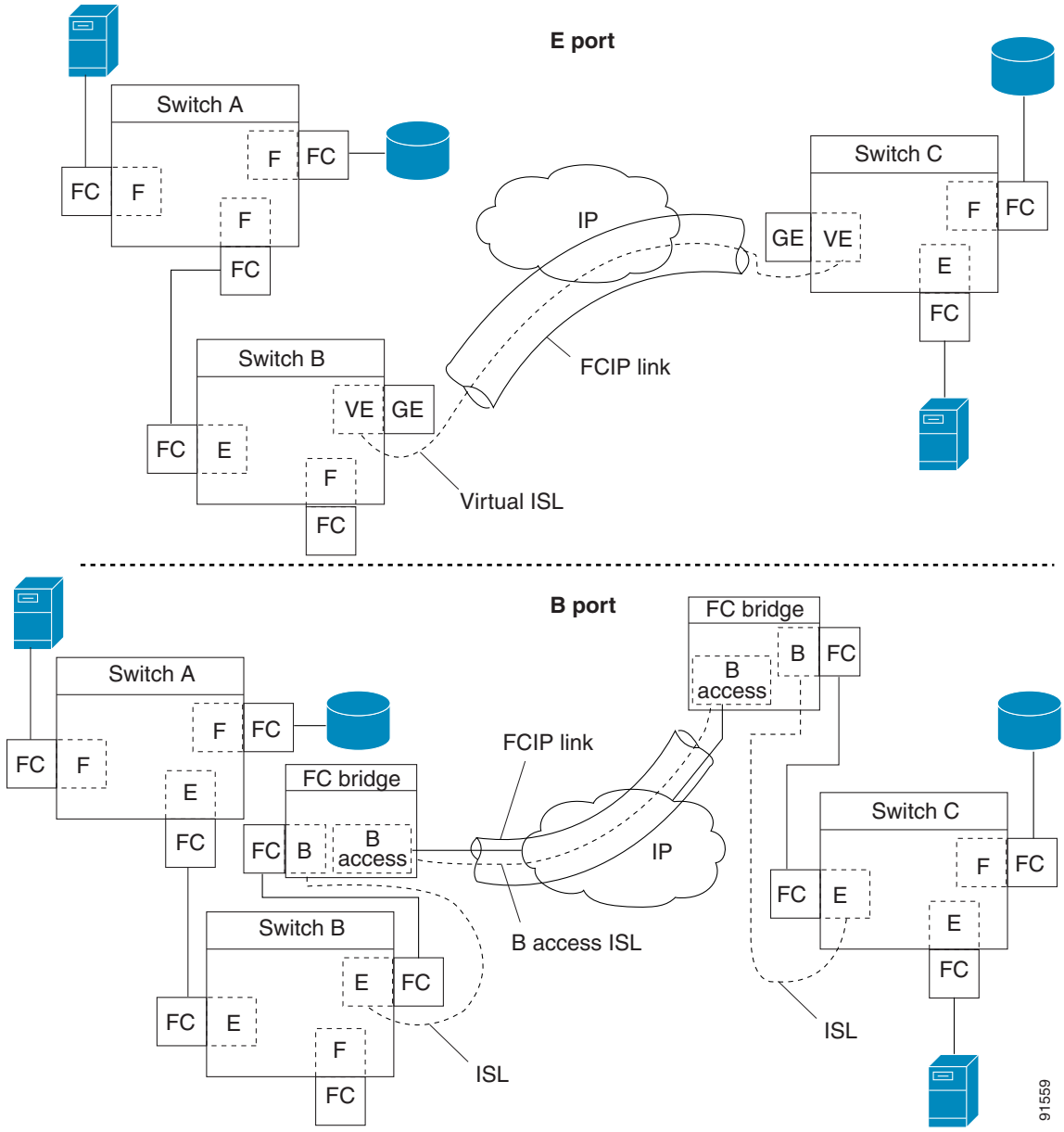
To establish an FCIP link with the peer, you can use the peer IP address option. This option configures both ends of the FCIP link. Optionally, you can also use the peer TCP port along with the IP address.

To establish a peer connection, you must first create the FCIP interface and enter the config-if submode.

FCIP B Port Interoperability Mode

While E ports typically interconnect Fibre Channel switches, some SAN extender devices, such as Cisco's PA-FC-1G Fibre Channel port adapter and the SN 5428-2 storage router, implement a bridge port model to connect geographically dispersed fabrics. This model uses B port as described in the T11 Standard FC-BB-2. Figure 2-11 shows a typical SAN extension over an IP network.

Figure 2-11 FCIP B Port and Fibre Channel E Port

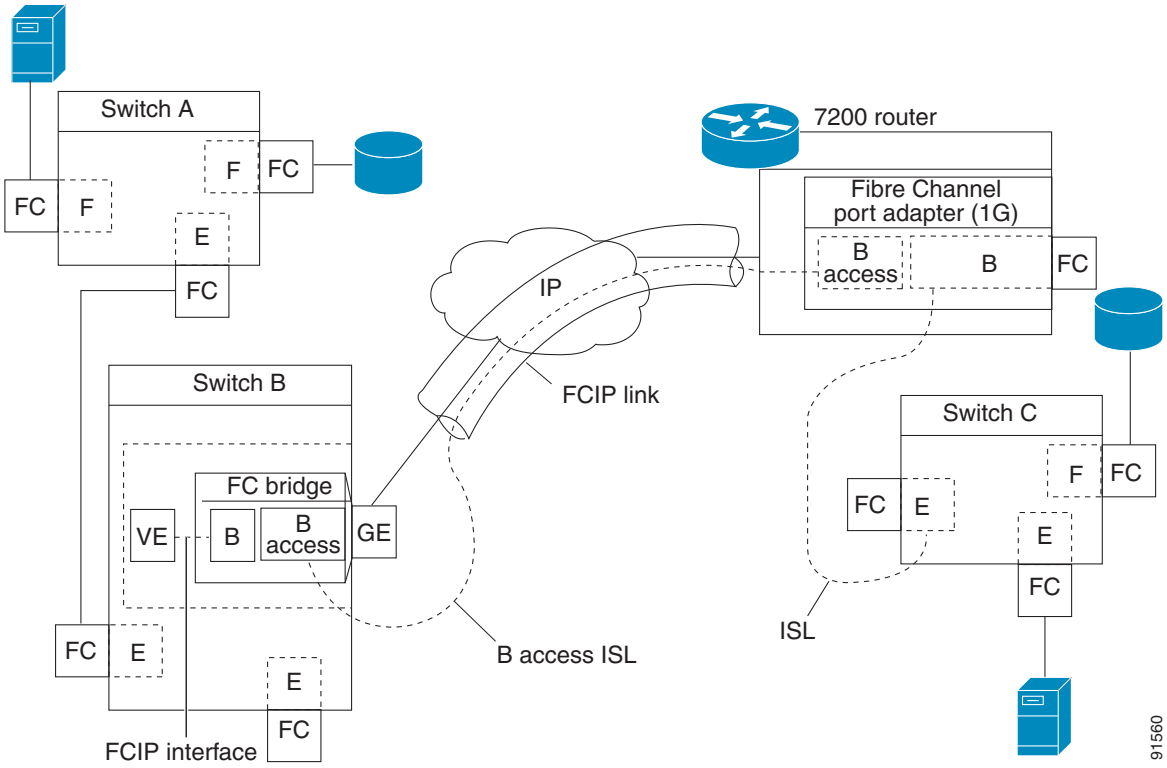


B ports bridge Fibre Channel traffic from a local E port to a remote E port without participating in fabric-related activities such as principal switch election, domain ID assignment, and Fibre Channel fabric shortest path first (FSPF) routing. For example, Class F traffic entering a SAN extender does not interact with the B port. The traffic is transparently propagated (bridged) over a WAN interface before exiting the remote B port. This bridge results in both E ports exchanging Class F information that ultimately leads to normal ISL behavior such as fabric merging and routing.

FCIP links between B port SAN extenders do not exchange the same information as FCIP links between E ports, and are therefore incompatible. This is reflected by the terminology used in FC-BB-2: *while VE ports establish a virtual ISL over an FCIP link, B ports use a B access ISL.*

The IPS module and MPS-14/2 module support FCIP links that originate from a B port SAN extender device by implementing the B access ISL protocol on a Gigabit Ethernet interface. Internally, the corresponding virtual B port connects to a virtual E port that completes the end-to-end E port connectivity requirement (see Figure 2-12).

Figure 2-12 FCIP Link Terminating in a B Port Mode



The B port feature in the IPS module and MPS-14/2 module allows remote B port SAN extenders to communicate directly with a Cisco MDS 9000 Family switch, eliminating the need for local bridge devices.

Quality of Service

The quality of service (QoS) parameter specifies the differentiated services code point (DSCP) value to mark all IP packets (type of service—TOS field in the IP header).

- The control DSCP value applies to all FCIP frames in the control TCP connection.
- The data DSCP value applies to all FCIP frames in the data connection.

If the FCIP link has only one TCP connection, that data DSCP value is applied to all packets in that connection.

E Ports

You can configure E ports in the same way you configure FCIP interfaces. The following features are also available for FCIP interfaces:

- An FCIP interface can be a member of any VSAN
- Trunk mode and trunk allowed VSANs
- PortChannels
- FSPF
- Fibre Channel domains (fcdomains)
- Importing and exporting the zone database from the adjacent switch

You can configure E ports in the same way you configure FCIP interfaces. The following features are also available for FCIP interfaces:

- An FCIP interface can be a member of any VSAN

  See the *Fabric Configuration Guide,Cisco DCNM for SAN*.
- Trunk mode and trunk allowed VSANs

  See the *Interfaces Configuration Guide,Cisco DCNM for SAN*.
- PortChannels
  - Multiple FCIP links can be bundled into a Fibre Channel PortChannel.
  - FCIP links and Fibre Channel links cannot be combined in one PortChannel.

    See the *Security Configuration Guide,Cisco DCNM for SAN*.
- FSPF

  See the *Fabric Configuration Guide, Cisco DCNM for SAN.*
- Fibre Channel domains (fcdomains)

  See the *System Management Configuration Guide, Cisco DCNM for SAN*.
- Importing and exporting the zone database from the adjacent switch

  See the *System Management Configuration Guide, Cisco DCNM for SAN*.

FCIP Write Acceleration

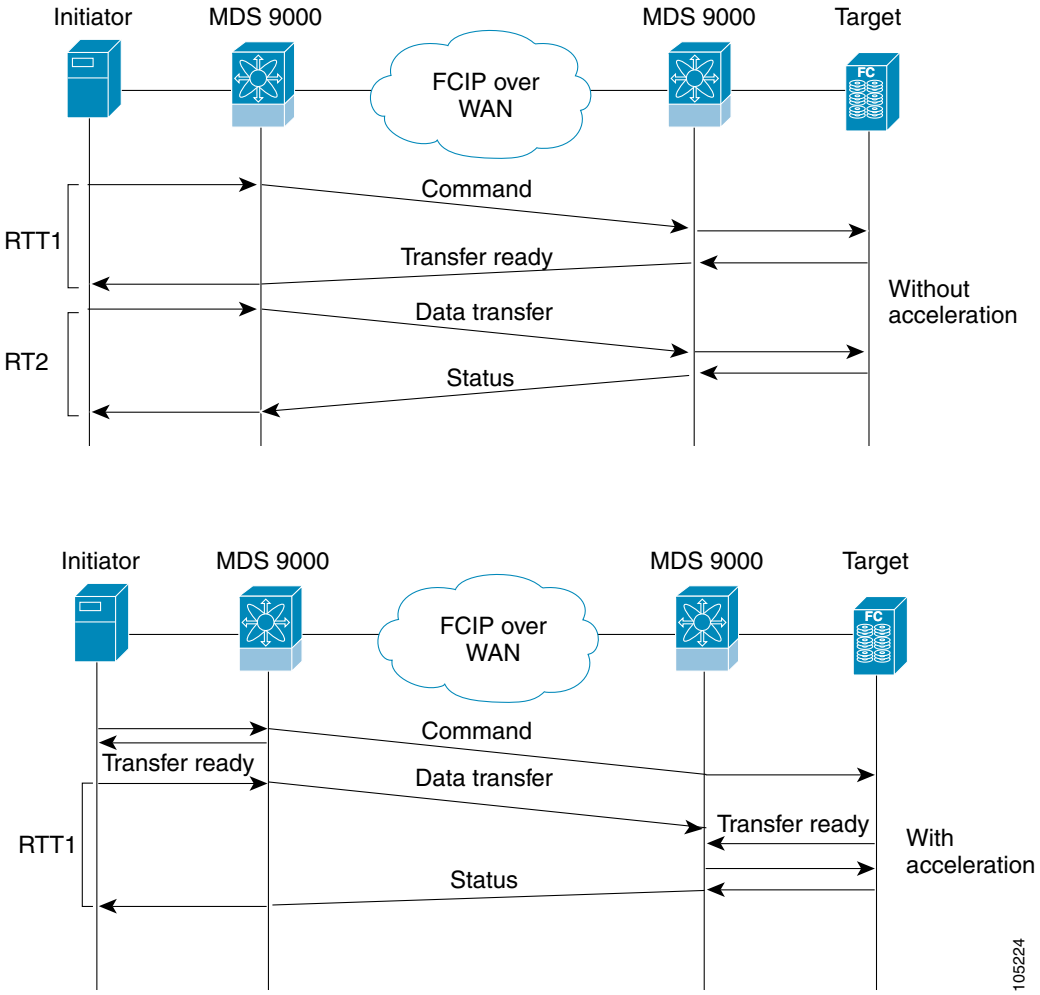
The FCIP write acceleration feature enables you to significantly improve application write performance when storage traffic is routed over wide area networks using FCIP. When FCIP write acceleration is enabled, WAN throughput is maximized by minimizing the impact of WAN latency for write operations.

Note The write acceleration feature is disabled by default and must be enabled on both sides of the FCIP link. If it is only enabled on one side of the FCIP tunnel the write acceleration feature will be turned operationally off.

Note IBM Peer to Peer Remote Copy (PPRC) is not supported with FCIP write acceleration.

The WRITE command (see Figure 2-13),without write acceleration requires two round-trip transfers (RTT), while the WRITE command with write acceleration only requires one RTT. The maximum sized Transfer Ready is sent from the host side of the FCIP link back to the host before the WRITE command reaches the target. This enables the host to start sending the write data without waiting for the long latency over the FCIP link of the WRITE command and Transfer Ready. It also eliminates the delay caused by multiple Transfer Readys needed for the exchange going over the FCIP link.

Figure 2-13 FCIP Link Write Acceleration



Tip FCIP write acceleration can be enabled for multiple FCIP tunnels if the tunnels are part of a dynamic PortChannel configured with channel mode active. FCIP write acceleration does not work if multiple non-PortChannel ISLs exist with equal weight between the initiator and the target port. Such a configuration might cause either SCSI discovery failure or failed WRITE or READ operations.

Tip Do not enable time stamp control on an FCIP interface with write acceleration configured.

Note Write acceleration cannot be used across FSPF equal cost paths in FCIP deployments. Native Fibre Channel write acceleration can be used with PortChannels. Also, FCIP write acceleration can be used in PortChannels configured with channel mode active or constructed with PortChannel Protocol (PCP).

Caution In Cisco MDS SAN-OS Release 2.0(1b) and later and NX-OS Release 4.x, FCIP write acceleration with FCIP ports as members of PortChannels are not compatible with the FCIP write acceleration in earlier releases.

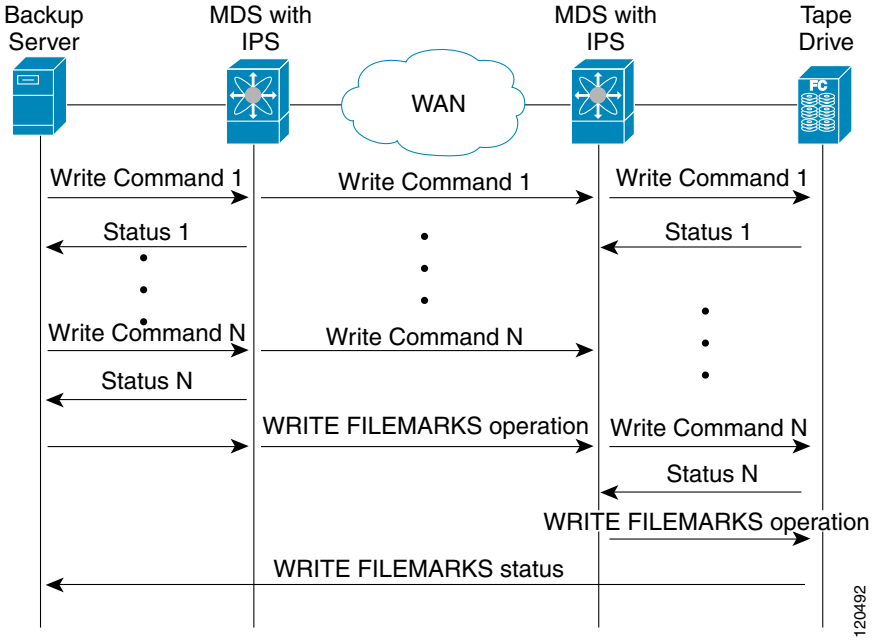
FCIP Tape Acceleration

The FCIP write acceleration feature enables you to significantly improve application write performance when storage traffic is routed over wide area networks using FCIP. When FCIP write acceleration is enabled, WAN throughput is maximized by minimizing the impact of WAN latency for write operations. The write acceleration feature is disabled by default and must be enabled on both sides of the FCIP link. Tapes are storage devices that store and retrieve user data sequentially. Cisco MDS NX-OS provides both tape write and read acceleration.

Applications that access tape drives normally have only one SCSI WRITE or READ operation outstanding to it. This single command process limits the benefit of the tape acceleration feature when using an FCIP tunnel over a long-distance WAN link. It impacts backup, restore, and restore performance because each SCSI WRITE or READ operation does not complete until the host receives a good status response from the tape drive. The FCIP tape acceleration feature helps solve this problem. It improves tape backup, archive, and restore operations by allowing faster data streaming between the host and tape drive over the WAN link.

In an example of tape acceleration for write operations, the backup server in (see Figure 2-14) issues write operations to a drive in the tape library. Acting as a proxy for the remote tape drives, the local Cisco MDS switch proxies a transfer ready to signal the host to start sending data. After receiving all the data, the local Cisco MDS switch proxies the successful completion of the SCSI WRITE operation. This response allows the host to start the next SCSI WRITE operation. This proxy method results in more data being sent over the FCIP tunnel in the same time period compared to the time taken to send data without proxying. The proxy method improves the performance on WAN links.

Figure 2-14 FCIP Link Tape Acceleration for Write Operations



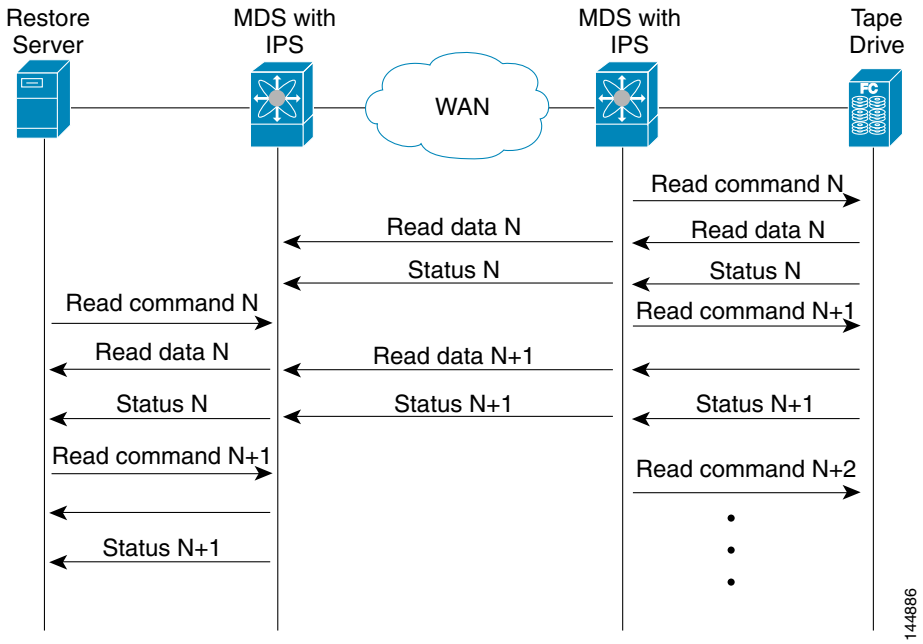
At the tape end of the FCIP tunnel, another Cisco MDS switch buffers the command and data it has received. It then acts as a backup server to the tape drive by listening to a transfer ready from the tape drive before forwarding the data.

Note In some cases such as a quick link up/down event (FCIP link, Server/Tape Port link) in a tape library environment that exports Control LUN or a Medium Changer as LUN 0 and tape drives as other LUNs, tape acceleration may not detect the tape sessions and may not accelerate these sessions. You need to keep the FCIP link disabled for a couple of minutes before enabling the link. This does not apply to tape environments where the tape drives are either direct FC attached or exported as LUN 0.

The Cisco NX-OS provides reliable data delivery to the remote tape drives using TCP/IP over the WAN. It maintains write data integrity by allowing the WRITE FILEMARKS operation to complete end-to-end without proxying. The WRITE FILEMARKS operation signals the synchronization of the buffer data with the tape library data. While tape media errors are returned to backup servers for error handling, tape busy errors are retried automatically by the Cisco NX-OS software.

In an example of tape acceleration for read operations, the restore server (see Figure 2-15) issues read operations to a drive in the tape library. During the restore process, the remote Cisco MDS switch at the tape end, in anticipation of more SCSI read operations from the host, sends out SCSI read operations on its own to the tape drive. The prefetched read data is cached at the local Cisco MDS switch. The local Cisco MDS switch on receiving SCSI read operations from the host, sends out the cached data. This method results in more data being sent over the FCIP tunnel in the same time period compared to the time taken to send data without read acceleration for tapes. This improves the performance for tape reads on WAN links.

Figure 2-15 FCIP Link Tape Acceleration for Read Operations



The Cisco NX-OS provides reliable data delivery to the restore application using TCP/IP over the WAN. While tape media errors during the read operation are returned to the restore server for error handling, the Cisco NX-OS software recovers from any other errors.

Note The FCIP tape acceleration feature is disabled by default and must be enabled on both sides of the FCIP link. If it is only enabled on one side of the FCIP tunnel, the tape acceleration feature is turned operationally off.

Tip FCIP tape acceleration does not work if the FCIP port is part of a PortChannel or if there are multiple paths between the initiator and the target port. Such a configuration might cause either SCSI discovery failure or broken write or read operations.

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

Note When you enable the tape acceleration feature for an FCIP tunnel, the tunnel is reinitialized and the write and read acceleration feature is also automatically enabled.

In tape acceleration for writes, after a certain amount of data has been buffered at the remote Cisco MDS switch, the write operations from the host are flow controlled by the local Cisco MDS switch by not proxying the Transfer Ready. On completion of a write operation when some data buffers are freed, the local Cisco MDS switch resumes the proxying. Likewise, in tape acceleration for reads, after a certain

amount of data has been buffered at the local Cisco MDS switch, the read operations to the tape drive are flow controlled by the remote Cisco MDS switch by not issuing any further reads. On completion of a read operation, when some data buffers are freed, the remote Cisco MDS switch resumes issuing reads.

The default flow control buffering uses the **automatic** option. This option takes the WAN latencies and the speed of the tape into account to provide optimum performance. You can also specify a flow control buffer size (the maximum buffer size is 12 MB).

Tip We recommend that you use the default option for flow-control buffering.

Tip Do not enable time-stamp control on an FCIP interface with tape acceleration configured.

Note If one end of the FCIP tunnel is running Cisco MDS SAN-OS Release 3.0(1) or later and NX-OS Release 4.x, and the other end is running Cisco MDS SAN-OS Release 2.x, and tape acceleration is enabled, then the FCIP tunnel will run only tape write acceleration, not tape-read acceleration.

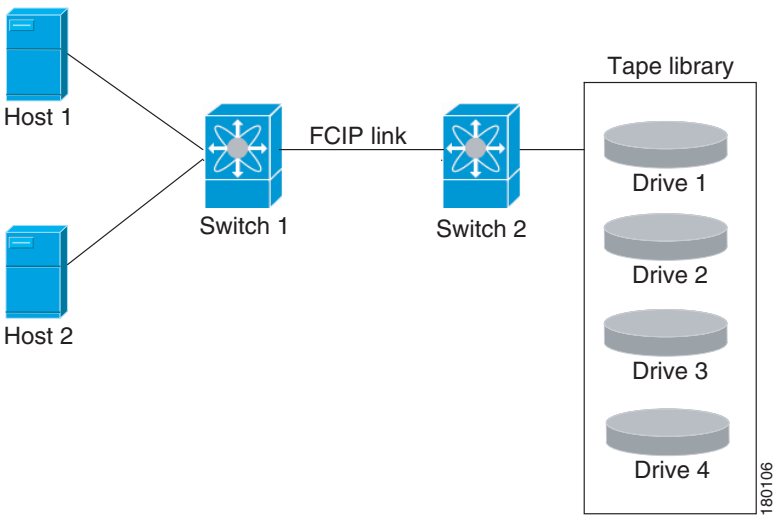
Note In Cisco MDS NX-OS Release 4.2(1), the FCIP Tape Acceleration feature is not supported on FCIP back-to-back connectivity between MDS switches.

Tape Library LUN Mapping for FCIP Tape Acceleration

If a tape library provides logical unit (LU) mapping and FCIP tape acceleration is enabled, you must assign a unique LU number (LUN) to each physical tape drive accessible through a target port.

Figure 2-16 shows tape drives connected to Switch 2 through a single target port. If the tape library provides LUN mapping, then all the four tape drives should be assign unique LUNs.

Figure 2-16 FCIP LUN Mapping Example



For the mappings described in Table 2-1 and Table 2-2, Host 1 has access to Drive 1 and Drive 2, and Host 2 has access to Drive 3 and Drive 4.

Table 2-1 describes correct tape library LUN mapping.

Table 2-1 Correct LUN Mapping Example with Single Host Access

Host	LUN Mapping	Drive
Host 1	LUN 1	Drive 1
	LUN 2	Drive 2
Host 2	LUN 3	Drive 3
	LUN 4	Drive 4

Table 2-2 describes incorrect tape library LUN mapping.

Table 2-2 Incorrect LUN Mapping Example with Single Hosts Access

Host	LUN Mapping	Drive
Host 1	LUN 1	Drive 1
	LUN 2	Drive 2
Host 2	LUN 1	Drive 3
	LUN 2	Drive 4

Another example setup is when a tape drive is shared by multiple hosts through a single tape port. For instance, Host 1 has access to Drive1 and Drive2, and Host 2 has access to Drive 2, Drive 3, and Drive 4. A correct LUN mapping configuration for such a setup is shown in Table 2-3.

Table 2-3 Correct LUN Mapping Example with Multiple Host Access

Host	LUN Mapping	Drive
Host 1	LUN 1	Drive 1
	LUN 2	Drive 2
Host 2	LUN 2	Drive 2
	LUN 3	Drive 3
	LUN 4	Drive 4

FCIP Compression

The FCIP compression feature allows IP packets to be compressed on the FCIP link if this feature is enabled on that link. By default the FCIP compression is disabled. When enabled, the software defaults to using the **auto** mode (if a mode is not specified).

Note The **auto** mode (default) selects the appropriate compression scheme based on the card type and bandwidth of the link (the bandwidth of the link configured in the FCIP profile's TCP parameters).

Table 2-4 lists the modes used for different cards.

Table 2-4 Algorithm Classification

Mode	IPS Card	MPS 14/2 Card	MSM-18/4/MDS 9222i/SSN-16
mode1	SW	HW	HW
mode2	SW	SW	HW
mode3	SW	SW	HW

Note With SAN-OS Release 3.3(1) and later and NX-OS Release 4.x, all compression options on the MDS 9222i switch and the MSM-18/4 module, mean hardware compression. Starting with Release 4.2(1), only auto compression and mode 2 compression are supported on the MDS 9222i switch, the MSM-18/4 module, and the SSN-16 module.

Table 2-5 lists the performance settings for different cards.

Table 2-5 Performance Settings

Bandwidth	IPS Cards	MPS 14/2 Card	MSM-18/4/MDS 9222i/SSN-16
Any	-	-	auto
>25 Mbps	mode 1	mode 1	auto
10-25 Mbps	mode 2	mode 2	auto
10 Mbps	mode 3	mode 3	auto

Note The Cisco MDS 9216i and 9222i Switches also support the IP compression feature. The integrated supervisor module has the same hardware components that are available in the MPS-14/2 module.

Caution The compression modes in Cisco SAN-OS Release 2.0(1b) and later and NX-OS Release 4.x are incompatible with the compression modes in Cisco SAN-OS Release 1.3(1) and earlier.

Tip While upgrading from Cisco SAN-OS Release 1.x to Cisco SAN-OS Release 2.0(1b) or later and NX-OS Release 4.x, we recommend that you disable compression before the upgrade procedure, and then enable the required mode after the upgrade procedure.

If both ends of the FCIP link are running Cisco SAN-OS Release 2.0(1b) or later and NX-OS Release 4.x and you enable compression at one end of the FCIP tunnel, be sure to enable it at the other end of the link.

Default Settings

Table 2-6 lists the default settings for FCIP parameters.

Table 2-6 Default FCIP Parameters

Parameters	Default
TCP default port for FCIP	3225
minimum-retransmit-time	200 msec
Keepalive timeout	60 sec
Maximum retransmissions	4 retransmissions
PMTU discovery	Enabled
pmtu-enable reset-timeout	3600 sec
SACK	Enabled
max-bandwidth	1 Gbps
min-available-bandwidth	500 Mbps
round-trip-time	1 msec
Buffer size	0 KB
Control TCP and data connection	No packets are transmitted
TCP congestion window monitoring	Enabled
Burst size	50 KB
TCP connection mode	Active mode is enabled
special-frame	Disabled
FCIP timestamp	Disabled
acceptable-diff range to accept packets	+/– 2000 msec
B port keepalive responses	Disabled
Write acceleration	Disabled
Tape acceleration	Disabled

Configuring FCIP

This section describes how to configure FCIP and includes the following topics:

Enabling FCIP

Detailed Steps

Note In Cisco MDS SAN-OS Release 2.0 and later and NX-OS Release 4.x, there is an additional login prompt to log into a switch that is not a part of your existing fabric.

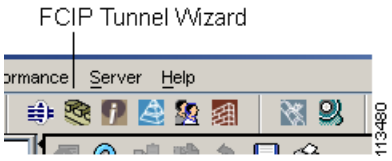
To create and manage FCIP links with DCNM-SAN, use the FCIP Wizard. Make sure that the IP Services Module is inserted in the required Cisco MDS 9000 Family switch, and that the Gigabit Ethernet interfaces on these switches are connected, and then verify the connectivity. The procedures for creating FCIP links using the FCIP Wizard are as follows:

- Select the endpoints.
- Choose the interfaces' IP addresses.
- Specify link attributes.
- (Optional) Enable FCIP write acceleration or FCIP compression.

To create FCIP links using the FCIP Wizard, follow these steps:

Step 1 Click the **FCIP Wizard** icon in the DCNM-SAN toolbar (See Figure 2-17).

Figure 2-17 FCIP Wizard



Step 2 Choose the switches that act as endpoints for the FCIP link and click **Next**.

Step 3 Choose the Gigabit Ethernet ports on each switch that will form the FCIP link.

Step 4 If both Gigabit Ethernet ports are part of MPS-14/2 modules, check the **Enforce IPSEC Security** check box and set the **IKE Auth Key**. See the *Security Configuration Guide, Cisco DCNM for SAN* for information on IPsec and IKE.

Check the **Use Large MTU Size (Jumbo Frames)** option to use jumbo size frames of 2300. Since Fibre Channel frames are 2112, we recommended that you use this option. If you uncheck the box, the FCIP Wizard does not set the MTU size, and the default value of 1500 is set.

Note In Cisco MDS 9000 SAN-OS, Release 3.0(3), by default the **Use Large MTU Size (Jumbo Frames)** option is not selected.

Step 5 Click **Next**.

You see the IP Address/Route input screen.

Step 6 Select **Add IP Route** if you want to add an IP route, otherwise retain the defaults.

Step 7 Click **Next**.

You see the TCP connection characteristics.

Step 8 Set the minimum and maximum bandwidth settings and round-trip time for the TCP connections on this FCIP link.

You can measure the round-trip time between the Gigabit Ethernet endpoints by clicking the **Measure** button.

Step 9 Check the **Write Acceleration** check box to enable FCIP write acceleration on this FCIP link.

See the "FCIP Write Acceleration" section on page 2-12.

Step 10 Check the **Enable Optimum Compression** check box to enable IP compression on this FCIP link.

See the "FCIP Compression" section on page 2-18.

Step 11 Check the Enable XRC Emulator check box to enable XRC emulator on this FCIP link.

For more information on XRC Emulator, see the *Fabric Configuration Guide, Cisco DCNM for SAN.*

Step 12 Click **Next.**

Step 13 Set the **Port VSAN** and click the **Trunk Mode** radio button for this FCIP link.

Step 14 Click **Finish** to create this FCIP link.

Modifying an FCIP Link

Once you have created FCIP links using the FCIP wizard, you may need to modify parameters for these links. This procedure includes modifying the FCIP profiles as well as the FCIP link parameters. Each Gigabit Ethernet interface can have three active FCIP links at one time.

To modify an FCIP link, follow these steps on both switches:

Step 1 Configure the Gigabit Ethernet interface.

Step 2 Create an FCIP profile, and then assign the Gigabit Ethernet interface's IP address to the profile.

Step 3 Create an FCIP interface, and then assign the profile to the interface.

Step 4 Configure the peer IP address for the FCIP interface.

Step 5 Enable the interface.

Creating FCIP Profiles

Detailed Steps

To create an FCIP profile in switch 1, follow these steps:

Step 1 Verify that you are connected to a switch that contains an IPS module.

Step 2 From DCNM-SAN, choose **Switches > ISLs > FCIP** in the Physical Attributes pane. From Device Manager, choose **FCIP** from the IP menu.

Step 3 Click the **Create Row** button in DCNM-SAN or the **Create** button on Device Manager to add a new profile.

Step 4 Enter the profile ID in the ProfileId field.

Step 5 Enter the IP address of the interface to which you want to bind the profile.

Step 6 Modify the optional TCP parameters, if desired. Refer to DCNM for SAN Online Help for explanations of these fields.

Step 7 (Optional) Click the **Tunnels** tab and modify the remote IP address in the Remote IPAddress field for the endpoint to which you want to link.

Step 8 Enter the optional parameters, if required.

See the"FCIP Profiles" section on page 2-4 for information on displaying FCIP profile information.

Step 9 Click **Apply Changes** icon to save these changes.

Checking Trunk Status

By default, trunk mode is enabled in all Fibre Channel interfaces. However, trunk mode configuration takes effect only in E-port mode. You can configure trunk mode as on (enabled), off (disabled), or auto (automatic). The default trunk mode is on. The trunk mode configuration at the two ends of an ISL, between two switches, determines the trunking state of the link and the port modes at both ends.

Detailed Steps

To check the trunk status for the FCIP interface on Device Manager, follow these steps:

Step 1 Make sure you are connected to a switch that contains an IPS module.

Step 2 Select **FCIP** from the IP menu.

Step 3 Click the **Trunk Config** tab if it is not already selected. You see the FCIP Trunk Config dialog box. This shows the status of the interface.

Step 4 Click the **Trunk Failures** tab if it is not already selected. You see the FCIP Trunk Failures dialog box.

Launching Cisco Transport Controller

Cisco Transport Controller (CTC) is a task-oriented tool used to install, provision, and maintain network elements. It is also used to troubleshoot and repair NE faults.

Detailed Steps

To launch CTC, follow these steps:

Step 1 Right-click an ISL carrying optical traffic in the fabric.

Step 2 Click **Element Manager**.

Step 3 Enter the URL for the Cisco Transport Controller.

Step 4 Click **OK**.

Configuring TCP Parameters

You can control TCP behavior in a switch by configuring the TCP parameters that are described in this section.

Note When FCIP is sent over a WAN link, the default TCP settings may not be appropriate. In such cases, we recommend that you tune the FCIP WAN link by modifying the TCP parameters (specifically bandwidth, round-trip times, and CWM burst size).

This section includes the following topics:

Configuring Minimum Retransmit Timeout

You can control the minimum amount of time TCP waits before retransmitting. By default, this value is 200 milliseconds (msec).

Configuring Keepalive Timeout

You can configure the interval that the TCP connection uses to verify that the FCIP link is functioning. This ensures that an FCIP link failure is detected quickly even when there is no traffic.

You can configure the first interval during which the connection is idle (the default is 60 seconds). When the connection is idle for the configured interval, eight keepalive probes are sent at 1-second intervals. If no response is received for these eight probes and the connection remains idle throughout, that FCIP link is automatically closed.

Note Only the first interval (during which the connection is idle) can be changed.

Configuring Maximum Retransmissions

You can specify the maximum number of times a packet is retransmitted before TCP decides to close the connection.

Configuring Path MTUs

Path MTU (PMTU) is the minimum MTU on the IP network between the two endpoints of the FCIP link. PMTU discovery is a mechanism by which TCP learns of the PMTU dynamically and adjusts the maximum TCP segment accordingly (RFC 1191).

By default, PMTU discovery is enabled on all switches with a timeout of 3600 seconds. If TCP reduces the size of the maximum segment because of PMTU change, the reset-timeout specifies the time after which TCP tries the original MTU.

Configuring Selective Acknowledgments

TCP may experience poor performance when multiple packets are lost within one window. With the limited information available from cumulative acknowledgments, a TCP sender can only learn about a single lost packet per round trip. A selective acknowledgment (SACK) mechanism helps overcome the limitations of multiple lost packets during a TCP transmission.

The receiving TCP sends back SACK advertisements to the sender. The sender can then retransmit only the missing data segments. By default, SACK is enabled on Cisco MDS 9000 Family switches.

Configuring Window Management

The optimal TCP window size is automatically calculated using the maximum bandwidth parameter, the minimum available bandwidth parameter, and the dynamically measured round-trip time (RTT).

Note The configured **round-trip-time** parameter determines the window scaling factor of the TCP connection. This parameter is only an approximation. The measured RTT value overrides the round trip time parameter for window management. If the configured **round-trip-time** is too small compared to the measured RTT, then the link may not be fully utilized due to the window scaling factor being too small.

The **min-available-bandwidth** parameter and the measured RTT together determine the threshold below which TCP aggressively maintains a window size sufficient to transmit at minimum available bandwidth.

The **max-bandwidth-mbps** parameter and the measured RTT together determine the maximum window size.

Note Set the maximum bandwidth to match the worst-case bandwidth available on the physical link, considering other traffic that might be going across this link (for example, other FCIP tunnels, WAN limitations). Maximum bandwidth should be the total bandwidth minus all other traffic going across that link.

Configuring Monitoring Congestion

By enabling the congestion window monitoring (CWM) parameter, you allow TCP to monitor congestion after each idle period. The CWM parameter also determines the maximum burst size allowed after an idle period. By default, this parameter is enabled and the default burst size is 50 KB.

The interaction of bandwidth parameters and CWM and the resulting TCP behavior is outlined as follows:

- If the average rate of the Fibre Channel traffic over the preceding RTT is less than the min-available-bandwidth multiplied by the RTT, the entire burst is sent immediately at the min-available-bandwidth rate, provided no TCP drops occur.
- If the average rate of the Fibre Channel traffic is greater than min-available-bandwidth multiplied by the RTT, but less than max-bandwidth multiplied by the RTT, then if the Fibre Channel traffic is transmitted in burst sizes smaller than the configured CWM value the entire burst is sent immediately by FCIP at the max-bandwidth rate.
- If the average rate of the Fibre Channel traffic is larger than the min-available-bandwidth multiplied by the RTT and the burst size is greater than the CWM value, then only a part of the burst is sent immediately. The remainder is sent with the next RTT.

The software uses standard TCP rules to increase the window beyond the one required to maintain the min-available-bandwidth to reach the max-bandwidth.

Note The default burst size is 50 KB.

Tip We recommend that this feature remain enabled to realize optimal performance. Increasing the CWM burst size can result in more packet drops in the IP network, impacting TCP performance. Only if the IP network has sufficient buffering, try increasing the CWM burst size beyond the default to achieve lower transmit latency.

Configuring Estimating Maximum Jitter

Jitter is defined as a variation in the delay of received packets. At the sending side, packets are sent in a continuous stream with the packets spaced evenly apart. Due to network congestion, improper queuing, or configuration errors, this steady stream can become lumpy, or the delay between each packet can vary instead of remaining constant.

You can configure the maximum estimated jitter in microseconds by the packet sender. The estimated variation should not include network queuing delay. By default, this parameter is enabled in Cisco MDS switches when IPS modules or MPS-14/2 modules are present.

The default value is 1000 microseconds for FCIP interfaces.

Configuring Buffer Size

You can define the required additional buffering—beyond the normal send window size —that TCP allows before flow controlling the switch's egress path for the FCIP interface. The default FCIP buffer size is 0 KB.

Note Use the default if the FCIP traffic is passing through a high throughput WAN link. If you have a mismatch in speed between the Fibre Channel link and the WAN link, then time stamp errors occur in the DMA bridge. In such a situation, you can avoid time stamp errors by increasing the buffer size.

Assigning a Peer IP Address

The basic FCIP configuration uses the peer's IP address to configure the peer information. You can also specify the peer's port number to configure the peer information. If you do not specify a port, the default 3225 port number is used to establish connection. You can specify an IPv4 address or an IPv6 address.

Detailed Steps

To assign the peer information based on the IPv4 address and port number, follow these steps:

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

You see the FCIP profiles and links in the Information pane.

From Device Manager, choose **IP > FCIP**.

You see the FCIP dialog box.

Step 2 Click the **Tunnels** tab. You see the FCIP link information.

Step 3 Click the **Create Row** icon in DCNM-SAN or the **Create** button in Device Manager.

You see the FCIP Tunnels dialog box.

Step 4 Set the ProfileID and TunnelID fields.

Step 5 Set the RemoteIPAddress and RemoteTCPPort fields for the peer IP address you are configuring.

Step 6 Check the **PassiveMode** check box if you do not want this end of the link to initiate a TCP connection.

Step 7 (Optional) Set the **NumTCPCon** field to the number of TCP connections from this FCIP link.

Step 8 (Optional) Check the **Enable** check box in the Time Stamp section and set the Tolerance field.

Step 9 (Optional) Set the other fields in this dialog box and click **Create** to create this FCIP link.

To assign the peer information based on the IPv6 address and port number, follow these steps:

Step 1 From DCNM-SAN, choose **ISLs > FCIP** from the Physical Attributes pane.

You see the FCIP profiles and links in the Information pane.

From Device Manager, choose **IP > FCIP**. You see the FCIP dialog box.

Step 2 Click the **Tunnels** tab. You see the FCIP link information.

Step 3 Click the **Create Row** icon in DCNM- SAN or the **Create** button in Device Manager.

You see the FCIP Tunnels dialog box.

Step 4 Set the ProfileID and TunnelID fields.

Step 5 Set the RemoteIPAddress and RemoteTCPPort fields for the peer IP address you are configuring.

Step 6 Check the **PassiveMode** check box if you do not want this end of the link to initiate a TCP connection.

Step 7 (Optional) Set the **NumTCPCon** field to the number of TCP connections from this FCIP link.

Step 8 (Optional) Check the **Enable** check box in the Time Stamp section and set the Tolerance field.

Step 9 (Optional) Set the other fields in this dialog box and click **Create** to create this FCIP link.

Configuring Active Connections

You can configure the required mode for initiating a TCP connection. By default, the active mode is enabled to actively attempt an IP connection. If you enable the passive mode, the switch does not initiate a TCP connection but waits for the peer to connect to it. By default, the switch tries two TCP connections for each FCIP link.

Note Ensure that both ends of the FCIP link are not configured as passive mode. If both ends are configured as passive, the connection is not initiated.

Enabling Time Stamp Control

You can instruct the switch to discard packets that are outside the specified time. When enabled, this feature specifies the time range within which packets can be accepted. If the packet arrived within the range specified by this option, the packet is accepted. Otherwise, it is dropped.

By default, time stamp control is disabled in all switches in the Cisco MDS 9000 Family. If a packet arrives within a 2000 millisecond interval (+ or –2000 msec) from the network time, that packet is accepted.

Note The default value for packet acceptance is 2000 microseconds.If the **time-stamp** option is enabled, be sure to configure NTP on both switches (see the *Cisco NX-OS Fundamentals Configuration Guide* for more information).

Tip Do not enable time stamp control on an FCIP interface that has tape acceleration or write acceleration configured.

Configuring B Ports

While E ports typically interconnect Fibre Channel switches, some SAN extender devices, such as Cisco's PA-FC-1G Fibre Channel port adapter and the SN 5428-2 storage router, implement a bridge port model to connect geographically dispersed fabrics. This model uses B port as described in the T11 Standard FC-BB-2. B ports bridge Fibre Channel traffic from a local E port to a remote E port without participating in fabric-related activities such as principal switch election, domain ID assignment, and Fibre Channel fabric shortest path first (FSPF) routing. The IPS module and MPS-14/2 module support FCIP links that originate from a B port SAN extender device by implementing the B access ISL protocol on a Gigabit Ethernet interface.

When an FCIP peer is a SAN extender device that only supports Fibre Channel B ports, you need to enable the B port mode for the FCIP link. When a B port is enabled, the E port functionality is also enabled and they coexist. If the B port is disabled, the E port functionality remains enabled.

Detailed Steps

To enable B port mode, follow these steps:

Step 1 Choose **ISLs > FCIP** from the Physical Attributes pane.

You see the FCIP profiles and links in the Information pane.

From Device Manager, choose **IP > FCIP**. You see the FCIP dialog box.

Step 2 Click the **Tunnels** tab.

You see the FCIP link information.

Step 3 Click the **Create Row** icon in DCNM-SAN or the **Create** button in Device Manager.

You see the FCIP Tunnels dialog box.

Step 4 Set the ProfileID and TunnelID fields.

Step 5 Set the RemoteIPAddress and RemoteTCPPort fields for the peer IP address you are configuring.

Step 6 Check the **PassiveMode** check box if you do not want this end of the link to initiate a TCP connection.

Step 7 (Optional) Set the NumTCPCon field to the number of TCP connections from this FCIP link.

Step 8 Check the **Enable** check box in the B Port section of the dialog box and optionally check the **KeepAlive** check box if you want a response sent to an ELS Echo frame received from the FCIP peer.

Step 9 (Optional) Set the other fields in this dialog box and click **Create** to create this FCIP link.

Configuring FCIP Write Acceleration

You can enable FCIP write acceleration when you create the FCIP link using the FCIP Wizard.

Detailed Steps

To enable write acceleration on an existing FCIP link, follow these steps:

Step 1 Choose **ISLs > FCIP** from the Physical Attributes pane on DCNM-SAN.

You see the FCIP profiles and links in the Information pane.

On Device Manager, choose **IP > FCIP**.

You see the FCIP dialog box.

Step 2 Click the **Tunnels (Advanced)** tab.

You see the FICP link information.

Step 3 Check or uncheck the **Write Accelerator** check box.

Step 4 Choose the appropriate compression ratio from the **IP Compression** drop-down list.

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

Configuring FCIP Tape Acceleration

Detailed Steps

To enable FCIP tape acceleration, follow these steps:

Step 1 From DCNM-SAN, choose **ISLs > FCIP** from the Physical Attributes pane.

You see the FCIP profiles and links in the Information pane.

From Device Manager, choose **IP > FCIP**.

You see the FCIP dialog box.

Step 2 Click the **Tunnels** tab. You see the FICP link information.

Step 3 Click the **Create Row** icon in DCNM-SAN or the **Create** button in Device Manager.

You see the FCIP Tunnels dialog box.

Step 4 Set the profile ID in the ProfileID field and the tunnel ID in the TunnelID fields.

Step 5 Set the RemoteIPAddress and RemoteTCPPort fields for the peer IP address you are configuring.

Step 6 Check the **TapeAccelerator** check box.

Step 7 (Optional) Set the other fields in this dialog box and click **Create** to create this FCIP link.

Verifying FCIP Configuration

To verify the FCIP interfaces and Extended Link Protocol (ELP) on Device Manager, follow these steps:

Step 1 Make sure you are connected to a switch that contains an IPS module.

Step 2 Select **FCIP** from the Interface menu.

Step 3 Click the **Interfaces** tab if it is not already selected. You see the FCIP Interfaces dialog box.

Step 4 Click the **ELP** tab if it is not already selected. You see the FCIP ELP dialog box.

Field Descriptions for FCIP

This section describes the field description for FCIP.

FCIP Monitor

Field	Description
C3 Rx Bytes	The number of incoming bytes of data traffic.
C3 Tx Bytes	The number of outgoing bytes of data traffic.
CF Rx Bytes	The number of incoming bytes of control traffic.
CF Tx Bytes	The number of outgoing bytes of control traffic.
Rx Error	The number of inbound frames that contained errors preventing them from being deliverable to a higher-layer protocol.

Field	Description
Tx Error	The number of outbound frames that could not be transmitted because of errors.
RxDiscard	The number of inbound frames that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol.
TxDiscard	The number of outbound frames that were chosen to be discarded even though no errors had been detected to prevent their being transmitted.

FCIP Interfaces Interfaces

Field	Description
Description	Alias name for the interface as specified by a network manager.
PortVsan	The VSAN ID to which this interface is statically assigned.
Oper	The current operating mode of the port.
AutoChannelCreate	If checked, automatically create the PortChannel.
Admin	The desired state of the interface.
Oper	The current operational state of the interface.
FailureCause	The cause of current operational state of the port.
LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value is N/A.
FICON Address	The FICON port address of this port.

FCIP Interfaces Trunk Failures

Field	Description
FailureCause	An entry is shown in this table if there is an error in the trunk status for the given VSAN.

FCIP FICON Configuration

Field	Description
Interface	This is a unique value that identifies the interface on this FCIP device to which this link pertains.
VSAN List Admin	This is the list of VSANs (in the range 1 through 2047) for which FICON tape acceleration is configured. Only VSANs with a cficonVsanEntry of CISCO-FICON-MIB present can be configured for FICON tape acceleration.
VSAN List Oper	This is the list of VSANs (in the range 1 through 2047) for which FICON tape acceleration is operationally ON.

FCIP Profiles

Field	Description
IP Address	The Internet address for this entity.
Port	A TCP port other than the FCIP well-known port on which the FCIP entity listens for new TCP connection requests.
SACK	Whether the TCP Selective Acknowledgement Option is enabled to allow the receiver end to acknowledge multiple lost frames in a single ACK, enabling faster recovery.
KeepAlive (s)	The TCP keep-alive timeout for all links within this entity.
ReTrans MinTimeout (ms)	The TCP minimum retransmit timeout for all the links on this entity.
ReTrans Max	The maximum number of times that the same item of data will be retransmitted over a TCP connection. If delivery is not acknowledged after this number of retransmissions then the connection is terminated.
Send BufSize (KB)	The aggregate TCP send window for all TCP connections on all Links within this entity. This value is used for egress flow control. When the aggregate of the data queued on all connections within this entity reaches this value, the sender is flow controlled.
Bandwidth Max (Kb)	This is an estimate of the bandwidth of the network pipe used for the B-D product computation, which lets us derive the TCP receive window to advertise.
Bandwidth Min (Kb)	The minimum available bandwidth for the TCP connections on the links within this entity.
Est Round Trip Time (us)	This is an estimate of the round trip delay of the network pipe used for the B-D product computation, which lets us derive the TCP receive window to advertise.
PMTU Enable	The path MTU discovery.
PMTU ResetTimeout (sec)	The time interval for which the discovered path MTU is valid, before MSS reverts back to the negotiated TCP value.
CWM Enable	If true, congestion window monitoring is enabled.

Field	Description
CWM BurstSize (KB)	The maximum burst sent after a TCP sender idle period.
Max Jitter	The maximum delay variation (not due to congestion) that can be experienced by TCP connections on this interface.

FCIP Tunnels

Field	Description
Interface	This identifies the interface on this FCIP device to which this link pertains.
Attached	The interface on which this FCIP link was initiated.
B Port Enable	If true, the B port mode is enabled on the local FCIP link.
B Port KeepAlive	If true, a message is sent in response to a (Fibre Channel) ELS Echo frame received from the peer. Some B Port implementations use ELS Echo request/response frames as link keep alive.
Remote IP Address	The Internet address for the remote FCIP entity.
Remote TCP Port	The remote TCP port to which the local FCIP entity will connect if and when it initiates a TCP connection setup for this link.
Spc Frames Enable	If true, the TCP active opener initiates FCIP special frames and the TCP passive opener responds to the FCIP special frames. If it is set to false, the FCIP special frames are neither generated nor responded to.
Spc Frames RemoteWWN	The world wide name of the remote FC fabric entity. If this is a zero length string then this link would accept connections from any remote entity. If a WWN is specified then this link would accept connections from a remote entity with this WWN.
Spc Frames Remote Profile Id	The remote FCIP entity's identifier.

FCIP Tunnels (Advanced)

Field	Description
Interface	The interface on which this FCIP link was initiated.
Timestamp Enable	If true, the timestamp in FCIP header is to checked.
Timestamp Tolerance	The accepted time difference between the local time and the timestamp value received in the FCIP header. By default this value will be EDTOV/2. EDTOV is the Error_Detect_Timeout Value used for Fibre channel Ports as the timeout value for detecting an error condition.
Number Connections	The maximum number of TCP connections allowed on this link.
Passive	If false, this link endpoint actively tries to connect to the peer. If true, the link endpoint waits for the peer to connect to it.

Field	Description
QoS Control	The value to be set for the ToS field in IP header for the TCP control connection.
QoS Data	The value to be set for the ToS field in IP header for the TCP Data connection.
IP Compression	What algorithm is used, if any.
Write Accelerator	The write accelerator allows for enhancing SCSI write performance.
Tape Accelerator	If true, the tape accelerator (which allows for enhancing Tape write performance) is enabled.
Tape Accelerator Oper	Write acceleration is enabled for the FCIP link.
TapeRead Accelerator Oper	Enabled automatically when the tape accelerator Oper is active.
FlowCtrlBufSize Tape (KB)	The size of the flow control buffer (64 K to 32 MB). If set to 0, flow control buffer size is calculated automatically by the switch.
IPSec	Indicates whether the IP security has been turned on or off on this link.
XRC Emulator	Check to enable XRC emulator. It is disabled by default.
XRC Emulator Oper	Indicates the operational status of XRC emulator.

FCIP Tunnels (FICON TA)

Field	Description
Interface	A unique value that identifies the interface on this FCIP device to which this link pertains.
VSAN List Admin	The list of VSANs for which FICON tape acceleration is configured.
VSAN List Oper	The list of VSANs for which FICON tape acceleration is operationally on.

FCIP Tunnels Statistics

Field	Description
Interface	A unique value that identifies the interface on this FCIP device to which this link pertains.
Rx IPCompRatio	The IP compression ratio for received packets on the FCIP device. The value of this object will be presented as a floating point number with two digits after the decimal point.
Tx IPCompRatio	The IP compression ratio for transmitted packets on the FCIP device. The value of this object will be presented as a floating point number with two digits after the decimal point.

FCIP XRC Statistics

Field	Description
ProfileId	Unique ID of the profile.
Interface	Name of the interface.
RRSAccelerated	The number of read record set IUs accelerated.
RRSForwarded	Number of read record set IUs forwarded.
BusyStatus	Number of instances of busy status received from the control unit.
UnitCheckStatus	Number of instances of unit check status received from the control unit.
cfmFcipLinkExtXRCEStats SelReset	Number of selective resets processed.
BufferAllocErrors	Number of buffer allocation errors.

Additional References

For additional information related to implementing FCIPs, see the following section:

- Related Document, page 2-35
- Standards, page 2-35
- RFCs, page 2-36
- MIBs, page 2-36

Related Document

Related Topic	Document Title
Cisco MDS 9000 Family Command Reference	*Cisco MDS 9000 Family Command Reference, Release 5.0(1a)*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	–

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified.	–

MIBs

MIBs	MIBs Link
• CISCO-FCIP-MGMT-EXT-MIB • CISCO-FCIP-MGMT-MIB • CISCO-FEATURE-CONTROL-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/dc-os/mibs

Feature History for FCIP

Table 2-7 lists the release history for this feature. Only features that were introduced or modified in 5.0(1a) or a later release appear in the table.

Table 2-7 Feature History for FCIP

Feature Name	Releases	Feature Information
Configuring FCIP	5.0(1a)	FCIP Compression