



CATE Storage and Backup Engineering
Citigroup Architecture and Technology Engineering

Cisco MDS FCIP v7.0 (MDS-9250i)

CSBE-15000-SG

Solutions Guide

1.0

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

1 Version Control

Version	Date	Author	Reviewed	Comments
0.1	16-Feb-2015	Scott Torgerson	Ludwig Derodel, Kevin Hobaugh, Tom Funke (Cisco)	Peer
0.5	17-Mar-2015	Scott Torgerson	Global Stakeholders	RFC
1.0	16-Apr-2015	Scott Torgerson	Global Stakeholders	Release to Production

2 Legal Notice

Information contained herein is for Internal Use and may be used only for business purposes authorized by Citigroup.

CITI, CITIBANK, CITICORP, and CITIGROUP are trademarks and service marks of Citicorp and are used and registered throughout the world. Citibank, Citicorp, Citigroup and their subsidiaries also claim rights in certain other trademarks and service marks contained in these pages.

3 Contact

Please address any comments or questions regarding the information contained in this document via email to the *CATE Storage [mailto:*CATE Storage and Backup Engineering](mailto:*CATE.Storage.and.Backup.Engineering) and Backup Engineering distribution list.

4 Latest Versions

It is recommended that the latest version of the document be used from the CSBE website at the following URL:
<http://catecollaboration.citigroup.net/domains/platstor/gdse/products/default.aspx>.
Newer versions may include certification on additional platforms, or comments on issues discovered after deployment.

5 Table Of Contents

1	VERSION CONTROL	2
2	LEGAL NOTICE.....	3
3	CONTACT.....	3
4	LATEST VERSIONS	3
5	TABLE OF CONTENTS	4
6	TABLE OF FIGURES.....	6
7	INTRODUCTION.....	7
7.1	MAJOR ENHANCEMENTS	7
8	APPLICABLE ENVIRONMENTS.....	8
8.1	COMPONENT CERTIFICATION MATRIX	9
9	BEST PRACTICES	10
9.1	MDS 9250i.....	10
9.2	VSANs.....	10
9.3	INTER VSAN ROUTING (IVR)	10
9.4	VSAN DOMAIN ID'S	10
9.5	PORT-CHANNELS	11
9.6	WRITE ACCELERATION	11
9.7	COMPRESSION.....	11
9.8	IPSEC ENCRYPTION	11
9.9	JUMBO FRAMES.....	12
9.10	DEDICATED FCIP BANDWIDTH (REPLICATION).....	12
9.11	SHARED FCIP BANDWIDTH (DATA MIGRATION).....	12
9.12	FCIP TUNNEL/PROFILE MAX BANDWIDTH.....	13
9.13	FCIP TUNNEL/PROFILE MIN BANDWIDTH	13
9.14	FCIP TUNNELS PER GIGE INTERFACE.....	13
9.15	FCIP QOS	14
9.16	IP ACLs	14
10	PLANNING/INSTALLATION/CONFIGURATION CHECKLIST.....	15
11	PLANNING STEPS	16
11.1	DETERMINE NUMBER OF REQUIRED FC PORTS.....	16
11.2	DETERMINE NUMBER OF GIGE PORTS INTO BANDWIDTH	16
11.3	DETERMINE THE AMOUNT OF TRAFFIC TO REPLICATE.....	16
11.4	DETERMINE THE NUMBER OF MDS-9250i SWITCHES	17
11.5	ATS FOR MDS-9250i DATACENTER INSTALLATION.....	17
11.5.1	MDS 9250i Power Supplies	17
11.6	ORDER THE MDS-9250i SWITCHES	18
11.7	OPEN A NETWORK PIF	18

12	INSTALLATION.....	20
13	CONFIGURATION.....	21
13.1	DISCOVER REMOTE SITE 9250i IN DCNM	22
13.2	ENABLE FCIP FEATURE.....	23
13.3	SETUP GIGE INTERFACES.....	23
13.4	SETUP STATIC ROUTES	24
13.5	GET RTT TIMES.....	24
13.6	SETUP FCIP PROFILES AND INTERFACES	25
13.7	PUT FCIP INTERFACES IN A PORT-CHANNEL	32
13.8	MAKE CROSS-SITE VSAN	33
13.9	ADD CROSS-SITE VSAN TO PORT-CHANNEL	33
13.10	ENABLE ENHANCED ZONING	34
13.11	CREATE ZONES AND ZONESET	34
13.12	CHECK ZONING CONNECTIVITY	35
13.13	ENABLE IP ACLS.....	36
13.14	ENABLE IPSEC ENCRYPTION (OPTIONAL)	38
14	REFERENCES.....	39
15	APPENDICES.....	40
15.1	APPENDIX A: DETERMINING FCIP GIGE MAX-BANDWIDTH-MBPS.....	40

6 Table of Figures

Figure 1 - CLI Example Diagram.....	21
Figure 2 – Open Fabric Screen.....	22
Figure 3 – Discover Fabric Screen.....	22
Figure 4 – Open Fabric Screen.....	23
Figure 5 – End to End Connectivity Screen	36
Figure 6 - IP ACLs Example Diagram	37
Figure 7 - Max-Bandwidth Example Diagram	40

7 Introduction

Using FCIP on the Cisco MDS series switches with line cards, or the new MDS-9250i switch, provides Citigroup the ability to extend SAN traffic to great distances to multiple sites across the existing Citigroup IP infrastructure. FCIP provides opportunities for Citigroup to implement secure enterprise-wide SAN strategies that are stable, interoperable, and scalable.

Using Cisco FCIP, Citigroup can connect local SANs to remote SANs in other locations via the IP network. Once connected the following project types could possibly take advantage of Cisco MDS FCIP.

- Asynchronous Data Replication (SRDF/A)
- Host initiator to remote pooled storage (for Data Migrations purposes only)

Note: This project focuses on the new MDS-9250i only. FCIP administrators requiring installation or configuration information for the MDS-9222i, SSN-16, or 18/4MSM should consult the [Cisco FCIP v6.0 Solutions Guide](#).

7.1 Major Enhancements

The major changes and enhancements to be added by this version of the Cisco MDS FCIP project are as follows:

- Certification of new Cisco NX-OS operating system
- Certification of new Cisco Device Manager
- Certification of new Cisco DCNM
- Certification of new Cisco 10Gb MDS 9250i
- Certification of multiple tunnels on each 10 GigE port

8 Applicable Environments

This document is scoped mainly at the new 10Gb MDS9250i as all previous environments upgraded Microcode due to a critical VTM which made CATE rely on all Cisco testing for the existing FCIP products.

This project and set of documents is specifically meant the following environments that will be impacted by the certification of the 10Gb MDS 9250i.

- Any data centers that are currently tech refreshing FCIP environments should use this version of FCIP as the 10Gb MDS-9250i will simplify the environment.
- Any data centers doing new FCIP deployments should use this version of FCIP that makes use of the 10Gb MDS-9250i.

8.1 Component Certification Matrix

This following table shows the hardware types and software components and the versions that will be certified for this project.

Component Matrix	
MDS Models	MDS-9506 MDS-9509 ¹ MDS-9513 MDS-9216i ² MDS-9222i ³ MDS-9250i ⁴
Supported Line Cards	18/4 MSM, SSN-16 ⁵
Operating Systems	NX-OS 5.2(8e) ⁶ NX-OS 6.2(11b) ⁷ (MDS-9250i Only)⁸
Device Manager	6.3(2)
DCNM	6.3(2)

Before installation or configuration of any FCIP hardware or components it should be validated by the FCIP implementer that all hardware and software types are listed in the above certified hardware and component matrix. Any hardware or software versions not listed in the above matrix will not be supported by CSBE.

¹ The MDS-9509 is now EOL. EOS date is currently listed as 4/30/2019

² The MDS-9216i is now EOL and EOS. Any FCIP deployments still using these in production, should tech refresh to a supported configuration.

³ The MDS-9222i is now EOL. EOS date is currently listed as 4/30/2020

⁴ The 10Gb MDS9250i switch is newly certified with this project. All future FCIP installs or tech refreshes should be completed using this switch.

⁵ No testing for the 18/4 MSM or SSN-16 was completed as part of this project. A critical VTM forced new code NX-OS 5.2(8e) to be loaded before testing could occur. CSBE relied solely on all FCIP testing completed by Cisco for these line cards.

⁶ No testing on NX-OS 5.2(8e) was completed as part of this project. See the above note.

⁷ All testing on the MDS-9250i was completed using NX-OS 6.2(11). Code 6.2(11b) was as a result of a VTM after the project testing was closed. It was validated by Cisco that no FCIP changes occurred between their code drops.

⁸ All testing on the MDS-9250i was completed using NX-OS 6.2(11). Code NX-OS 6.2(11) should ONLY be loaded on the MDS-9250i. It should not be loaded on any other MDS models shown in the component matrix.

9 Best Practices

FCIP administrators should understand all of the following best practices prior to ordering, installing, or configuring the new MDS-9250i.

9.1 MDS 9250i

The base MDS-9250i configuration comes with (20) 16Gb FC ports and (2) 10Gb Ethernet ports. The base configuration of (20) FC ports can be upgraded in place, or ordered up to (40) FC ports. Since most current arrays are still using 8Gb RA ports, FCIP administrators should calculate how many FC ports they need prior to ordering. The MDS-9250i should be used for all new deployments and tech refreshes.

9.2 VSANs

VSANs are a group of switch ports on the same switch (local VSAN) or spread across multiple switches at the same site (cross-switch VSAN), or spread across multiple switches and sites (cross-site VSAN). Cross-site VSANs will be the best practice for all FCIP replication environments. These cross-site VSANs should include a small number (8-12) of DMX RAs in each VSAN.

VSAN IDs are required for each VSAN that will be created. VSAN IDs 500 through 799 should be used when creating FCIP VSANs (Cross-Site).

9.3 Inter VSAN Routing (IVR)

IVR uses a transit VSAN between two local VSANs on different switches. This transit VSAN will route traffic between the two local VSANs and segregate any type of fabric events from being routed to the other VSAN. Although IVR adds this type of functionality it also adds a layer of complexity to the SAN and it will no longer be certified for FCIP.

9.4 VSAN Domain ID's

When a cross-switch or cross-site VSAN is created it will require that 2 domain IDs be used (one for each switch or one for each site). When VSANs are created they should always use static domain IDs that are unique across both sites.⁹ These domain IDs should also be consistent with Citi SAN standards such as all even Domain IDs on the "A" fabric and all odd Domain IDs on the "B" fabric (ex: If the cross-site VSAN spans across "A" fabric switches then "A" fabric domain IDs should be used).

⁹ Failure to have a unique domain ID across both sites will not allow the two sites to join. The two sites would be segmented until unique Domain IDs are used.

9.5 Port-Channels

Cisco MDS FCIP Solutions provide Port-Channeling which allows implementers to bundle FCIP GigE interfaces into one big pipe which alleviates the need to manually lay out cross-site zones for load balancing and performance purposes.

Port-Channels¹⁰ refer to the aggregation of multiple physical interfaces into one logical interface to provide higher aggregated bandwidth, load balancing, and link redundancy. Port-Channels can connect to interfaces across switching modules, so a failure of a switching module cannot bring down the Port-Channel link. It will be considered a best practice to put all FCIP Tunnels into port-channels.

9.6 Write Acceleration

The FCIP write acceleration feature enables FCIP implementers and designers 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. It will be a CSBE best practice to have write acceleration enabled for all FCIP interfaces.

9.7 Compression

The FCIP compression feature allows IP packets to be compressed on the FCIP GigE interface if it is enabled. Compression is considered a CSBE best practice and should be enabled and placed in “**mode 2**”. By default the FCIP compression is disabled. Once enabled, the software defaults to using the **auto** mode.

9.8 IPSEC Encryption

With the introduction of the 18/4 multi-protocol services module, both hardware compression and hardware encryption have been incorporated in to a single service module. As such, it is currently possible to natively compress and encrypt the FCIP data without any additional VPN Acceleration Modules (VAM) in the switches. Encryption algorithms that are supported are AES, DES, 3DES with SHA-1, MD5-HMAC and AES-XCBCMAC. However, due to its inherent weakness, DES is not recommended for storage applications.

¹⁰ MDS FCIP Port-Channels are **NOT** the same as Cisco Routers Ether-Channels. When connecting MDS FCIP GigE interfaces to an intermediate Cisco Routers, the Network Engineers should **NOT** configure Ether-Channeling for the FCIP connections coming into the router. The FCIP connections should be treated as separate GigE interfaces at the router that already has load balanced data coming across. On the Cisco Routers these FCIP interfaces should be treated just like a server connection.

The Cisco best practice is to compress the data prior to encryption because encrypted data tends to compress very poorly. Although IPSEC encryption is certified by CSBE it should only be deployed for application and environments that require encryption since it limits throughput into the GigE interfaces. Administrators enabling IPSEC should use AES as the encryption type with a 256bit key and SHA for authentication.

9.9 Jumbo Frames

Without jumbo frames enabled Cisco FCIP uses an MTU size of 1500 which means that every Fiber Channel packet will be split into 2 IP packets. In order to get a single Fiber Channel frame into a single IP packet, CSBE recommends jumbo frame sizes of 2300 bytes with encryption disabled, and 2500 bytes if encryption is enabled. Setting the MTU size higher will only fill the IP packet with empty space.

Citi Global Network Engineering does not support Jumbo Frames on the shared Citi networks, but does support Jumbo Frames on dedicated replication networks. As a result, CSBE will consider Jumbo Frames MTU set to 2300 (or 2500 if encryption is enabled) a best practice when running on dedicated replication networks. *If for any reason the Regional Network teams will not support Jumbo Frames on dedicated replication networks, the FCIP implementer should not attempt to use them.*

9.10 Dedicated FCIP Bandwidth (Replication)

CSBE and Global Network Engineering, recommends using dedicated bandwidth for all ongoing data replication environments (ex: SRDF/A or HUR). Dedicated bandwidth means bandwidth supplied by Citi networking that is not shared with normal traffic. Dedicated bandwidth will still be considered dedicated even if it is shared with other replication projects using different FCIP equipment. On dedicated bandwidth Jumbo Frames should be enabled in order to achieve higher throughput.

9.11 Shared FCIP Bandwidth (Data Migration)

CSBE recommends that all data migrations take place on the normal shared Citi network with Jumbo Frames disabled. When using shared Bandwidth for data migrations the FCIP administrators should inform their local applied network engineering team of when data migrations will start, how much bandwidth they will consume, and how long the migration will take.

9.12 FCIP Tunnel/Profile Max Bandwidth

This value determines the maximum bandwidth that an FCIP GigE port can run at. This value should be calculated using the formula given in the [Appendix A: Determining FCIP GigE max-bandwidth-mbps](#) section of this document.

9.13 FCIP Tunnel/Profile Min Bandwidth

This value represents the minimum amount of bandwidth in the FCIP path that you expect to be always available. This value determines the aggressiveness of FCIP recovery — a higher value is more aggressive, a lower value is less aggressive. A value that is too high can cause congestion and packet drops for any traffic traversing shared network links.

Bandwidth allocation strongly favors the FCIP traffic when mixed with conventional TCP traffic, which recovers from drops more slowly. To cause FCIP to behave more fairly, use a lower value for min-bandwidth. FCIP will start at a lower rate and increment the send rate every Round Trip Time (RTT), just like a classic TCP slow start.

The CSBE best practice is to set this value to 80% of max-bandwidth on all dedicated replication FCIP bandwidth. For shared FCIP bandwidth this parameter should be set to 75% of the max-bandwidth value.

9.14 FCIP Tunnels per GigE Interface

An FCIP tunnel is basically an ISL that is carried over the IP network. From an IP networking perspective, each FCIP Tunnel requires a pair of static IP addresses and TCP ports with the TCP port number defaulting to 3225.

FCIP tunnels appear as virtual E_Ports (or TE_Ports if carrying VSANs) between the Cisco MDS switches on the local and remote sites. By adding additional FCIP tunnels, one is effectively adding additional equal-cost paths between the two data centers. These equal-cost paths can be used by the Fibre Channel FSPF routing protocol for load-balancing and recovery purposes.

It will be a CSBE best practice to build (6) FCIP tunnels on each 10 GigE port using the same IP address for each but using different TCP Port numbers (Port #300-305). **The total of the (6) FCIP tunnels max bandwidth settings should NOT exceed 6000 Mb (Megabits) because of the [known limitation](#) of the MDS-9250 discussed in the Release Notes Document.**

9.15 FCIP QOS

QOS (Quality of Service) can be configured down to the individual zone level. The three levels that are supported are low, medium, and high. FCIP implementers requiring higher levels of service for certain replication groups in a replication environment can use QOS at the zone or VSAN level to enforce this behavior.

9.16 IP ACLs

IPv4 Access Control Lists (IPv4-ACLs) can provide basic network security to all MDS FCIP GigE Interfaces. IPv4-ACLs restrict IP-related traffic based on the configured IP filters. A filter contains the rules to match an IP packet, and if the packet matches, the rule also stipulates if the packet should be permitted or denied. CSBE recommends creating IP ACLs for each FCIP GigE interface pair allowing all TCP traffic. An ACL should also be created for each pair allowing all IP traffic so that troubleshooting tools such as ping and measure-rtt will work on the FCIP GigE connections.

10 Planning/Installation/Configuration Checklist

The following steps should be followed in the order given to get FCIP properly installed and configured.

Planning Steps:

- ✓ [Determine Number of Required FC Ports](#)
- ✓ [Determine the Number of GigE Ports into Bandwidth](#)
- ✓ [Determine Amount of Data to Replicate](#)
- ✓ [Determine the Number of MDS-9250i](#)
- ✓ [Determine if ATS is Required in Purchase Order](#)
- ✓ [Order MDS-9250i Switches](#)
- ✓ [Open a Network PIF](#)

Installation Steps:

- ✓ [Validate the MDS-9250i Installation](#)

Configuration Steps:

- ✓ [Discover Remote Site MDS in Local Fabric Manager](#)
- ✓ [Enable FCIP on All MDS Switches](#)
- ✓ [Setup GigE interfaces](#)
- ✓ [Setup Static Routes](#)
- ✓ [Get RTT Times](#)
- ✓ [Create FCIP Profiles and FCIP Interfaces](#)
- ✓ [Put FCIP Interfaces in a Port-Channel](#)
- ✓ [Make Cross-Site VSAN](#)
- ✓ [Add Cross-Site VSAN to Port-Channel](#)
- ✓ [Enable Enhanced Zoning](#)
- ✓ [Create Zones and Zoneset](#)
- ✓ [Check Zoning Connectivity](#)
- ✓ [Enable IP ACLs](#)
- ✓ [Enable IPsec Encryption \(Optional\)](#)

11 Planning Steps

Planning steps for a new MDS-9250i should start several months prior to the installation. Without any escalations these planning steps could take 8-12 weeks.

11.1 Determine Number of Required FC Ports

The number of FC ports required in each deployment is important because it will determine the following items when ordering the MDS-9250i switches:

- If the MDS-9250i base config (20 FC ports only) can be used, or if it should be ordered with 40 FC ports.
- If the number of FC ports for either the A or B fabric exceeds 40, then it will determine that multiple MDS-9250i switches be ordered per site.

If the FCIP deployment is part of a tech refresh, the number of FC ports would simply be determined by adding together the current number of FC ports being used in the existing 18/4 MSM cards or MDS-9222i and adding growth. If the FCIP deployment is new, then the number of Array RA ports that will be connected to the MDS-9250i switches will have added to the number of FC ports required for growth.

11.2 Determine Number of GigE Ports into Bandwidth

The Number of GigE ports plugging into the Network Circuits on the A and B SANs is important and will determine the following:

- Number of MDS-9250i switches required
- The Max Bandwidth parameter of each FCIP Tunnel on GigE ports

For every FCIP deployment, both 10 GigE ports on all MDS-9250i switches will be plugged into the same Fabric Circuits. On an A Fabric 9250i, both GigE ports would plug into A Fabric WAN circuits.

Note: Due to limitation on the MDS-9250i, each 10Gb port is limited to 6Gb. See [Release Notes document Known Issues](#) for further details.

11.3 Determine the Amount of Traffic to Replicate

If the FCIP deployment is part of a tech refresh, the amount of traffic being replicated can be found by looking at historical MDS FCIP data. If the FCIP deployment is new then the amount of data that will be replicated by each array would have to be determined using that array vendors or application owners process.

Each replication application should have its own documented process for determining the amount of bandwidth it requires. All SRDF/A applications should use the [V-MAX SRDF/A Solution Qualification Process \(Section 4.3\)](#) in the SRDF/A Solutions Guides. All HUR applications should use the [HDS/VSP/HUS VM Remote Replication Solutions Guide \(Sections 4\)](#)

11.4 Determine the Number of MDS-9250i Switches

With the availability of 10Gb bandwidth in Citigroup, the number of GigE ports required for bandwidth should not come into play any longer. However, there are a few items that will determine the number of MDS-9250i switches to be ordered for an FCIP deployment.

- A minimum of (4) switches per deployment must be ordered.
- If the number of required FC ports exceeds 80 at a site, then (8) switches would be needed.

A minimum number of (4) MDS-9250i switches should be used for each FCIP deployment. That would be (1) MDS-9250i for the A and B fabric at each site. This would allow ~24Gb¹¹ of throughput from each site into the Replication WAN circuits, and allow for (80) FC ports for replication.

More switches at each site should only be considered if either the required number of FC ports exceeds (80) or if the total amount of replication bandwidth required exceeds ~24Gb from one site to the other. If it is determined that more MDS-9250i switches are needed, they should only be ordered in groups of (4) to keep the A and B fabrics balanced at each site.

11.5 ATS for MDS-9250i Datacenter Installation

An Automatic Transfer Switch is designed to provide redundant power to connected equipment. The ATS is connected to two AC input sources and can provide seamless power transfer from one input source to the other in the event that one source becomes unavailable. The transfer time from one input source to the other occurs quickly and safely so that there is no disruption to the connected devices thereby providing redundant power to single corded devices (e.g., power supplies)

11.5.1 MDS 9250i Power Supplies

The MDS 9250i has three power supplies and operates in 2+1 redundancy mode which means that two power supplies are required to operate the system and

¹¹ Due to a limitation in the MDS-9250i, there is a throughput limitation on each MDS-9250i 10Gb port to ~6Gb throughput. See Release Notes for more information about this limitation. All calculations pertaining to 9250i GigE ports should not exceed 6Gbps per 10 Gb interface.

one is an active spare. In many data centers, power is provided to racks in a fully redundant configuration using two sources: Grid A and Grid B. If power grid redundancy is required, an Automatic Transfer Switch (ATS) can meet this requirement. The ATS solution provides redundant power to the 9250i standby power supply making it available in the event of a power failure on either grid. The solution consists of attaching one of the MDS 9250i power supplies to an ATS and attaching power sources from both grids to the ATS. With this configuration, the standby power supply will remain powered-up if either grid fails. The ATS transfer time from one input source to the other input source occurs in 8-12 milliseconds (typically, and 16 ms max) and therefore is non-disruptive to the MDS 9250i. Typical power supplies, including the MDS 9250i power supplies, will operate for at least 20 milliseconds after the input voltage drops to zero. When power from one grid fails, the MDS 9250i will remain up using power from the other grid together with power from the ATS switch which is powered by both grids.

As a result of non-redundant grid power, implementers of the MDS-9250i should first ask the datacenter personnel if they can provide the ATS for installation. If the datacenter is unable to provide the ATS, then it should be added as a line item in the Purchase Order for the MDS-9250i. See the [Release Notes Document](#) Known Issues section for more detail on this issue.

11.6 Order the MDS-9250i Switches

Once all of the information from the previous sections is known, the MDS-9250i switches should be ordered. When ordering the MDS-9250i switches, it is important to remember that base configuration will only come with (20) FC ports. If more than 20 FC ports are required per switch then the high density configuration should be ordered that comes with (40) FC ports. It must also be known if an ATS (see previous sections) should be ordered from the vendor with the MDS-9250i.

11.7 Open a Network PIF

After all the FCIP and application information is known, a Network PIF will need to be opened to engage the local Applied Network Engineering team. The PIF will contain all details needed to build the IP network that the MDS FCIP GigE ports will connect to. Since the process for Opening a network PIF is highly regionalized, each regional FCIP implementer should use their regional process for initiating a project with their local applied network engineering team.

Once the Network PIF is opened, the Applied Network Engineering Team will work with the FCIP implementer to validate the PIF requirements, bandwidth needs, and network redundancy needed. After the configuration is validated and checked, the Applied Network Group will order any network equipment (if

necessary) and network circuits (if necessary) for the project. It can take up to 3 months for all equipment and network circuits to be delivered.

12 Installation

As a result of FCIP being a pre-installed component of the Cisco MDS NX-OS operating system, there are no specific installation instructions for FCIP. All instructions for installing a complete Cisco MDS (which includes FCIP) are shown in the [Cisco MDS Solutions Guide](#).

The MDS-9250i switch should be turned over to the FCIP administrators fully installed and fully integrated into all Citigroup compliance systems. At this point FCIP administrator should be able to log into the MDS-9250i using their SOE ID as a validation.

13 Configuration

For this release of FCIP, there are major changes in the design and the configuration. This is due to the certification of the MDS-9250i 10Gb FCIP switches. As a result of the new MDS-9250i administrators can expect the following major changes to the design and configuration.

- Far fewer GigE ports will be required to support replication from one data center to the other.
- Multiple FCIP tunnels will now be used across each GigE interface
- Multiple FCIP tunnels will be realized by using different TCP ports on the same GigE IP addresses as opposed to using sub-interfacing

As a result of FCIP going from 1Gb to 10Gb, readers of this document should read the [Best Practices](#) section of this document prior to starting the configuration of a new MDS-9250i.

All CLI commands given in this configuration section will be based on the LAB test environment depicted in the diagram below. All implementer should get their specific IP Addresses and subnet masks from the network administrator working the PIF.

Note: The following LAB example only simulates an A Fabric. In production these same configuration commands would also have to be completed on the B fabric switches.

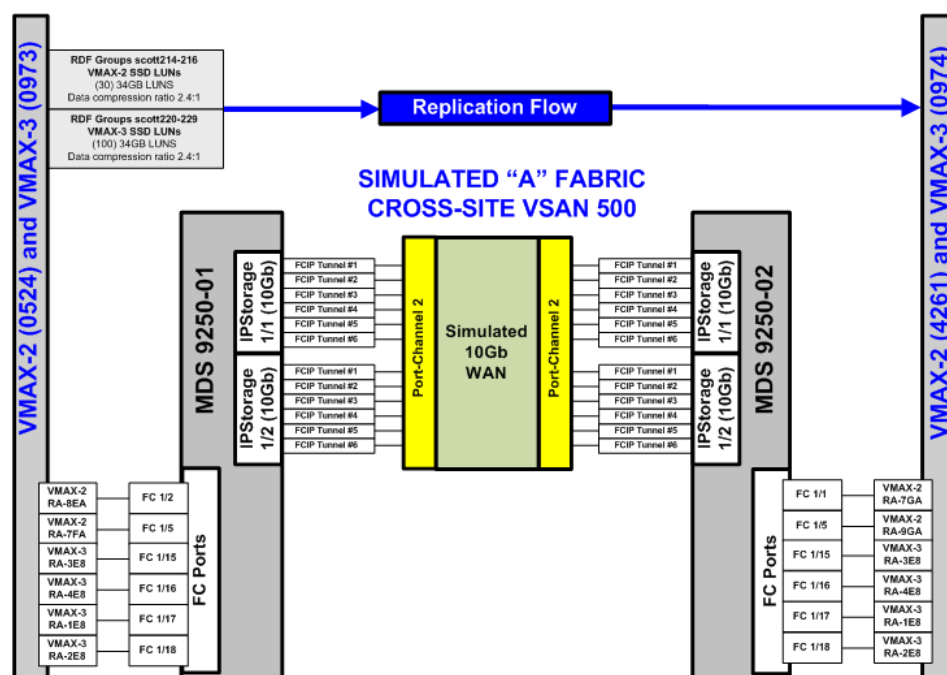


Figure 1 - CLI Example Diagram

13.1 Discover Remote Site 9250i in DCNM

Note: Prior to discovering the remote site MDS on the Local Fabric Manager, the FCIP Administrator should do the following: **1 – Validate that the remote MDS switches that will be discovered have the same admin password as the local MDS.** **2 – Add the local DCNM and MDS IP Addresses to the ACL list on the remote MDS management port that will be discovered.**

This step will get all MDS switches that will participate in the FCIP configuration on the same Cisco DCNM view. On the DCNM where the FCIP configuration will be managed, discover the remote site MDS using the following steps (this process assumes the local MDS has already been discovered).

Launch Fabric Manager and log in.

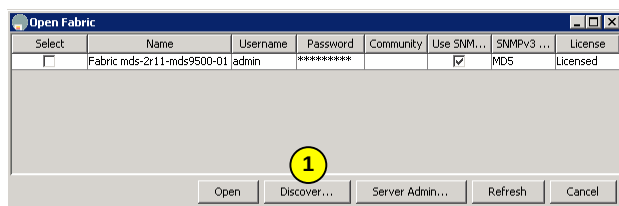


Figure 2 – Open Fabric Screen

1. Hit the *Discover* button and the following screen will appear



Figure 3 – Discover Fabric Screen

1. Enter the Management port IP Address of the remote site MDS
2. Enter the password for the remote MDS
3. Hit the *Discover* button and the following screen will appear.

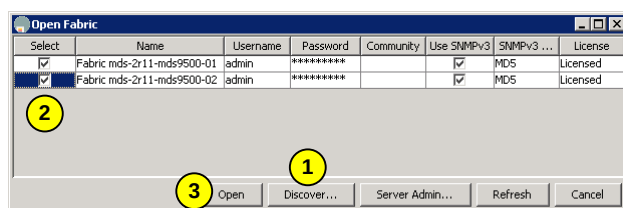


Figure 4 – Open Fabric Screen

1. Continue to discover all remote MDS until all are listed in DCNM.
2. Once all MDS at remote sites are discovered, put a check in each MDS checkbox so that all will appear in DCNM.
3. Hit the open button and DCNM will open and should display icons for all MDS switches/directors that were discovered.

13.2 Enable FCIP Feature

Note: All of the following CLI commands are given in a format that they could be run in the DCNM *Tools->Run_CLI_Commands* window

In order to create FCIP Interfaces and Tunnels the following commands must be run on all MDS-9250i switches at both the local and remote sites.

```
conf t
fcip enable
exit
```

13.3 Setup GigE Interfaces

After the FCIP feature is enabled on all switches the next step would be to configure each GigE port on all switches at both the Local and Remote Sites using the following CLI commands.

Local Site Switch Commands:

```
conf t

interface IPStorage 1/1
ip address 10.98.10.50 255.255.255.0
switchport mtu 2300
shut
no shut
exit

interface IPStorage 1/2
ip address 10.98.20.50 255.255.255.0
switchport mtu 2300
shut
no shut
exit
```

```
exit
```

Remote Site Switch Commands:

```
conf t

interface IPStorage 1/1
ip address 10.98.15.50 255.255.255.0
switchport mtu 2300
shut
no shut
exit

interface IPStorage 1/2
ip address 10.98.25.50 255.255.255.0
switchport mtu 2300
shut
no shut
exit
exit
```

13.4 Setup Static Routes

After the GigE ports are configured, static routes should be setup on all MDS switches at both the local and remote site. Note that the routes of each switch are configured to use the remote switch.

Local Site Switch Commands:

```
conf t
ip route 10.98.15.50 255.255.255.255 interface IPStorage 1/1 distance 1
ip route 10.98.25.50 255.255.255.255 interface IPStorage 1/2 distance 1
exit
```

Remote Site Switch Commands:

```
conf t
ip route 10.98.10.50 255.255.255.255 interface IPStorage 1/1 distance 1
ip route 10.98.20.50 255.255.255.255 interface IPStorage 1/2 distance 1
exit
```

13.5 Get RTT Times

The RTT (Round Trip Time) between the local and remote sites will need to be known in order to configure the FCIP profiles. To find the RTT time between the 10 GigE pairs, these commands need only be run on the local site switch.

Local Site Switch Commands:

```
# ips measure-rtt 10.98.15.50 interface IPStorage 1/1
Round trip time is 27 micro seconds (0.03 milli seconds)

# ips measure-rtt 10.98.25.50 interface IPStorage 1/2
Round trip time is 26 micro seconds (0.02 milli seconds)
```

Note: In the above output, the micro seconds number should be used when configuring the FCIP tunnels. Use the highest value of all the FCIP pairs. In the above example that would be 27 micro seconds.

13.6 Setup FCIP Profiles and Interfaces

Now (6) FCIP profiles and (6) FCIP interfaces need to be setup for each 10 GigE port on each switch at both the local and remote sites. Note that in the output below that each profile and interface uses the same IP address but a different port is used. Note also that here the RTT time is used from the previous step..

Note: In the following commands the max-bandwidth parameter was calculated as 10000Mbps / (12) FCIP tunnels going across = 833 (rounded down to 830Mbps). See [Appendix A](#) for more detailed explanation.

FCIP Tunnels and Interfaces for Local Site Switch GigE Port #1

```
conf t

fcip profile 1
ip address 10.98.10.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 300
exit

interface fcip 1
use-profile 1
peer-info ipaddr 10.98.15.50 port 300
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 2
ip address 10.98.10.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 301
exit

interface fcip 2
use-profile 2
peer-info ipaddr 10.98.15.50 port 301
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 3
```

```
ip address 10.98.10.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 302
exit

interface fcip 3
use-profile 3
peer-info ipaddr 10.98.15.50 port 302
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 4
ip address 10.98.10.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 303
exit

interface fcip 4
use-profile 4
peer-info ipaddr 10.98.15.50 port 303
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 5
ip address 10.98.10.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 304
exit

interface fcip 5
use-profile 5
peer-info ipaddr 10.98.15.50 port 304
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 6
ip address 10.98.10.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 305
exit

interface fcip 6
use-profile 6
```

```
peer-info ipaddr 10.98.15.50 port 305
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

exit
```

FCIP Tunnels and Interfaces for Local Site Switch GigE Port #2

```
conf t

fcip profile 7
ip address 10.98.20.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 300
exit

interface fcip 7
use-profile 7
peer-info ipaddr 10.98.25.50 port 300
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 8
ip address 10.98.20.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 301
exit

interface fcip 8
use-profile 8
peer-info ipaddr 10.98.25.50 port 301
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 9
ip address 10.98.20.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 302
exit

interface fcip 9
use-profile 9
peer-info ipaddr 10.98.25.50 port 302
switchport trunk mode on
ip-compression mode2
```

```
write-accelerator
no shut
exit

fcip profile 10
ip address 10.98.20.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 303
exit

interface fcip 10
use-profile 10
peer-info ipaddr 10.98.25.50 port 303
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 11
ip address 10.98.20.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 304
exit

interface fcip 11
use-profile 11
peer-info ipaddr 10.98.25.50 port 304
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 12
ip address 10.98.20.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 305
exit

interface fcip 12
use-profile 12
peer-info ipaddr 10.98.25.50 port 305
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

exit
```

FCIP Tunnels and Interfaces for Remote Site Switch GigE Port #1

```
conf t

fcip profile 1
ip address 10.98.15.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 300
exit

interface fcip 1
use-profile 1
peer-info ipaddr 10.98.10.50 port 300
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 2
ip address 10.98.15.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 301
exit

interface fcip 2
use-profile 2
peer-info ipaddr 10.98.10.50 port 301
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 3
ip address 10.98.15.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 302
exit

interface fcip 3
use-profile 3
peer-info ipaddr 10.98.10.50 port 302
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 4
ip address 10.98.15.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 303
```

```
exit

interface fcip 4
use-profile 4
peer-info ipaddr 10.98.10.50 port 303
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 5
ip address 10.98.15.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 304
exit

interface fcip 5
use-profile 5
peer-info ipaddr 10.98.10.50 port 304
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 6
ip address 10.98.15.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 305
exit

interface fcip 6
use-profile 6
peer-info ipaddr 10.98.10.50 port 305
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

exit
```

FCIP Tunnels and Interfaces for Remote Site Switch GigE Port #2

```
conf t

fcip profile 7
ip address 10.98.25.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 300
exit

interface fcip 7
```

```
use-profile 7
peer-info ipaddr 10.98.20.50 port 300
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 8
ip address 10.98.25.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 301
exit

interface fcip 8
use-profile 8
peer-info ipaddr 10.98.20.50 port 301
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 9
ip address 10.98.25.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 302
exit

interface fcip 9
use-profile 9
peer-info ipaddr 10.98.20.50 port 302
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 10
ip address 10.98.25.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 303
exit

interface fcip 10
use-profile 10
peer-info ipaddr 10.98.20.50 port 303
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit
```

```

fcip profile 11
ip address 10.98.25.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 304
exit

interface fcip 11
use-profile 11
peer-info ipaddr 10.98.20.50 port 304
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

fcip profile 12
ip address 10.98.25.50
tcp max-bandwidth-mbps 830 min-available-bandwidth-mbps 660 round-trip-
time-us 27
port 305
exit

interface fcip 12
use-profile 12
peer-info ipaddr 10.98.20.50 port 305
switchport trunk mode on
ip-compression mode2
write-accelerator
no shut
exit

exit

```

13.7 Put FCIP Interfaces in a Port-Channel

Once the FCIP profiles and interfaces have been created, the FCIP interfaces now need to be added to a port-channel at both the local and remote sites using the following CLI commands.

Local Site and Remote Site Switch Commands:

```

conf t

interface fcip1, fcip2, fcip3, fcip4, fcip5, fcip6, fcip7, fcip8,
fcip9, fcip10, fcip11, fcip12
channel-group 2
exit

exit

```

13.8 Make Cross-Site VSAN

Now the Cross-Site VSAN should be created on both the local site and remote site switches. Use the following CLI commands to create the Cross-Site VSAN.

Local Site Switch Commands:

```
conf t

vsan database
vsan 500 name ReplicationA_VSAN suspend
exit

fcdomain domain 200 static vsan 500

vsan database
no vsan 500 suspend
vsan 500 interface fc1/2, fc1/5, fc1/15, fc1/16, fc1/17, fc1/18
y
y
y
y
y
y
y
y
y
exit

exit
```

Remote Site Switch Commands:

```
conf t

vsan database
vsan 500 name ReplicationA_VSAN suspend
exit

fcdomain domain 201 static vsan 500

vsan database
no vsan 500 suspend
vsan 500 interface fc1/1, fc1/5, fc1/15, fc1/16, fc1/17, fc1/18
y
y
y
y
y
y
y
y
y
y
exit

exit
```

13.9 Add Cross-Site VSAN to Port-Channel

Once the Cross-Site VSAN has been created it should now be added to the Port-Channel on both the local and remote site switches using the following CLI commands.

Local Site and Remote Site Switch Commands:

```
conf t

interface port-channel 2
switchport trunk mode on
switchport trunk allowed vsan 1 no-warning
switchport trunk allowed vsan add 500
exit

interface fcip1, fcip2, fcip3, fcip4, fcip5, fcip6, fcip7, fcip8,
fcip9, fcip10, fcip11, fcip12
shut
no shut
exit

interface port-channel 2
shut
no shut
exit

exit
```

13.10 Enable Enhanced Zoning

After all FCIP configurations are complete, enhanced zoning should be enabled for both the local and remote site switches using the following CLI commands.

Local and Remote Site Switch Commands:

```
conf t
system default zone mode enhanced
exit
```

13.11 Create Zones and Zoneset

After enhanced zoning has been enabled, now all the Zones and the Zoneset for each Cross-Site VSAN on both the A and B Fabric should be created using the following CLI commands.

Note: Zone and Zoneset creation commands should only be run on the local site switches for both the A and B fabric.

Local Site Switch Commands:

```
conf t

zone name RDF0524-8E__RDF4261-7G vsan 500
member pwnn 50:00:09:73:00:08:31:1c
```

```

member pwnn 50:00:09:72:08:42:95:98
exit

zone name RDF0524-7F__RDF4261-9G vsan 500
member pwnn 50:00:09:73:00:08:31:58
member pwnn 50:00:09:72:08:42:95:a0
exit

zone name RDF0973-1E8__RDF0974-1E8 vsan 500
member pwnn 50:00:09:73:50:0f:34:08
member pwnn 50:00:09:73:50:0f:38:08
exit

zone name RDF0973-2E8__RDF0974-2E8 vsan 500
member pwnn 50:00:09:73:50:0f:34:48
member pwnn 50:00:09:73:50:0f:38:48
exit

zone name RDF0973-3E8__RDF0974-3E8 vsan 500
member pwnn 50:00:09:73:50:0f:34:88
member pwnn 50:00:09:73:50:0f:38:88
exit

zone name RDF0973-4E8__RDF0974-4E8 vsan 500
member pwnn 50:00:09:73:50:0f:34:c8
member pwnn 50:00:09:73:50:0f:38:c8
exit

zoneset name FCIP_RDF_Fabric vsan 500
member RDF0524-8E__RDF4261-7G
member RDF0524-7F__RDF4261-9G
member RDF0973-1E8__RDF0974-1E8
member RDF0973-2E8__RDF0974-2E8
member RDF0973-3E8__RDF0974-3E8
member RDF0973-4E8__RDF0974-4E8
exit

zoneset activate name FCIP_RDF_Fabric vsan 500

exit

exit

```

13.12 Check Zoning Connectivity

After the cross-site VSAN is activated everything that is needed for Data Migration or Replication connectivity should be in place. At this point that connectivity should be checked for all zones that span across the local and remote sites. Launch DCNM and from the main screen select Tools, Connectivity, and then End to End Connectivity from the pull-down menus and the following screen will appear.

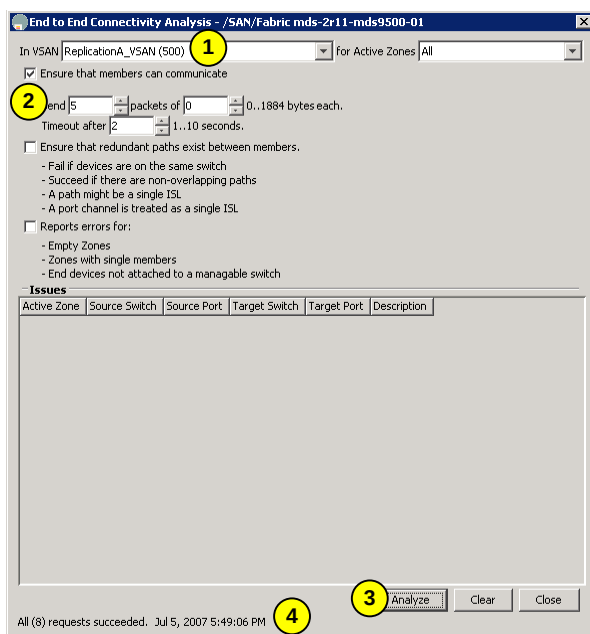


Figure 5 – End to End Connectivity Screen

1. Select the cross-site VSAN in the pull-down menu.
2. Leave all of these values at default.
3. Hit the *Analyze* button.
4. The test will run for a few minutes and the results will then be displayed in the section at the bottom of the screen. If all tests succeeded then all connectivity is complete.

13.13 Enable IP ACLs

IP ACLs should be entered on a GigE port basis. This means that each GigE interface will have (2) IP ACLs that have (2) IP addresses in them. The first ACL would list the local GigE port IP listed first followed by the remote GigE port IP listed second. The second ACL would be the reverse of the first ACL in that it would list the remote GigE port IP first followed by the local GigE port IP.

The commands below are based on the diagram shown below, which is a slightly more detailed diagram, than the one given at the beginning of the configuration section of this document.

Note: that this diagram only shows the A fabric which means commands shown in this example are only run on (1) switch at each site. In a real production environment the commands would be run on the A and B fabric switches which would be (2) switches at each site.

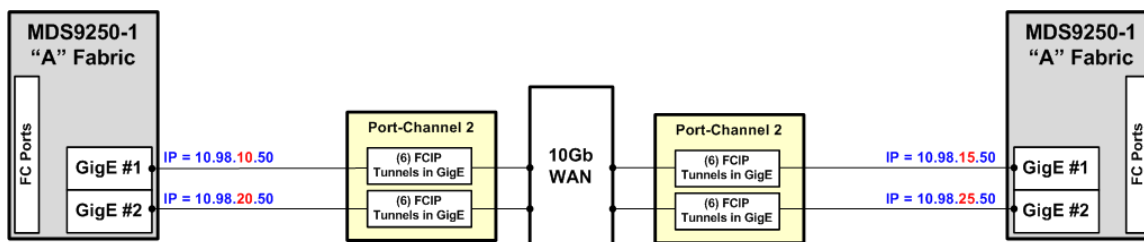


Figure 6 - IP ACLs Example Diagram

Note: Extreme caution should be taken when enabling ACLs and only GigE port pair at a time should be enabled to prevent dropping the whole port channel if a mistake occurs.

Use the following commands on both the local and remote MDS switches to enable IP ACLs on the GigE interfaces.

Local Site Switch Commands For GigE Port #1

```
conf t

ip access-list FCIPGigE1 permit ip 10.98.10.50 0.0.0.0 10.98.15.50
0.0.0.0
ip access-list FCIPGigE1 permit ip 10.98.15.50 0.0.0.0 10.98.10.50
0.0.0.0

interface IPStorage 1/1
ip access-group FCIPGigE1
shut
no shut
exit

exit
```

Remote Site Switch Commands For GigE Port #1

```
conf t

ip access-list FCIPGigE1 permit ip 10.98.15.50 0.0.0.0 10.98.10.50
0.0.0.0
ip access-list FCIPGigE1 permit ip 10.98.10.50 0.0.0.0 10.98.15.50
0.0.0.0

interface IPStorage 1/1
ip access-group FCIPGigE1
shut
no shut
exit

exit
```

After the First GigE port pair has been completed and both GigE ports are back online, then the second GigE port on each switch can be completed using the following CLI commands.

Local Site Switch Commands For GigE Port #2

```
conf t

ip access-list FCIPGigE2 permit ip 10.98.20.50 0.0.0.0 10.98.25.50
0.0.0.0
ip access-list FCIPGigE2 permit ip 10.98.25.50 0.0.0.0 10.98.20.50
0.0.0.0

interface IPStorage 1/2
ip access-group FCIPGigE2
shut
no shut
exit

exit
```

Remote Site Switch Commands For GigE Port #2

```
conf t

ip access-list FCIPGigE2 permit ip 10.98.25.50 0.0.0.0 10.98.20.50
0.0.0.0
ip access-list FCIPGigE2 permit ip 10.98.20.50 0.0.0.0 10.98.25.50
0.0.0.0

interface IPStorage 1/2
ip access-group FCIPGigE2
shut
no shut
exit

exit
```

13.14 Enable IPsec Encryption (Optional)

Due to the performance loss that can occur when encryption is enabled, it is only recommended for applications that require encryption. Currently, no FCIP instances of FCIP encryption could be found in production and as such the commands will not be included in the solutions guide. Any customer requiring encryption can contact CSBE and the commands will be given.

14 References

Document	Location
CSBE Cisco MDS – Main Page	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/ciscomds.aspx
Cisco MDS FCIP v7.0 – Project Scope	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/platforms/CiscoMDSFCSwitches/CSBE-15000-PS.pdf
Cisco MDS FCIP v7.0 – Release Notes	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/platforms/CiscoMDSFCSwitches/CSBE-15000-RN.pdf
Cisco MDS FC Switch Certification Solutions Guide	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/platforms/CiscoMDSFCSwitches/07002-sg_v4.8.pdf
Cisco MDS FC Switch Certification Release Notes	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/platforms/CiscoMDSFCSwitches/08002-rn_v3.2.pdf
SRDF/A for Long Distance Replication Solutions Guide	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/platforms/Symmetrix/09039-SG.pdf
HDS VSP/HUS VM Remote Replication	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/platforms/Tagmastore/CSBE-11072-SG.pdf

15 Appendices

15.1 Appendix A: Determining FCIP GigE max-bandwidth-mbps

In order to know what value to set for the FCIP GigE max-bandwidth-mbps (port speed), the following information must be known first.

1. Amount of total bandwidth
2. How many network circuits
3. How many FCIP tunnels will go across each network circuit

Once all of the above information is known, the Max Bandwidth (port speed) for each FCIP GigE port FCIP Tunnel can be calculated using the following formula:

$$\text{(Total Bandwidth on each Circuit) / (Number FCIP Tunnels on each Circuit)} \\ = \text{Port Speed for each GigE connection on the Pipe.}$$

Note: In the above formula, it is important to note that due to the MDS-9250i limitation that the total of ALL FCIP Tunnels on a single 10 GigE port cannot exceed 6000Mbps. (See [Release Notes Document](#) Known Issues Section for more detail). Meaning that using the CSBE best practice of (6) FCIP tunnels per 19 GigE port, the max-bandwidth parameter should not exceed 1000Mbps.

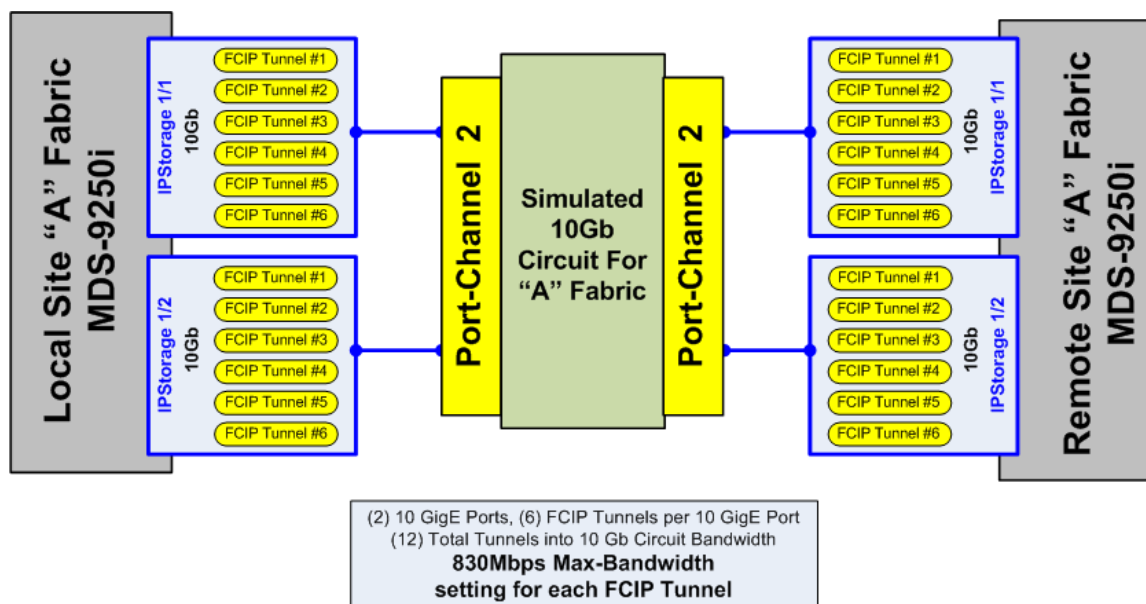


Figure 7 - Max-Bandwidth Example Diagram

10Gbps Bandwidth (or 10000 Mbps) / 12 Tunnels = 833 Mbps Max-Bandwidth (Rounded down to 830) setting for each FCIP Tunnel.