



**CATE Storage and Backup Engineering
Citi Architecture and Technology Engineering**

Cisco MDS SAN Switch

GDSE-07002-SG

Solutions Guide

Version 4.9

Version Control

Version	Date	Author	Reviewed	Comments
2.0	20-Feb-08	Kevin Hobaugh	Global Stakeholders	Changes to FM Server. Releasing document as v2.0. Certifying: SAN OS 3.2(1a) Fabric Manager 3.2(2c)
2.1	11-Apr-08	Kevin Hobaugh	Global Stakeholders	Corrected directory in Section 5 Modified Section 7: -IAS/Windows Local Auth -SHA/AES Modified Section 21 Appendix D. -Updated IP Access List for EMC SSH thru ESRS Modified Section 9: -Vendor Remote Access
2.2	8-Jul-08	Kevin Hobaugh	Global Stakeholders	- Minor addition to Section 21 Appendix D. Added command to disable link-state-trap on host interfaces. - Updated Section 17 Known Issues. Added bugs: (CSCso63759,CSCsq68599,CSCsm62681) - Updated Section 13.3 with note about port security issue. - Updated Section 23 Appendix F – revised show tech support commands - Added Section 5.10.1 with Active Directory back out instructions
2.3	21-Jul-08	Kevin Hobaugh	Global Stakeholders	- Minor addition: Section 7.7 Functional ID's, password change frequency - Updated Section 17 Known issues. Added bug: CSCsl97949
2.4	22-Aug-08	Kevin Hobaugh	Parul Jain	Peer Review SAN-OS 3.3(1c) Fabric Manager 3.3(1c)
2.5	25-Aug-08	Kevin Hobaugh	Global SAN Stakeholders	RFC
3.0	15-Sept-08	Kevin Hobaugh	Global SAN Stakeholders	Production SAN-OS 3.3(1c) Fabric Manager 3.3(1c) Modified: Section 5: Mgmt Server Build Section 6.6: Switch config, SANOS upgrade

Version	Date	Author	Reviewed	Comments
				Section 13: Port Security made Optional Section 16: Firmware upgrade/downgrade Wizard Appendix F: Revision History
3.1	20-Nov-08	Kevin Hobaugh	Gary Johnson	Peer Review - Added Secondary IAS Server -Created a shortcut to configure the Secondary IAS Server -Added local authentication as secondary to IAS/AD on the switches -Removed MSCHAP command. Using PAP <i>Revision Details in Appendix F.</i>
3.1	21-Nov-08	Kevin Hobaugh	Global SAN Stakeholders	RFC
3.2	5-Dec-08	Kevin Hobaugh	Global SAN Stakeholders	Production
3.3	19-Jan-10	Kevin Hobaugh	GDSE	Peer Review
3.3	12-Feb-10	Kevin Hobaugh	Global SAN Stakeholders	RFC
3.4	19-April-10	Kevin Hobaugh	Global SAN Stakeholders	Production NX-OS 4.2.1a & Fabric Mgr 4.2.3a
3.5	22-July-10	Kevin Hobaugh	Global SAN Stakeholders	Minor revision: Modified ACL's for SSH to allow "any any" after receiving Security Office approval.
3.6	24-Aug-10	Kevin Hobaugh	Global SAN Stakeholders	Minor revision: Newer version of Hi-Track (v5.1.0) released for switches purchased from HDS (SPAC: Htmr5110)
3.7	05-Dec-11	Kevin Hobaugh	GDSE	Peer Review Adding: NX-OS 5.2.1 Data Center Network Manager 5.2.1
3.8	22-Dec-11	Kevin Hobaugh	Global SAN Stakeholders	RFC: NX-OS 5.2.1 Data Center Network Manager 5.2.1
3.9	06-Jan-12	Kevin Hobaugh	Global SAN Stakeholders	Production NX-OS 5.2.1 Data Center Network Manager 5.2.1

Version	Date	Author	Reviewed	Comments
4.0	28-Feb-12	Kevin Hobaugh	Global SAN Stakeholders	Production Patch Fix for SNMP Timeout Issue
4.1	28-Dec-12	Kevin Hobaugh	Global SAN Stakeholders	Production Adding Security Review Findings and “required” modifications (Section 21) Added two additional Fabric design examples
4.11	30-July-13	Kevin Hobaugh	CSBE	Peer Review: NX-OS 5.2(8b) Modified SAN Design Tiers
4.2	2-Aug-13	Kevin Hobaugh	Global SAN Stakeholders	RFC
4.2	9-Aug-13	Kevin Hobaugh	Global SAN Stakeholders	RFP Added standalone install for Device Mgr and DCNM Client (bat files)
4.3	6-Nov-13	Kevin Hobaugh	Global SAN Stakeholders	-Modified Section 2.12.2 Added information on using the MDS 9148's for the Host Edge -Added Section 2.12.6 MDS 9148 Port Layout ISL/Host
4.4	18-Dec-13	Kevin Hobaugh	Global SAN Stakeholders	RFC NX-OS 5.2(8c)
4.4	17-Jan-14	Kevin Hobaugh	Global SAN Stakeholders	RFP NX-OS 5.2(8c)
4.5	06-Jun-14	Kevin Hobaugh	CSBE	Peer Review: NX-OS 5.2(8d) NX-OS 6.2(7) DCNM 6.3.1 MDS 9710 Director
4.5	09-Jun-14	Kevin Hobaugh	Global SAN Stakeholders	RFC: NX-OS 5.2(8d) NX-OS 6.2(7) DCNM 6.3.1 MDS 9710 Director
4.6	30-Jun-14	Kevin Hobaugh	Global SAN Stakeholders	RFP: NX-OS 5.2(8d) NX-OS 6.2(7) DCNM 6.3.2 MDS 9710 Director Adding NPV support for MDS 9148 New Large SAN Design (4-Core)

Version	Date	Author	Reviewed	Comments
4.6	18-Aug-14	Kevin Hobaugh	Global SAN Stakeholders	Minor change: Added sections to comply with GNAST certification efforts (Modified Section 1 and added Section 26)
4.7	3-Dec-14	Kevin Hobaugh	CSBE	Peer Review: MDS 9148s Certification NX-OS 6.2(9a) for MDS 9710, 9148 and 9148s NX-OS 5.2(8e) for MDS 9500 SANs
4.7	8-Dec-14	Kevin Hobaugh	Global SAN Stakeholders	RFC/RFP GNU Bash VTM fix
4.8	6-Feb-15	Kevin Hobaugh	Global SAN Stakeholders	RFC/RFP: Minor revision to port-channel numbers on the Host Edge switches
4.9	20-Mar-15	Kevin Hobaugh	Global SAN Stakeholders	Alert: VTM fix NX-OS 5.2(8f) / 6.2(11b) Inserted Section 26: “SeedSwitchUpdater” for changing from old seed switch to new seed switch HiTrack v7.1 (HDS Monitoring)

Legal Notice

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

CITI, CITIBANK, CITICORP, CITIGROUP and the Umbrella Device 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.

Contact

Please address any comments or questions regarding the information contained in this document via email to the “*CATE Storage and Backup Engineering” distribution list.

Latest Versions

It is recommended that the latest version of the document be used from the [CATE - Storage and Backup Engineering](#) website. Newer versions may include certification on additional platforms, or comments on issues discovered after deployment.

Regional Reviewers

Region	Reviewed By
Asia Pacific	
EMEA	
Japan	
Latin America/Mexico	
North America	

Table of Contents

1. INTRODUCTION	11
1.1. DOCUMENT PURPOSE	11
1.2. OWNER OF STANDARD	11
1.3. INTENDED AUDIENCE.....	11
1.4. PRINCIPLES	11
1.4.1. REVISION HISTORY.....	11
1.4.2. KEY FEATURE CHANGES	11
2. FABRIC DESIGN GUIDE (REQUIREMENTS).....	12
2.1. CERTIFIED MODELS AND SOFTWARE VERSIONS	12
2.2. COMMON HARDWARE AND SOFTWARE REQUIREMENTS	13
2.3. FABRIC TOPOLOGIES	13
2.3.1. SINGLE TIER (COLLAPSED CORE)	13
2.3.2. TWO TIER (CORE-EDGE)	13
2.3.3. THREE TIER (EDGE-CORE-EDGE)	14
2.3.4. N PORT VIRTUALIZATION	14
2.3.5. DUAL FABRICS	14
2.4. SCALABILITY CONSIDERATIONS	15
2.5. ISL DESIGN BEST PRACTICES	15
2.6. TAPE SANS	16
2.7. SAN ARCHITECTURE DESIGN EXAMPLES.....	16
2.7.1. SINGLE TIER SAN – SMALL (< 384 PORTS)	17
2.7.2. TWO TIER SAN (CORE-EDGE) – MEDIUM (< 4900 PORTS)	17
2.7.3. THREE TIER SAN (EDGE-CORE-EDGE)	19
2.7.3.1. DUAL CORE EDGE-CORE-EDGE – LARGE (< 6000 PORTS)	20
2.7.3.2. QUAD CORE EDGE-CORE-EDGE – XLARGE (<10,000 PORTS)	21
2.8. LINE CARD AND SWITCH LAYOUT	23
2.8.1. MDS 9500 SWITCH PORT LAYOUT	23
2.8.2. MDS 9710 SWITCH PORT LAYOUT	25
2.8.3. MDS 9710 PORT CHANNEL LAYOUT	25
2.8.3.1. MDS 9710 PORT CHANNEL LAYOUT (TWO-TIER)	26
2.8.3.2. MDS 9710 PORT CHANNEL LAYOUT (THREE-TIER)	26
2.8.4. MDS 9148S SWITCH PORT LAYOUT	30
2.8.5. MDS 9148S PORT CHANNEL LAYOUT	30
3. PHYSICAL INSTALL CONSIDERATIONS	31
3.1. RACK	31
3.2. POWER AND COOLING	31
3.3. ETHERNET AND CONSOLE CONNECTIONS	33
3.4. KEEP FAN TRAY CLEAR.....	33
3.5. POWER SUPPLY CIRCUITS	33
3.6. INFRASTRUCTURE FIBRE CHANNEL CABLING	34
3.6.1. 8GB SFP CABLE DISTANCES	34
3.6.2. 16GB SFP CABLE DISTANCES	35
4. FABRIC/SWITCH MANAGEMENT INFRASTRUCTURE	36
4.1. ARCHITECTURE	36
4.2. MANAGEMENT SERVER SIZING AND PLACEMENT	37

4.3.	TERMINAL SERVICES LICENSE	38
4.4.	RADIUS AUTHENTICATION SERVER (NPS).....	38
5.	MANAGEMENT SERVER BUILD	38
5.1.	JAVA RUNTIME ENVIRONMENT	38
5.2.	INSTALL DCNM SERVER COMPONENTS	39
5.2.1.	INSTALLING DCNM SERVER	39
5.2.2.	DEVICE MANAGER AND DCNM CLIENT INSTALLED	47
5.2.3.	DISCOVER SAN FABRIC.....	48
5.3.	INSTALL SSH CLIENT	50
5.4.	INSTALL SFTP SERVER	51
5.5.	CONFIGURE DCNM WITH CITI SSH	51
5.6.	CONFIGURE CALL-HOME	53
5.6.1.	CALL-HOME TO EMC.....	53
5.6.2.	CALL-HOME TO HDS	54
5.7.	CONFIGURE DCNM TO AUTHENTICATE TO ACTIVE DIRECTORY	61
5.7.1.	BACK OUT DCNM AUTHENTICATION TO ACTIVE DIRECTORY	63
5.8.	MANAGEMENT SERVER ACCESS CONTROL.....	65
5.9.	REBOOT THE SERVER.....	65
5.10.	DOWNGRADE TO PREVIOUS DCNM VERSION.....	65
6.	SWITCH CONFIGURATION STEPS.....	65
6.1.	STEP 1: DESIGN VSAN IDS AND DOMAIN IDS.....	65
6.1.1.	STEP 1A: MIGRATIONS AND DOMAIN IDS (NPV)	67
6.2.	STEP 2: NAMING STANDARD	68
6.3.	STEP 3: CUSTOMIZE CONFIGURATION TEMPLATE	69
6.3.1.	CONFIGURATION ITEMS IN THE TEMPLATE.....	69
6.4.	STEP 4: POWER UP AND FIRST LOGIN	70
6.5.	STEP 5: CONFIGURE IP ADDRESS & DEFAULT GATEWAY	70
6.6.	STEP 6: UPGRADE NX-OS TO CSBE CERTIFIED VERSION	70
6.7.	STEP 7: CONFIGURATION COMMANDS	72
6.8.	STEP 9: OBTAIN AND INSTALL LICENSING	72
7.	USER IDS AND AUTHENTICATION	72
7.1.	INTERACTIVE AUTHENTICATION (NPS / ACTIVE DIRECTORY).....	72
7.1.1.	CREATE ACTIVE DIRECTORY SECURITY GROUPS	74
7.1.1.1.	SWITCH ROLES	74
7.1.1.1.1.	STORAGE ADMIN	74
7.1.1.1.2.	VENDOR.....	75
7.1.1.1.3.	SCRIPT.....	75
7.1.1.1.4.	FACILITY	75
7.1.2.	INSTALL WINDOWS NETWORK POLICY SERVER ("NPS").....	76
7.1.3.	CONFIGURE NPS.....	79
7.2.	CRYPTOGRAPHY (SHA / AES)	88
7.3.	STORAGE PERSONNEL AUTHENTICATION	88
7.4.	VENDOR AUTHENTICATION	90
7.5.	PURPOSE OF NETWORK-ADMIN ROLE.....	90
7.6.	NON-INTERACTIVE AUTHENTICATION.....	91
7.7.	FUNCTIONAL IDS.....	93
8.	AUDIT TRAIL MANAGEMENT (SEMS).....	94

8.1.	SEMS INCLUDE LIST	95
9.	VENDOR REMOTE ACCESS	95
9.1.	EMC REMOTE ACCESS REGISTRATION	95
9.2.	HDS REMOTE ACCESS REGISTRATION.....	95
10.	INTEGRATION WITH ECC	96
11.	INTEGRATION WITH SANSCREEN	96
12.	INTEGRATION WITH HPNA	96
13.	MONITORING THE SWITCH WITH ESS.....	96
13.1.	IMPLEMENTATION STEPS	97
13.2.	TRAPS TO MONITOR.....	97
13.3.	TESTING	103
14.	N_PORT ID VIRTUALIZATION (NPIV).....	103
15.	SWITCH BACKUP AND RESTORE PROCESS	104
15.1.	SWITCH BACKUP VIA DCNM WEB CLIENT	104
15.2.	SWITCH RESTORE VIA DCNM WEB CLIENT	106
15.2.1.	PREREQUISITE	106
15.2.2.	OPS – RESTORE FROM BACKUP	106
15.2.3.	VENDOR: (REPLACE FAILED SWITCH WITH SPARE).....	110
15.2.4.	OPS: (MERGE NEW NPV SWITCH WITH FABRIC)	111
15.3.	MANAGEMENT SERVER BACKUP AND RECOVERY	112
16.	PORT GROUP MONITORING	112
17.	PORT MONITORING	113
17.1.	DEFAULT PORT MONITOR POLICY SETTINGS	114
17.2.	RECOMMENDED CITI PORT MONITOR POLICY SETTINGS	115
17.2.1.	ISL TRUNK MONITORING (CORE OR CORE/STORAGE SWITCHES).....	115
17.2.2.	STORAGE PORT MONITORING (STORAGE OR CORE/STORAGE EDGE SWITCH)	117
17.2.3.	HOST PORT MONITORING (HOST EDGE SWITCH).....	119
17.2.4.	TROUBLESHOOTING PORT MONITORING ALERTS	121
18.	DCNM WEB CLIENT - PERFORMANCE MANAGER.....	122
18.1.	LAUNCHING DCNM WEB CLIENT	123
19.	FIRMWARE UPGRADES/DOWNGRADES.....	124
19.1.	PRE-STAGE NX-OS FILES VIA DCNM.....	124
19.2.	SOFTWARE (FIRMWARE) INSTALL WIZARD	127
20.	NEW LICENSING MODEL FOR DCNM 6.3.X	131
20.1.	INSTALLING LICENSES FOR NEWLY PURCHASED SWITCHES	132
21.	KNOWN ISSUES AND BUG FIXES	132

22.	SECURITY REVIEW FINDINGS	133
22.1.	DATA CENTER NETWORK MANAGER FINDINGS (OPEN)	133
22.2.	DATA CENTER NETWORK MANAGER FINDINGS (CLOSED).....	133
22.2.1.	APP135 (N2) - POSTGRESQL	133
22.3.	DCNM PERFORMANCE MANAGER FINDINGS (OPEN)	134
22.3.1.	LOW - APP042 AND CVA0034 (H4) – FILE AND DIRECTORY PROTECTION.....	134
22.3.2.	CVA0077 (M1) – BROWSER AUTO-COMPLETE	135
22.3.3.	CVA0204 (M3) – SENSITIVE INFORMATION.....	135
22.3.4.	LOW - CVA0052 (M4) – FORCEFUL BROWSING	135
22.3.5.	LOW - CVA0029 (M6) – CACHE	136
22.3.6.	CVA2503 (L1) – SSL SIGNED CERTIFICATE.....	136
22.4.	DCNM PERFORMANCE MANAGER FINDINGS (CLOSED).....	137
22.4.1.	APP035 AND CVA0106 (H6) – AUTHORIZATION / ACCESS CONTROL / ENTITLEMENT	137
22.4.2.	APP118 AND CVA0035 (M5) – SESSION IDENTIFIER PASSAGE	137
22.4.3.	APP122 AND CVA0274 (M7) – SECURE COOKIES.....	138
22.4.4.	CVA0286 (M2) – CROSSFRAME SCRIPTING.....	140
23.	APPENDIX A: PARTS LIST FOR CISCO MDS SWITCHES.....	142
24.	APPENDIX B: GLOSSARY	144
25.	APPENDIX C: SWITCH CONFIGURATION	146
25.1.	INITIAL SWITCH SETUP	146
25.2.	BASE CONFIG	146
25.2.1.	MDS 9148 WITH NPV ENABLED.....	146
25.2.2.	MDS 9710 CORE AND/OR STORAGE EDGE	149
25.3.	CUSTOM CONFIGURATION (VARIABLE SETTINGS)	151
25.3.1.	MDS 9148 WITH NPV ENABLED.....	151
25.3.2.	MDS 9710 STORAGE EDGE EXAMPLE.....	154
25.3.3.	MDS 9710 CORE EXAMPLE.....	156
25.4.	FINAL CONFIGURATION SETTINGS.....	160
26.	APPENDIX D: SEED SWITCH UTILITY	162
27.	APPENDIX E: TEST SCOPE / TESTING / RESULTS.....	163
28.	APPENDIX F: REVISION HISTORY.....	163

1. Introduction

1.1. Document Purpose

Cisco MDS Fibre Channel Switches are the standard for building Storage Area Networks (SAN) at Citi. This Solutions Guide will aid global SAN operations teams in designing and deploying SANs based on MDS. For the latest version of this document and for other related documentation please visit the CSBE homepage for MDS at:

<http://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/ciscomds.aspx>

Please see appendix B for a description of terms used in this document

1.2. Owner of Standard

CSBE (CATE Storage & Backup Engineering) is the owner of this standard and the related documents.

1.3. Intended Audience

The intended audience is Global and Regional Operations and Integration personnel responsible for designing, building, supporting, and managing the Cisco MDS Fibre Channel SAN (Storage Area Network).

1.4. Principles

1.4.1. Revision History

See “Version Control” on page 2 of this document.

1.4.2. Key Feature Changes

See the corresponding “Release Notes” document on the CSBE Cisco Webpage.

<http://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/ciscomds.aspx>

2. Fabric Design Guide (Requirements)

2.1. Certified Models and Software Versions

Director Models	MDS 9500 Series: Cisco 9500 Multilayer Director (9506, 9509 ¹ , 9513) MDS 9710
Switch Model	Cisco MDS 9124 ¹ , 9148, 9148s Cisco MDS 9222i ¹ and 9250i – FCIP
NX-OS Version	Existing SAN and FCIP SANs MDS 9100, 9200, 9500: NX-OS 5.2(8f) - New SAN architecture MDS 9710, 9100 and 9250i: NX-OS 6.2(11b)
Supervisor	MDS 9500 Series: Supervisor 2 MDS 9710: Supervisor 1
FAB Modules	MDS 9500 Series: Fab 3 (For increased bandwidth) Fab 2 ¹ Module MDS 9710 Series: Fab 1 (Up to 6, minimum of 3 for 16gb Full Line Rate. Additional Fab modules for redundancy)
Line Cards	MDS 9500 Series: 32 and 48 port 8gb generation 4 Advanced FC line cards 18/4-Port Multiservice Module SSN-16 line card Note²: 12, 24 and 48 port 4gb gen 2 line cards Note²: 24 and 48 port 8gb gen 3 line cards MDS 9710 Series: 48 port 16gb line cards (w/8 or 16gb SFP's)
Management Software	Data Center Network Manager 6.3.2 supported on: Windows 2008 R2 64-bit <i>CLI access via SSH is supported from any platform</i>

¹ End of Sale. Supported in existing environments only.

² End of Life: Replace as soon as possible

NOTE: Two MDS 9513 Fabric 3 modules will increase the active backplane bandwidth of the MDS 9513 Director to **256 Gbps full duplex per slot** when used in conjunction with the 8Gbps Generation 4 Advanced FC modules. NX-OS 5.2.1 minimum is required.

MDS 9710 requires a minimum of 3 Fabric 1 modules to provide 16Gbps Full Line Rate. Additional Fab 1 modules (up to 6) provide redundancy in case of a failed Fabric 1 module.

2.2. Common Hardware and Software Requirements

- All new switch environments should be ordered with MDS 9710 and/or MDS 9148s switches
- MDS 9710 directors should come with Supervisor 1 and Fabric 1 modules
- Existing MDS 9500 switch environments can replace old modules with newer Gen 4 modules as long as Fab 3 modules are installed and the upgrade instructions are followed in the [Cisco MDS NX-OS 5.2\(8e\) - Release Notes](#).
- All switches must be ordered with
 - Cisco DCNM-SAN Advanced Edition (comparable to Cisco Fabric Manager Server License). – Required for performance monitoring and reporting
- All switches in a fabric must be ordered from the same vendor. **Intermixing EMC and HDS supplied switches in the same fabric is strictly prohibited.**
- All line cards in a switch must be supplied by the vendor who supplied the switch. **Intermixing EMC and HDS supplied line cards is strictly prohibited.**
- **Not following these rules will cause vendor support issues.**

2.3. Fabric Topologies

CSBE has certified the use of the following fabric topologies for fabrics contained within the datacenter (“Local SAN”).

2.3.1. Single Tier (Collapsed Core)

The Cisco MDS family, especially the 9710, has a much higher density and Full Line Rate throughput at 8 or 16Gbps per port (16Gb at an additional cost). Current single Core-edge designs can be easily collapsed into a single tier. A single tier design has the advantage of not using any ISLs thereby reducing cost and complexity, and optimizing performance.

2.3.2. Two Tier (Core-Edge)

A core-to-edge fabric topology is recommended to provide any-to-any connectivity, evenly distribute traffic, maximize the ease of scalability and maintain a single hop between devices. In this topology, the core switch connects to tier 1 devices and to edge switches. The tier 1 devices are those requiring high bandwidth and availability such as storage arrays, media servers, streaming streamers, and tape devices. Servers should be attached to the edge switches.

SAN environments where a single 9710 core will still not meet the connectivity requirements should consider a 2-tier **dual core** dual fabric architecture. In this design, ISL's from all edge switches are connected to a pair of dual core switches in each fabric. Storage ports are evenly distributed between the pair of dual core switches in each fabric. While this approach increases the total ISL requirements, it effectively doubles the number of core ports available and maintains a single hop architecture. In large environments such as this, consideration should be given to the increased operational risk of having twice as many servers attached to the same SAN fabrics. Change management policy and procedures may need to be enhanced to reduce the risk of change affecting both large fabrics at the same time.

2.3.3. Three Tier (Edge-Core-Edge)

For those regions that want to increase the port count, the Edge-Core-Edge design allows you to increase port count as you grow. This gives you the ability to connect Host Edges and Storage Edges to a central Core director(s). The Core director(s) are used only for ISL connectivity to the Edge switches. Storage Edge switches are typically MDS 9710's and Host Edge switches are **NPV enabled MDS 9148 or 9148s switches**. This design can scale to 7000+ ports.

2.3.4. N Port Virtualization

Typically, Fibre Channel networks are deployed using a core-edge model with a large number of fabric switches connected to edge devices. Such a model is cost-effective because the per-port cost for director class switches is much higher than that of fabric switches. However, as the number of ports in the fabric increases, the number of switches deployed also increases, and you can end up with a significant increase in the number of domain IDs (the maximum number supported is 239). This challenge becomes even more difficult when additional blade chassis are deployed in Fibre Channel networks.

NPV addresses the increase in the number of domain IDs needed to deploy a large number of the ports by making a fabric or blade switch appear as a host to the core Fibre Channel switch, and as a Fibre Channel switch to the servers in the fabric or blade switch. NPV aggregates multiple locally connected N ports into one or more external NP links, which shares the domain ID of the NPV core switch among multiple NPV switches. NPV also allows multiple devices to attach to same port on the NPV core switch, which reduces the need for more ports on the core.

2.3.5. Dual Fabrics

Dual fabrics should be implemented to provide high availability. Storage arrays and servers should be dual connected to each of the fabrics. This provides increased bandwidth and two independent data paths. There is also protection from single path failure (HBA, cable, switch) and allows for non-disruptive maintenance of the combined SAN. The fabrics should be designed symmetrically for ease of management.

2.4. Scalability Considerations

Selection of switch model, topology and type of line cards should be based on the maximum number of host ports that the SAN will ever support. A good estimate of this number can be obtained by assessing the current host port need and then growing this by an annual increase estimate for the life of the equipment. For example, if there is a demand for 20 host ports today, and the demand is expected to grow by 25% each year, and technology refresh for this type of equipment happens every 5 years in your region, the fabric should be built for supporting 63 host ports.

2.5. ISL Design Best Practices

For Cisco ISLs, all equal cost paths are load balanced using a source/destination/OXID hash. This load balancing is applied to load balance individual ISLs within a Port Channel, and to load balance Port Channels.

- Assume fan-in ratio on the storage ports to be 10:1. This is a rule of thumb and can be modified depending on performance requirements if known.
- Switches should be interconnected by Port Channels. Each Port Channel should have at least two member links (ISLs), and each Port Channel member link should come from a different line card. This way the Port Channel can survive a line card failure.
- Each Port Channel can be scaled to 16 member links, and that should provide enough bandwidth for most topologies. A second Port Channel should only be considered when the first is fully populated with 16 links. Having a bigger Port Channel is desirable over having multiple Port Channels because failure of a Channel causes disruptive FSPF convergence to be triggered unlike failure of a member link within a Channel.
- The entire Port Channel should be provisioned upfront; although MDS allows for non-disruptive addition of members to the Port Channel, Operations may run out of ports by over-allocating ports to hosts, or may even forget to address Port Channel bandwidth as hosts are being added to the fabric.
- **MDS 9710 Gen 1 Line Cards (16Gpbs)**
 - The MDS 9710 Gen 1 Line Card has 48 ports and 768Gbps bandwidth. It can be purchased with 8 or 16Gbps SFPs. These line cards operate at **Full Line Rate**, no oversubscription.
 - The following can be used to calculate number of members in the Port Channel:

If number of host ports that will use this Port Channel is H, and each host connects with S Gbps speed, and the storage port fan-in ratio is F

Total port channel bandwidth required = $(H * S)/F$

Number of port channel members = $(H * S)/F/8$

Example: If there are 44 host ports operating at 4 Gbps and fan-in ratio is 10, number of members in the port channel = 2.

- **MDS 9513 Gen 4 Line Cards (8 Gbps) with Fab 3 Modules:**

- The Fab 3 Module increases the line card bandwidth to 256 Gbps. With the 32 and 48 port 8 Gbps Advanced FC (Gen 4) line cards, this allows **Full Line Rate** on the 32 port line card and 1.5:1 oversubscription on the 48 port line card. It is recommended that the 32 port line cards be used for ISL's and Storage ports.
- The following can be used to calculate number of members in the Port Channel:

If number of host ports that will use this Port Channel is H, and each host connects with S Gbps speed, and the storage port fan-in ratio is F

Total port channel bandwidth required = $(H * S)/F$

Number of port channel members = $(H * S)/F/8$

Example: If there are 100 host ports operating at 4 Gbps and fan-in ratio is 10, number of members in the port channel = 5.

2.6. Tape SANs

Because most fabrics run out of storage ports on the core as the SAN grows, GDSE recommends building separate physical fabrics for backup purposes. Smaller sites with predictable storage and tape port growth may share the disk fabrics with tape after partitioning the tape fabrics off into their own VSANs. Any tape traffic traversing ISLs should also be partitioned off by using VSAN trunking. If a core-edge topology is being used for disk fabric, the edge ports can be used to connect hosts to the tape SAN. In this case, a dedicated tape core should be used to connect tape devices. The tape core switch should be collocated with the disk edge switch(s) so that if the disk fabric is running out of edge ports the tape edge ports can be conveniently migrated to the tape core.

For more detailed information on Tape SANs, refer to the [Cisco MDS Tape SAN Design Guide](#) located on the CSBE Cisco Webpage.

2.7. SAN Architecture Design Examples

CATE Storage and Backup Engineering are updating its design best practices to further leverage the use of the **MDS 9148 and 9148s Switches** which are currently certified. Going forward, the MDS 9148s should be purchased; it is 8 or 16gb capable and is cheaper than its predecessor when 8gb SFPs are utilized.

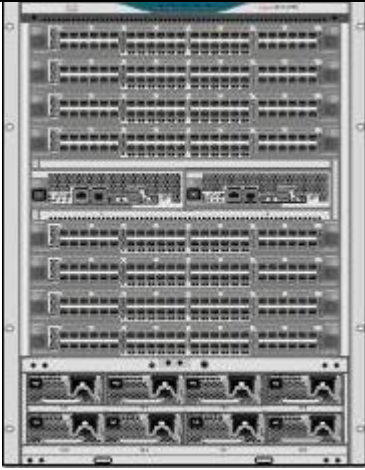
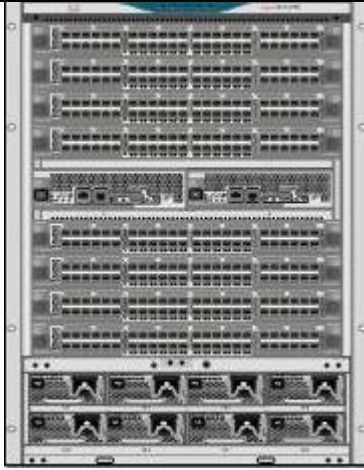
Using the MDS 9148s switches on the Host Edge will provide considerable savings on the cost of a SAN versus using Directors at the Host edge.

The following examples are provided to aid Operations teams in designing their fabrics. The examples utilize the MDS 9148s switch and the MDS 9710 director and assume a 3 year technology refresh cycle and 25% year over year growth in host port count. Please see appendix A for detailed parts lists needed to build each design. Please note that none of these designs consider reserving slots for optional future modules.

2.7.1. Single Tier SAN – Small (< 384 ports)

MDS 9710 – Single Tier

This design utilizes a single tier MDS 9710 with full line rate/non-blocking at 4/8/16Gbps 48 port modules for host and storage.

Fabric A		Fabric B	
1 x MDS 9710 8 x 48 port LC		1 x MDS 9710 8 x 48 port LC	

Max port count = 384 per Fabric (Total SAN = 768 ports)

Max host = 346 at 4/8/16Gbps

Max storage = 38 at 4/8/16Gbps

Host to Disk fan-in ratio of 10

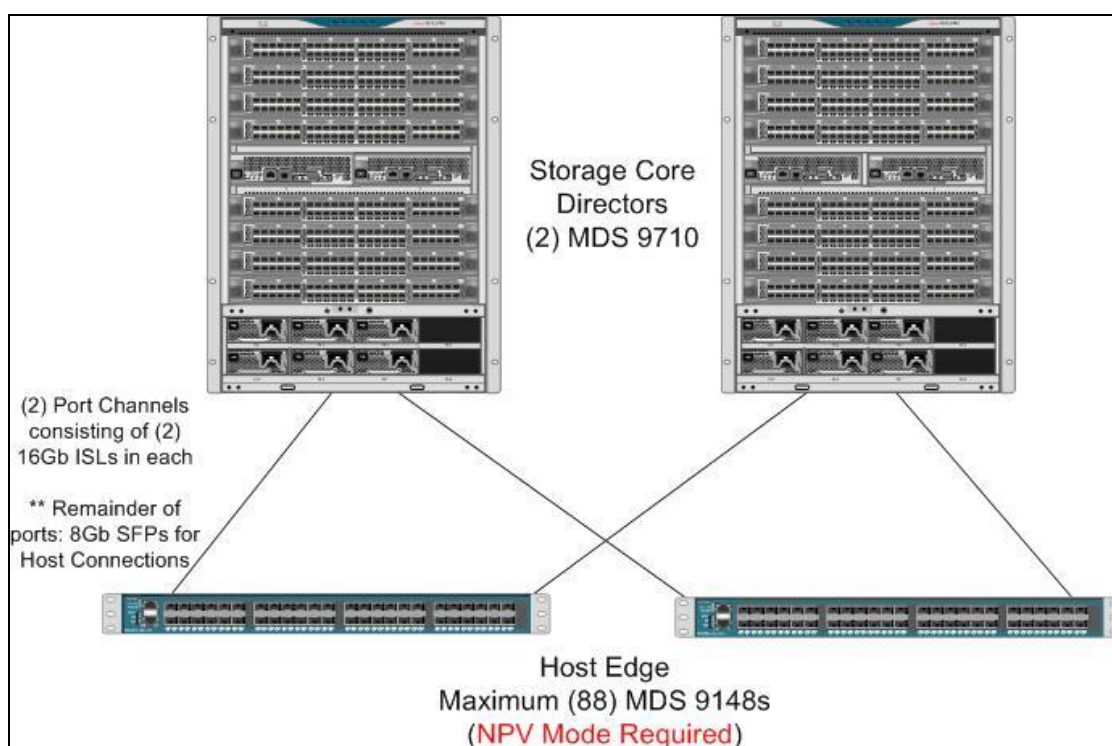
2.7.2. Two Tier SAN (Core-Edge) – Medium (< 4900 ports)

The Dual Core Two Tier SAN design was created for environments that would scale no larger than 3500 ports.

*CATE requires that the MDS 9148s Host Edge switches have **NPV enabled**. The Host Edge switches will look like an N-Port to the Core MDS 9710 Directors. The Core MDS 9710 Directors will require **NPIV** and the “**fport-channel-trunk**” feature be enabled.*

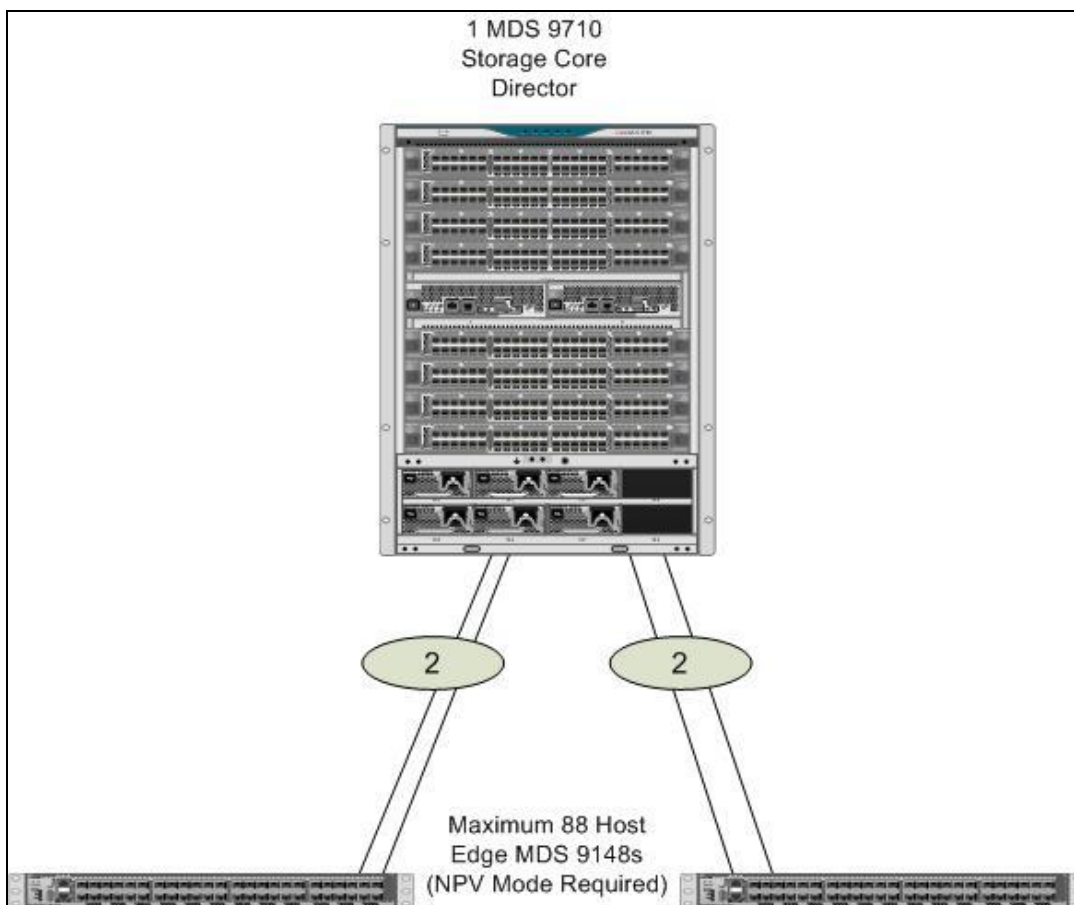
- The Edge MDS 9148s utilizes full line rate/non-blocking at 2/4/8Gbps (8gb SFP) or 4/8/16Gbps (16gb SFP) on the 48 port switch for Host connectivity (**no oversubscription on the 48 port switch**)

- The Core MDS 9710 utilizes full line rate/non-blocking 4/8/16Gbps ports in the 48 port modules for Storage
 - ISLs utilize full line rate/non-blocking 16Gbps ports from the MDS 9710 48 port modules to the MDS 9148s
 - Two 16Gbps ISL's (per Port-Channel) are recommended for the MDS 9148s. Port layout is shown in Section 2.8.4
 - 16Gb SFP's should be used for ISL connectivity and 8Gb SFP's for Host connectivity.
 - This SAN configuration can scale to 88 Host Edge MDS 9148 switches. SAN's can be built smaller and scaled up as demand increases.
 - CATE requires all MDS 9148s switches be **NPV Mode** enabled
 - This configuration also enables the ability to utilize a top of rack or end of row SAN design
 - The MDS 9148s switch uses considerable less power and cooling
 - CATE Storage Engineering also recommends that one or two spare MDS 9148s' be kept onsite incase a replacement is needed
 - NPV aggregates multiple locally connected N ports into NP links, which share the domain ID of the NPV core switch among multiple NPV switches.
 - **Note:**
Take into consideration virtualized hosts sharing a single port. Virtualized hosts increase the FLOGI count. Dual Core Directors can accommodate 4000 FLOGIs (2000 FLOGIs each).
- Monitor fabric FLOGIs to make sure the limits aren't exceeded.**



Fabric Design Type	Fabric Layout	Core Directors	Core Ports per Director	Total Core Ports	ISL Port-Channels	Total ISLs in each Core	Total Core ISL Ports	Edge Switches	Edge Ports per Switch	Total Edge Ports	Total Edge ISL Ports	Max Fabric Port Count	Max Fabric Storage Ports	Max Fabric Host Ports	Total SAN Ports (Fab A & B)	Host to Disk Fan-In Ratio	ISL Fan-In Ratio (x:1)
Two Tier with Dual Cores	2-mds9710 Cores (8x48 LC) 88-mds9148s edges	2	384	768	2	176	352	88	48	4224	352	4992	416	3872	9984	9.30769	11

Another example of a Two-Tier SAN using a single Core director:



Fabric Design Type	Fabric Layout	Core Directors	Core Ports per Director	Total Core Ports	ISL Port-Channels	Total ISLs in each Core	Total Core ISL Ports	Edge Switches	Edge Ports per Switch	Total Edge Ports	Total Edge ISL Ports	Max Fabric Port Count	Max Fabric Storage Ports	Max Fabric Host Ports	Total SAN Ports (Fab A & B)	Host to Disk Fan-In Ratio	ISL Fan-In Ratio (x:1)
Two Tier with Single Core	1-mds9710 Cores (8x48 LC) 88-mds9148s edges	1	384	384	2	176	176	88	48	4224	176	4608	208	4048	9216	19.4615	23

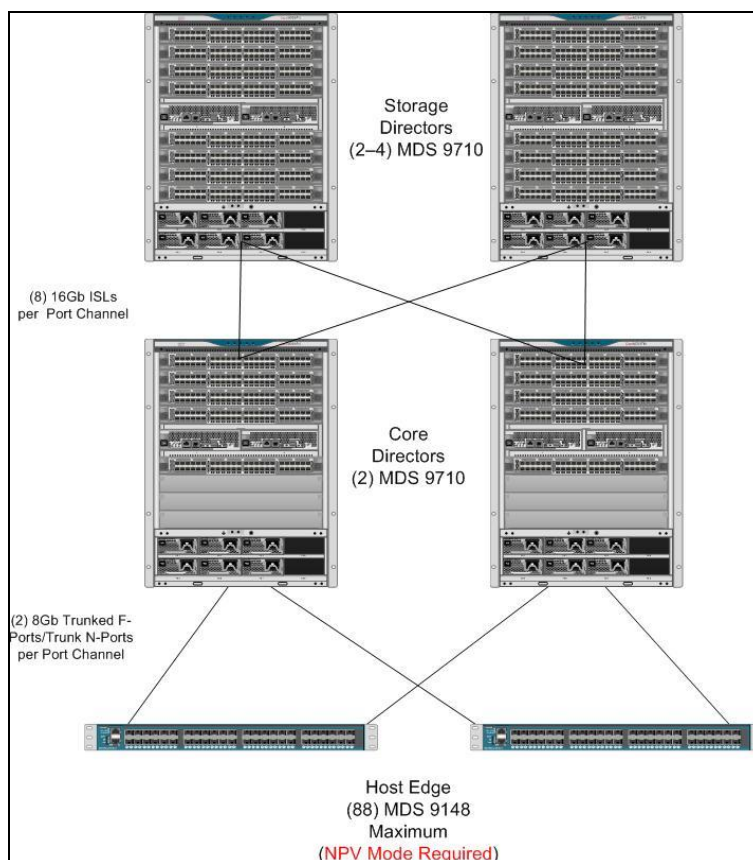
2.7.3. Three Tier SAN (Edge-Core-Edge)

For those regions that want to increase the port count, or have a “Single SAN” in a Data Center, the Edge-Core-Edge design provides that scalability. Edge-Core-Edge gives you the ability to connect Host Edges and Storage Edges to Core director(s) and grow the port count as needed. The Edge Core Edge design can scale to 7000+ ports per fabric.

CATE requires that the MDS 9148 Host Edge switches have **NPV enabled**. The Host Edge switches will look like an N-Port to the Core MDS 9710 Directors. The Core MDS 9710 Directors will require **NPIV** and the “**fport-channel-trunk**” feature be enabled.

2.7.3.1. Dual Core Edge-Core-Edge – Large (< 6000 ports)

- The Edge MDS 9148 utilizes full line rate/non-blocking at 2/4/8/Gbps on the 48 port switch for Host connectivity (**no oversubscription on the 48 port switch**)
- The Core MDS 9710 utilizes full line rate/non-blocking 4/8/16Gbps ports in the 48 port modules for Storage
- ISLs utilize full line rate/non-blocking 8Gbps ports between the MDS 9710 Storage Directors and the MDS 9710 Core Directors
- Two 8Gbps TF-Nport Trunks (per Port-Channel) are recommended for the Port-Channels between the MDS 9148 and the MDS 9710 Core Directors.
- 8Gb SFP's should be used for Port-Channel connectivity only.
- 8Gb SFP's should be used for Host and storage connectivity (until 16Gb storage ports are available).
- This SAN configuration can scale to 88 Host Edge MDS 9148 switches (in NPV Mode). SAN's can be built smaller and scaled up as demand increases.
- NPV aggregates multiple locally connected N ports into NP links, which share the domain ID of the NPV core switch among multiple NPV switches.
- This configuration also enables the ability to utilize a top of rack or end of row SAN design
- The MDS 9148 switch uses considerable less power and cooling
- CATE Storage Engineering also recommends that one or two spare MDS 9148's be kept onsite incase a replacement is needed
- **Note:**
88 Host Edge switch maximum does not take into consideration virtualized hosts sharing a single port. Virtualized hosts increase the FLOGI count. Dual Core Directors can accommodate 4000 FLOGIs (2000 FLOGIs each).
Monitor fabric FLOGIs to make sure the limits aren't exceeded.
- If you reach the limit, a second Core Pair of Directors can be implemented with another set of Host Edge Switches. Reserve ports in the Storage Directors to connect to 2nd Core Pair. This Dual Core will become a Quad Core (next section).



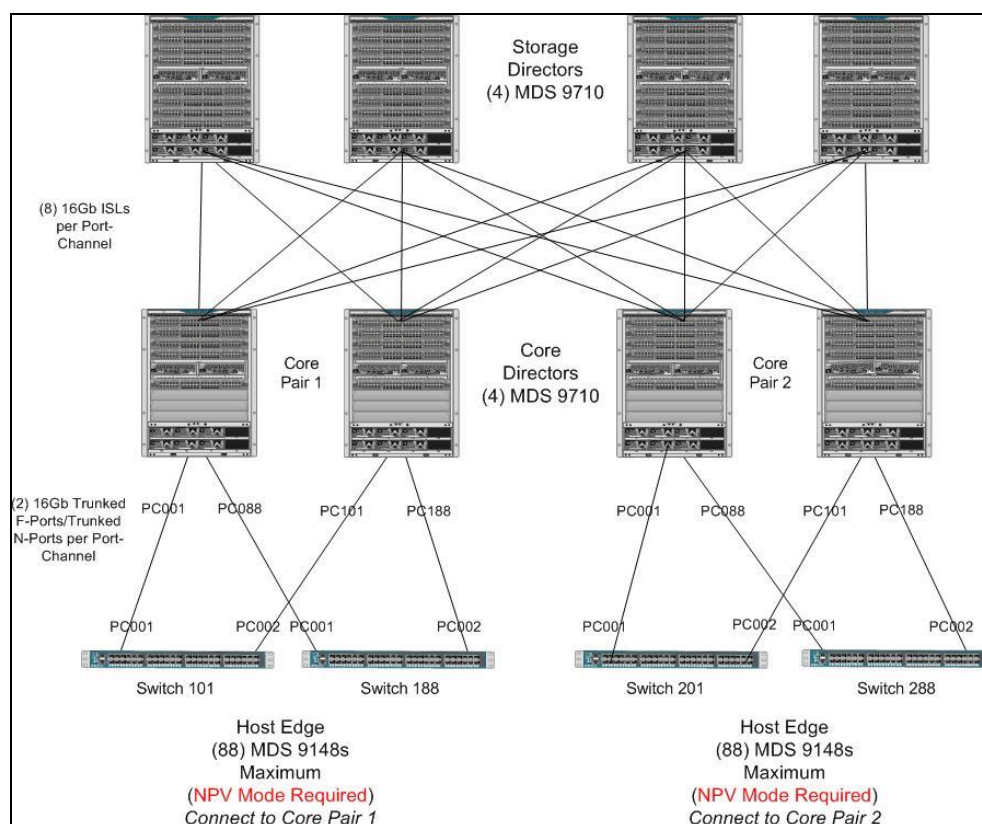
Fabric Design Type	Fabric Layout	Cores	Core Ports per Director	Total Core Ports	Total Core ISL Ports	Storage Edge Directors	ISLs per Port-Channel	Storage Edge Ports per Director	Total Storage Edge Ports	Total Storage Edge ISL Ports	Host Edge Directors	ISLs per Port-Channel	Host Edge Ports per Director	Total Host Edge Ports	Total Host Edge ISL Ports	Max Fabric Port Count	Max Fabric Storage Ports	Max Fabric Host Ports	Total SAN Ports (Fab A & B)	Host to Disk Fan-In Ratio	ISL Fan-In Ratio (x:1)
Dual Core Three Tier	2 - mds9710 cores *5 x 48 port LC 2 - mds9710 storage *8 x 48 port LC 40 - mds9148s host	2	240	480	416	4	8	384	1536	64	88	2	48	4224	352	6240	1472	3872	12480	2.6304	11

2.7.3.2. Quad Core Edge-Core-Edge – Xlarge (<10,000 Ports)

- The Edge MDS 9148 utilizes full line rate/non-blocking at 2/4/8/Gbps on the 48 port switch for Host connectivity (**no oversubscription on the 48 port switch**)
- The Core MDS 9710 utilizes full line rate/non-blocking 4/8/16Gbps ports in the 48 port modules for Storage
- ISLs utilize full line rate/non-blocking 16Gbps ports between the MDS 9710 Storage Directors and the MDS 9710 Core Directors
- Two 8Gbps TF-Nport Trunks (per Port-Channel) are recommended for the Port-Channels between the MDS 9148 and the MDS 9710 Core Directors.
- 8Gb SFP's should be used for Port-Channel connectivity only.
- 8Gb SFP's should be used for Host and storage connectivity (until 16Gb storage ports are available).

- This SAN configuration can scale to 176 Host Edge MDS 9148 switches (in NPV Mode). 88 Host Edge switches to Core Pair 1 and 88 Host Edge switches to Core Pair 2. SAN's can be built smaller and scaled up as demand increases.
- NPV aggregates multiple locally connected N ports into NP links, which share the domain ID of the NPV core switch among multiple NPV switches.
- This configuration also enables the ability to utilize a top of rack or end of row SAN design
- The MDS 9148 switch uses considerable less power and cooling
- CATE Storage Engineering also recommends that one or two spare MDS 9148's be kept onsite incase a replacement is needed
- **Note:**
88 Host Edge switch maximum does not take into consideration virtualized hosts sharing a single port. Virtualized hosts increase the FLOGI count. Dual Core Directors can accommodate 4000 FLOGIs (2000 FLOGIs each).

Monitor fabric FLOGIs to make sure the limits aren't exceeded.



Fabric Design Type	Fabric Layout	Cores	Core Ports per Director	Total Core Ports	Total Core ISL Ports	Storage Edge Directors	ISLs per Port-Channel	Storage Edge Ports per Director	Total Storage Edge Ports	Total Storage Edge ISL Ports	Host Edge Switches	ISLs per Port-Channel	Host Edge Ports per Director	Total Host Edge Ports	Total Host Edge ISL Ports	Max Fabric Port Count	Max Fabric Storage Ports	Max Fabric Host Ports	Total SAN Ports (Fab A & B)	Host to Disk Fan-In Ratio	ISL Fan-In Ratio (x:1)
Quad Core Three Tier	4 - mds9710 cores *5 x 48 port LC	2	240	480	416	4	8	384	1536	128	88	2	48	4224	352	10944	1408	7744	21888	5.5	11
	4 - mds9710 storage *8 x 48 port LC 88 - mds9148s host	2	240	480	416																

2.8. Line Card and Switch Layout

This section provides line card and switch details, consisting of:

- Ports
- Port-Groups
- ISL distribution
- Host and Storage connections

2.8.1. MDS 9500 Switch Port Layout

32 Port Gen 4 line card – Core and Edge (ISL Cards):



Port Group	Port	SFP	Port	SFP
1	1	8Gbps (ISL)	2-4	8Gbps
2	5	8Gbps (ISL)	6-8	8Gbps
3	9	8Gbps (ISL)	10-12	8Gbps
4	13	8Gbps (ISL)	14-16	8Gbps
5	17	8Gbps (ISL)	18-20	8Gbps
6	21	8Gbps (ISL)	22-24	8Gbps
7	25	8Gbps (ISL)	26-28	8Gbps
8	29	8Gbps (ISL)	30-32	8Gbps

32 Port Gen 4 line card – Core (Storage Ports):



Port Group	Port	SFP
1	1-4	8Gbps
2	5-8	8Gbps
3	9-12	8Gbps
4	13-16	8Gbps
5	17-20	8Gbps
6	21-24	8Gbps
7	25-28	8Gbps
8	29-32	8Gbps

48 Port Gen 4 line card – Edge (Host Ports):



Port Group	Port	SFP
1	1-6	8Gbps
2	7-12	8Gbps
3	13-18	8Gbps
4	19-24	8Gbps
5	25-30	8Gbps
6	31-36	8Gbps
7	37-42	8Gbps
8	43-48	8Gbps

Generation 4 Line Card Oversubscription:

Each generation 4 slot on the MDS 9513 switch has around 256 Gbps of total bandwidth (with Fab 3 Modules). That means each slot can support $256\text{Gb}/8 = 32$ ports operating at full 8 Gbps. The 48 port line card therefore has ports that share bandwidth.

	Generation 4 Modules
	8 Gbps FC
32 port *	Full rate
48 port *	1.5 to 1 oversubscription

* Supports port bandwidth reservation

The sharing does not happen across all the ports on the line card; bandwidth is dedicated to “port groups” and ports within a port group share bandwidth.

Line Card (Gen 4)	Ports Per Port Group	Port Groups	Bandwidth Per Port Group
32 port	4	8	32
48 port	6	8	32

Because of the fan-in ratio of 10:1 on the storage side, such sharing of bandwidth on the front end does not reduce the end-to-end bandwidth.

- The 48 port line card is recommended for host ports only. It should not be used for ISL, storage or tape ports
 - Hosts (applications) that are known to generate high IO traffic all the time, such as media servers or streaming servers, should be provisioned on 32 port line cards.
1.
 - Port utilization on 48 port line cards should be continuously monitored using the Performance Manager. Utilization for 6 ports in the group should be aggregated to see if total group capacity of 32 Gbps is being reached on multiple occasions. If this is the case, hosts generating more traffic within the group should be moved to less utilized port groups,

or moved to a 32 port line card. It is a good idea to have a 32 port line card with a few ports open to support such moves.

2.

Dedicating Bandwidth on the 48 port Gen 4 Line Card:

Certain oversubscribed front end ports from the 48 port line card can be dedicated bandwidth. This may be required when one or more less important applications in the port group occasionally generate high IO traffic and rob more important applications of bandwidth, in which case it is a good idea to set aside bandwidth for the important applications. Another use of this configuration is when the shared ports must be used for ISLs, in which case the ports must be guaranteed 8 Gbps of bandwidth.

Dedicating bandwidth to ports must be carefully planned and ports that are provided dedicated bandwidth should be distributed between port groups. As a best practice, using shared bandwidth ports for storage, tape and ISL should be avoided.

2.8.2. MDS 9710 Switch Port Layout

48 Port Full Line Rate 16Gbps Line Card – Port Groups (DS-X9448-768K)



Port Group	Port	Storage Edge	3 Tier Core (Edge-Core-Edge)	2 Tier Core (Core –Edge)
1	1-4	16Gbps (ISL to Core)	16Gbps (ISL to Storage)	8Gbps (ISL to Host Edge)
2	5-8	Reserve (ISL to Core)	Reserve (ISL to Storage)	8Gbps (ISL to Host Edge)
3	9-12	8Gbps (Storage)	8Gbps (ISL to Host Edge)	8Gbps (ISL to Host Edge)
4	13-16	8Gbps (Storage)	8Gbps (ISL to Host Edge)	8Gbps (ISL to Host Edge)
5	17-20	8Gbps (Storage)	8Gbps (ISL to Host Edge)	8Gbps (Storage)
6	21-24	8Gbps (Storage)	8Gbps (ISL to Host Edge)	8Gbps (Storage)
7	25-28	8Gbps (Storage)	8Gbps (ISL to Host Edge)	8Gbps (Storage)
8	29-32	8Gbps (Storage)	8Gbps (ISL to Host Edge)	8Gbps (Storage)
9	33-36	8Gbps (Storage)	8Gbps (ISL to Host Edge)	8Gbps (Storage)
10	37-40	8Gbps (Storage)	8Gbps (ISL to Host Edge)	8Gbps (Storage)
11	41-44	8Gbps (Storage)	8Gbps (ISL to Host Edge)	8Gbps (Storage)
12	45-48	8Gbps (Storage)	8Gbps (ISL to Host Edge)	8Gbps (Storage)

2.8.3. MDS 9710 Port Channel Layout

The new SAN architecture design best practice is to use MDS 9710's for the Storage Core and MDS 9148's for the Host Edge switches. The use of MDS 9148's will increase the number of Port Channels to the core directors. For management of these Port Channels, it's wise to standardize the numbering of the Port-Channels.

2.8.3.1. MDS 9710 Port Channel Layout (Two-Tier)

The example below provides Port connections and Port-Channel numbers for a Two-Tier SAN, consisting of **(2) MDS 9710 Storage Core directors** and (40-60) MDS 9148 Host Edges per Fabric (Fabric A and Fabric B). It's recommended that:

- Host Edge switch Port-Channels should be connected to the Core starting in the right hand ports of the Director, reserving the right side of the director for Storage connections.
- **NOTE:**
Host Port-Channels – Uplinks within these **NPV** Port-Channels are connected differently in this design scenario. Please note, this is different than how Port-Channel links are typically connected to the Core (see [Cisco recommendation](#) of Port Channel Layout in the next section)
- Port-Channel Numbering:

Fabric A:

Port-Channels 1-60 Fabric A Core1

Port-Channels 101-160 Fabric A Core 2

Fabric B:

Port-Channels 1-60 SAN B Core1

Port-Channels 101-160 SAN B Core 2

2.8.3.2. MDS 9710 Port Channel Layout (Three-Tier)

Dual Core

The example below provides Port-Channel numbers for a Three-Tier Dual Core (Edge-Core-Edge).

- Storage Edge – (2-4) MDS 9710 Directors
- Core – Dual Core – (2) MDS 9710 Directors
- Host Edge – (up to 88) MDS 9148 Switches
- Storage Port-Channels connections should be spread evenly across Core Director modules.
For ease of management, it's recommended that:
 - Storage Port-Channels should be connected to the Core starting in the left hand ports of both the Storage and Core Directors
- For ease of management, it's recommended that Host Edge switch uplinks in a Port-Channel should be connected to the Core Directors starting in the right hand ports of the Director Line Cards.
- Port-Channel Numbering:

Fabric A:

Host Port-Channels 001 - Core1 Port-Channels 001-088

Host Port-Channels 002 - Core2 Port-Channels 101-188

Storage Port-Channels 201-204 Core 1

Storage Port-Channels 211-214 Core 2

Fabric B:

Host Port-Channels 001 - Core1 Port-Channels 001-088

Host Port-Channels 002 - Core2 Port-Channels 101-188

Storage Port-Channels 201-204 Core 1

Storage Port-Channels 211-214 Core 2

- **NOTE:**

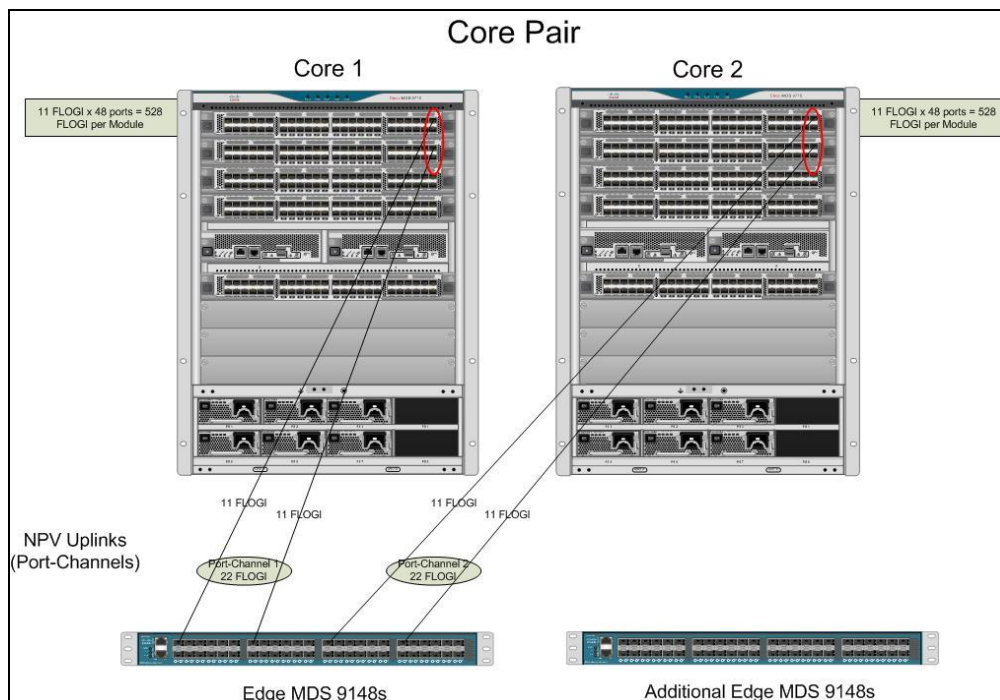
Host Port-Channels – Uplinks within these **NPV** Port-Channels are connected differently in this design scenario. Please note, this is different than how Port-Channel links are typically connected to the Core.

In the event that a Core Director in a Core Pair were to fail and subsequently a line card in the other Core Director were to fail, the Fabric could become UNSTABLE and jeopardize the health of the entire Fabric.

To keep the Fabric STABLE if such a rare event were to take place, Cisco recommends that both Host edge switch uplinks within a Port-Channel should be connected into the **same Line Card** in the Core Directors.

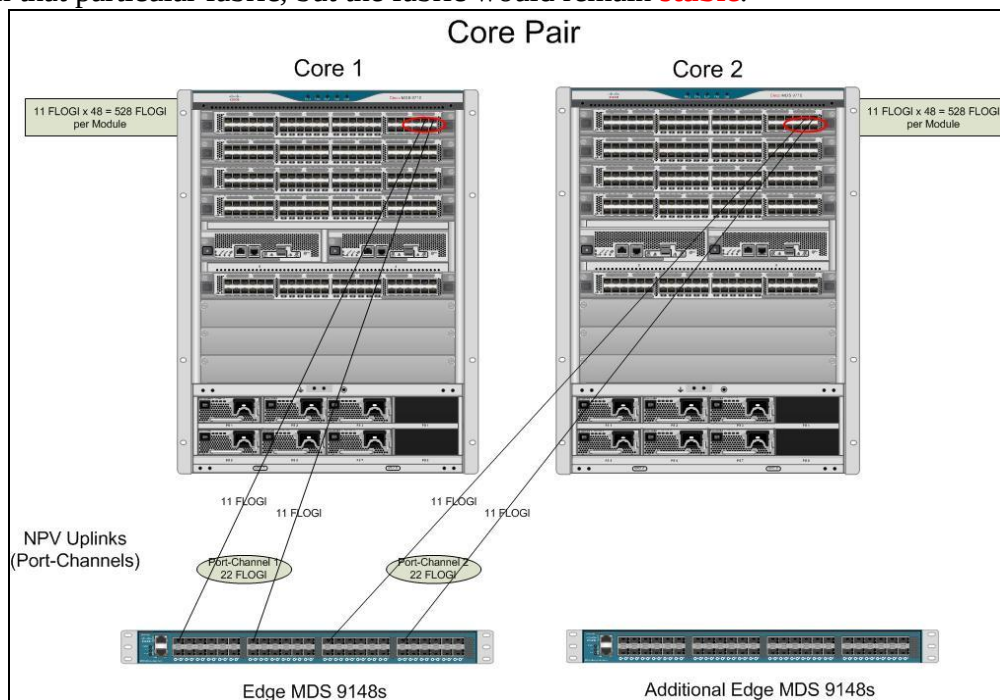
Failure Scenario:

- Assume that all the modules in each of the MDS 9710 Directors and MDS 9148 Host Edge switches are filled with connections
- On the MDS 9148 NPV switches, NPV balances the FLOGIs evenly across the 2 uplinks in port channel 1 to Core 1 and evenly across the 2 uplinks in port channel 2 to Core 2. This occurs on all of the 9148 switches attached to this Core Pair (see diagram below).
- Each MDS 9148 will send approximately 22 FLOGIs up through the uplinks to each of the MDS 9710 Cores.
11 FLOGIs from each switch x 48 Core Ports on a module = 528 FLOGIs on the each module.
All the modules in the MDS 9710 Cores will have approximately 500 FLOGIs.
- Failure Example: If Core 1 Director FAILS. All of the MDS 9148 switches will redirect their FLOGIs through the other uplinks to Core 2.
- At this point each Module in the 2nd Core will now have approximately 1000 FLOGIs.
- That is not a problem. BUT. If a Line Card were to fail while under this condition, the MDS 9148's connected to that failed Line Card would redirect all of its 1000 FLOGIs through the other uplink in the port-channel to the other Line Card which already has 1000 FLOGIs.
- The other Line Card would try to log the extra 1000 FLOGIs, when it already has 1000 FLOGIs. The Line Card and exceed the 1000 FLOGI maximum
- This situation could potentially cause the fabric to become **unstable**.



Cisco Recommendation:

Attach the MDS 9148 Port-Channel uplinks on the same Core Line Card. If this unlikely scenario occurs where a Core fails and the Line Card fails on the 2nd Core Director, the FLOGI's won't failover to a 2nd Line Card that is already full of FLOGI's. Those hosts will lose access to their disks from that particular fabric, but the fabric would remain **stable**.



Quad Core

The example below provides Port-Channel numbers for a Three-Tier Dual Core (Edge-Core-Edge).

- Storage Edge – (2-4) MDS 9710 Directors
- Core – Quad Core – Two pairs of MDS 9710 Directors (total of 4 Directors)
- Host Edge – up to 88 per Core pair for a total of 176 MDS 9148 Switches
- Storage Port-Channels – Links within the Port-Channel should be connected starting in the left hand ports of both the Storage and Core Directors and be spread evenly across Director modules.
- Port-Channel Numbering:

Fabric A:

Host Port-Channels 001 (Core Pair1) Core1 Port-Channels 001-088

Host Port-Channels 002 (Core Pair1) Core2 Port-Channels 101-188

Host Port-Channels 001 (Core Pair2) Core3 Port-Channels 001-088

Host Port-Channels 002 (Core Pair2) Core4 Port-Channels 101-188

Storage Port-Channels 211-214 Core 1 (Core Pair1) Same Port-Channel number on both ends

Storage Port-Channels 221-224 Core 2 (Core Pair1) Same Port-Channel number on both ends

Storage Port-Channels 231-234 Core 3 (Core Pair2) Same Port-Channel number on both ends

Storage Port-Channels 241-244 Core 4 (Core Pair2) Same Port-Channel number on both ends

Fabric B:

Host Port-Channels 001 (Core Pair1) Core1 Port-Channels 001-088

Host Port-Channels 002 (Core Pair1) Core2 Port-Channels 101-188

Host Port-Channels 001 (Core Pair2) Core3 Port-Channels 001-088

Host Port-Channels 002 (Core Pair2) Core4 Port-Channels 101-188

Storage Port-Channels 211-214 Core 1 (Core Pair1) Same Port-Channel number on both ends

Storage Port-Channels 221-224 Core 2 (Core Pair1) Same Port-Channel number on both ends

Storage Port-Channels 231-234 Core 3 (Core Pair2) Same Port-Channel number on both ends

Storage Port-Channels 241-244 Core 4 (Core Pair2) Same Port-Channel number on both ends

- **NOTE:**
Host Port-Channels – Uplinks within these **NPV** Port-Channels are connected differently in this design scenario. Please note, this is different than how Port-Channel links are typically connected to the Core.
In the event that a Core Director in a Core Pair were to fail and subsequently a line card in the other Core Director were to fail, the Fabric could become UNSTABLE and jeopardize the health of the entire Fabric.

To keep the Fabric STABLE if such a rare event were to take place, Cisco recommends that both Host edge switch uplinks within a Port-Channel should be connected into the **same Line Card** in the Core Directors.

For ease of management, it's recommended that Host Edge switch uplinks in a Port-Channel should be connected to the Core Directors starting in the right hand ports of the Director Line Cards.

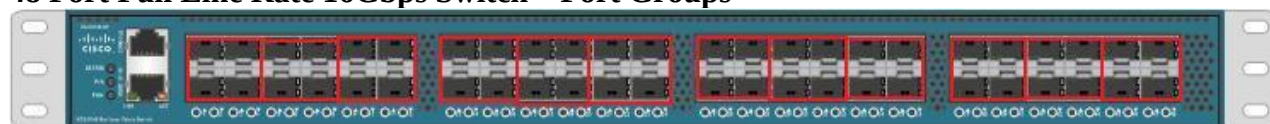
Failure Scenario and Cisco Recommendation

- The same failure scenario that is documented (above) in Dual Core, also applies to Quad Core. See the example under Dual Core.

2.8.4. MDS 9148s Switch Port Layout

The example below provides Port connections and Port-Channel numbers for a Two-Tier SAN, consisting of (2) MDS 9710 Storage Core directors and up to (88) MDS 9148s Host Edges per SAN (SAN A and SAN B). The same layout is used for the Three-Tier SAN designs.

48 Port Full Line Rate 16Gbps Switch – Port Groups



Port Group	Port	SFP	Port	SFP
1	1	16Gbps (ISL-Core1)	2-4	8Gbps (Host)
2	5-8	8Gbps (Host)		
3	9-12	8Gbps (Host)		
4	13	16Gbps (ISL-Core1)	14-16	8Gbps (Host)
5	17-20	8Gbps (Host)		
6	21-24	8Gbps (Host)		
7	25	16Gbps (ISL-Core2)	26-28	8Gbps (Host)
8	29-32	8Gbps (Host)		
9	33-36	8Gbps (Host)		
10	37	16Gbps (ISL-Core2)	38-40	8Gbps (Host)
11	41-44	8Gbps (Host)		
12	45-48	8Gbps (Host)		

2.8.5. MDS 9148s Port Channel Layout

These Port-Channel numbers will also be used for the MDS 9148 switches that are in Core Pair2 (Quad Core Design). Using the same port-channel numbers on all the MDS 9148 switches will make it easier to configure a switch. It's not necessary to have matching Port-Channel numbers on the Core and Host Edge Switches. The base config for each MDS 9148 will be the same, except for the IP address.

	Port-Channel# to Core1		Port-Channel# to Core2	
Fabric A&B				
MDS 9148 Edge Switches	Port 1	Port 13	Port 25	Port 37
Edge 1	1	1	2	2

Edge 2	1	1	2	2
Edge 3	1	1	2	2
Edge 4	1	1	2	2
Edge 5	1	1	2	2
Edge 6	1	1	2	2
Edge 7	1	1	2	2
Edge ..	..	..	..	..
Edge 88	1	1	2	2

3. Physical Install Considerations

3.1. Rack

The Cisco MDS can either be installed in EMC provided cabinets, or customer provided 2 or 4 post rack as per the following table. HDS does not currently offer cabinets for the MDS, and therefore if switches are purchased from HDS they must be installed in customer provided racks. Because Citi is planning to procure MDS from either vendor, **GDSE recommends using racks (not EMC's cabinet) to have a standardized environment.**

Rack Type	MDS 9710	MDS 9513	MDS 9506	MDS 9100/9200
EMC Model	ED-1700-C (Not supported in this cabinet yet.)	ED-1700-C	ED-1700-C	ED-1700-C
EIA (4-Post)	Yes	Yes	Yes	Yes
Telco (2-Post)	No	No	Yes	Yes

At most two MDS 9513s or MDS 9710s can be installed in a EIA 4 post rack. A fully loaded 9513 or 9710 can weigh up to 400 lb, and Cisco recommends that a mechanical lift be used to install the fully loaded switch in the rack.

Cisco recommends that you maintain a minimum air space of 2.5 inches (6.4cm) between walls and the chassis air vents and a minimum horizontal separation of 6 inches (15.2 cm) between two chassis to prevent overheating.

It is a common mistake to order the wrong type of power cables that will not go into the power outlets on the rack. Locking type power connectors are preferred.

3.2. Power and Cooling

The charts below compare the power and cooling requirements for MDS 9710, MDS 9513 Chassis, line cards, and the MDS 9148 Switch.

Note: These numbers are Cisco's worst case scenario.

MDS 9710 FC Modules

Module	Watts	Ports	Watts per Port
DS-X9448-768K (48 Port 16Gb)	550	48	11.45

Module	BTU	Ports	BTU per Port
DS-X9448-768K (48 Port 16Gb)	No Data	48	-

MDS 9710 Chassis and Supervisor

Module	Watts	Chassis w/o FC modules
DS-C9710 w Fans	1800	2630 Watts
(2) DS-X97-SF1-K9 (Sup1)	380	
(3) DS-X9710-FAB1	450	

Module	BTU	Chassis w/o FC modules
DS-C9710 w Fans	No Data	- BTU
(2) DS-X97-SF1-K9 (Sup1)	-	
(3) DS-X9710-FAB1	-	

MDS 9513 FC Modules

Module	Watts	Ports	Watts per Port
DS-X9232-256K9 (Gen4 Adv Mod)	302	32	9.44
DS-X9248-256K9 (Gen4 Adv Mod)	310	48	6.45

Module	BTU	Ports	BTU per Port
DS-X9232-256K9 (Gen4 Adv Mod)	1323	32	41.34
DS-X9248-256K9 (Gen4 Adv Mod)	1387	48	28.90

MDS 9513 Chassis and Supervisor

Module	Watts	Chassis w/o FC modules
DS-C9513 w/ Front and Rear Fans	318	670 Watts
(2) DS-x9530-SF2A-K9	352	

Module	BTU	Chassis w/o FC modules
DS-C9513 w/ Front and Rear Fans	1358	2434 BTU
(2) DS-x9530-SF2A-K9	1076	

MDS 9148 Switch

Switch/Module	Watts	Ports	Watts per Port
MDS 9148 switch	120	48	2.5
MDS 9148s	125	48	2.6

Switch/Module	BTU	Ports	BTU per Port
MDS 9148 switch	410	48	8.54
MDS 9148s switch	410	48	8.54

3.3. Ethernet and Console Connections

For new SAN implementations the following are recommended:

- **Dedicated IP subnet for the MDS's** and the management stations
- (2) **100 or 1000 Mbps full duplex** Ethernet connections, and
- (2) Cisco RS232 console connections going to a terminal server²
- Each MDS Supervisor uses its own Ethernet and Console connections. Although two Ethernet connections are used, the switch only needs one IP address

3.4. Keep Fan Tray Clear

On the 9513 and 9506 switches, there is a full height fan tray on the left of the switch. Whenever a fan fails, the entire tray has to be pulled out and replaced within 5 minutes. If the tray is not replaced within that time, the switch will shutdown to prevent damage to the circuitry. **It is very important that cables do not obstruct the removal and insertion of the fan tray.**

3.5. Power Supply Circuits

MDS 9500 series switch comes with two power supply units, and each unit has two power connections. The best practice is to connect both connections of each power supply to the same power circuit, and each power supply to a different power circuit. This way if one power circuit fails, only one power supply will be impacted. Because the switch uses power supplies in a redundant fashion, failure of one power supply will not bring down the overall power supply capacity.

The MDS 9710 director has power supply modules on the front of the chassis. The power supplies can be powered down/up individually. The 9710 has 8 slots for Power Supplies. A minimum of 3 are required. Additional Power Supplies provide redundancy. The Cisco and CATE recommendation is to install 6 power supplies, connecting 3 to one power circuit and 3 to a second power circuit.

² The console connections are required for (1) initial configuration of switch (2) recover from a bad ACL command (3) watch detailed firmware upgrade progress (4) recover from ACS related misconfiguration or outage

3.6. Infrastructure Fibre Channel Cabling

Leverage existing fibre plant (OM3) to accommodate SAN switch hardware for Edge-Core-Edge design in a central location until switch space capacity is reached.

- Core level director (ISL) switches (4 x Cisco MDS 9710) per fabric (total of 8 per SAN Island) will not grow based on design.
- Storage level director Edge switches count which initially are also (4 x Cisco MDS 9710) per fabric (total of 8 per SAN Island) will increase in the future as new storage hardware is procured. We need reserve some space for future expansion (estimating that number of storage edge switches may double in 4 to 5 years)
- Host level ToR switches (9148S) for server connectivity can be installed centrally until maximum capacity. Additional 9148S expansion will occur at either End-of-Row or Top of Rack close to the servers. Adding switches at End-of-Row or Top-of-Rack will reduce the amount of fibre cabling the SDT team will need to support for server connectivity (8 fibre uplinks for only ISLs vs. 96 fibre cables for direct server connectivity)
- Distance permitted, all ISL links will be configured at 16Gbps.
- In some instances where 9148S will be deployed in ToR or EoR and distance exceeds 16Gbps capabilities of multimode fibre, the ISL links will use 8Gbps SFPs instead of 16Gbps. ISL bandwidth at 8Gbps is not a concern as existing production utilization reports show ISL links are less than 25% utilized.
- Any remaining/available 16Gbps SFPs can be installed at the storage edge 9710 to allow for future 16Gbps storage array connections.
- All teams (SDT, Storage Ops and CATE) have agreed that single mode fibre and single mode GBIC will not be deployed as part of this solution as it is cost prohibitive.

3.6.1. 8Gb SFP Cable Distances

SFP+	Wavelength (nanometers)	Fiber Type	Core Size (microns)	Baud Rate (GBd)	Cable Distance	Optical Multimode Classification
DS-SFP-FC8G-SW	850	MMF	62.5	2.125	150 m (492 ft)	OM1
			62.5	4.25	70 m (230 ft)	OM1
			62.5	8.5	21 m (69 ft)	OM1
			50	2.125	300 m (984 ft)	OM2
			50	4.25	150 m (492 ft)	OM2
			50	8.5	50 m (164 ft)	OM2
			50	2.125	500 m (1640 ft)	OM3
			50	4.25	380 m (1246 ft)	OM3
			50	8.5	150 m (492 ft)	OM3
			50	2.125	520 m (1706 ft)	OM4
			50	4.25	400 m (1312 ft)	OM4

			50	8.5	190 m (623 ft)	OM4
DS-SFP-FC8G-LW	1310	SMF	9	2.125	10 km (6.2 mi)	
			9	4.25	10 km (6.2 mi)	
			9	8.5	10 km (6.2 mi)	

3.6.2. 16Gb SFP Cable Distances

SFP+	Wavelength (nanometers)	Fiber Type	Core Size (microns)	Baud Rate (GBd)	Cable Distance	Optical Multimode Classification
DS-SFP-FC16G-SW	850	MMF	62.5	4.25	70 m (230 ft)	OM1
			62.5	8.5	21 m (69 ft)	OM1
			62.5	14.025	15 m (49 ft)	OM1
			50	4.25	150 m (492 ft)	OM2
			50	8.5	50 m (164 ft)	OM2
			50	14.025	35 m (115 ft)	OM2
			50	4.25	380 m (1247 ft)	OM3
			50	8.5	150 m (492 ft)	OM3
			50	14.025	100 m (328 ft)	OM3
			50	4.25	400 m (1312 ft)	OM4
			50	8.5	190 m (623 ft)	OM4
			50	14.025	125 m (410 ft)	OM4
DS-SFP-FC16G-LW	1310	SMF	9	14.025	10 km (6.2 mi)	
			9	8.5	10 km (6.2 mi)	
			9	4.25	10 km (6.2 mi)	

4. Fabric/Switch Management Infrastructure

4.1. Architecture

Please refer to the following figure, the MDS switches will be directly connected to the Citi corporate network, called Global Data Network (“GDN”). A Windows 2008 64-bit SOE server (“Management Server”) will be used to host software applications to manage one or more MDS switches and fabrics. The Management Server and MDS switches will reside on a dedicated corporate IP subnetnetwork. Although Cisco MDS management applications are Java based and can run on other platforms including Solaris, GDSE is certifying Windows because that opens up the possibility of using virtual servers instead of physical servers for cost reduction. Citi Storage Operations personnel will log on to this server from their SOE workstations using Windows Remote Desktop Client. SSH client on the Windows server and any other authorized servers can also be used to bring up a CLI session and to run scripts.

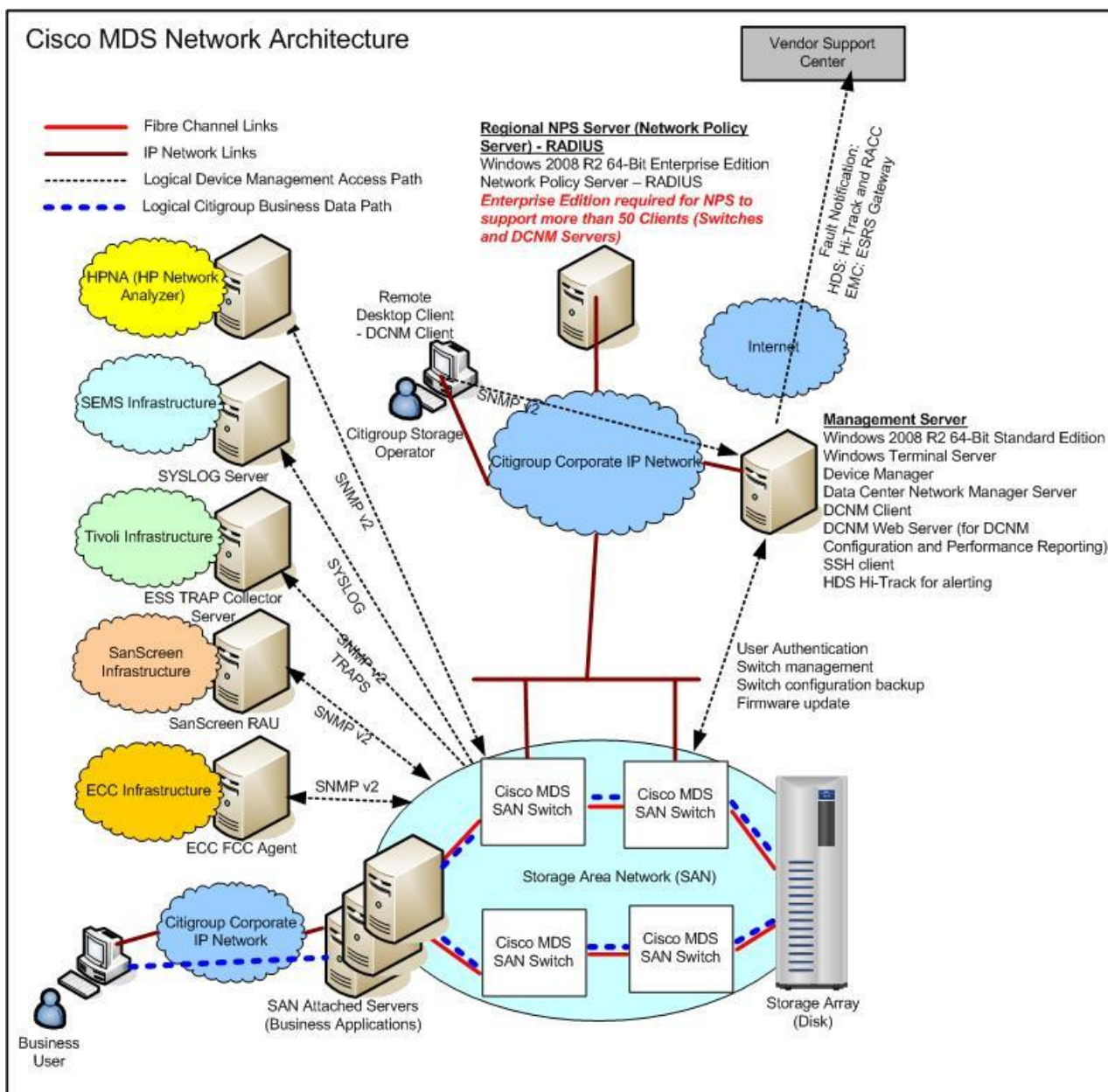
The switches will also interact with SYSLOG, ESS TRAP Collector, and SanScreen Remote Acquisition Unit (RAU) servers.

Syslog Server: GDSE recommends using a SOE Solaris server for capturing SYSLOG events emitted by the MDS switches. This is because the Solaris server already has a SYSLOG daemon that can do the job and GDSE has tested this configuration. Running a third party SYSLOG server on the Windows Management Server is an option; however there are three challenges with that approach:

1. There is not a certified SYSLOG server software for Windows SOE build
2. The Data Center Network Manager Server software itself uses UDP port 514 to listen to SYSLOG messages from the switches. This port cannot be reconfigured. In order for another SYSLOG server to run on the same server, the Management Server will have to be assigned a second IP address, and the SYSLOG server bound to that IP address. Alternatively, a different Windows server must be used.
3. GDSE has not tested this configuration

ESS Trap Collector Server: This server is a part of the ESS infrastructure.

SanScreen RAU Server: This is the server that runs the SanScreen RAU agent. Either an existing RAU server can be configured to additionally include the MDS switches, or the RAU agent can be installed on the Management Server itself.



4.2. Management Server Sizing and Placement

Managing fabrics across WAN links is not recommended because the GUI management applications interact with the switch in real time, and therefore user response is tightly linked to network performance. Each site should have its own Management Servers. To provide redundancy for DCNM operations, it's a good practice to have one DCNM management server for managing the "A" Fabrics in the data center and separate DCNM management server for managing the "B" Fabrics.

At least 12 GB of RAM is recommended on the server to support four simultaneous DCNM sessions. The Management Server can either be a physical server, or a virtual machine within ESX infrastructure.

4.3. Terminal Services License

The Management Server must be licensed for Terminal Services because the server will be accessed via Remote Desktop by Storage Operations personnel. Please consult with your SA on how to obtain and deploy this license.

4.4. RADIUS Authentication Server (NPS)

Previously, DCNM Client, Device Manager and SSH used Microsoft Interactive Authentication Server (IAS/Active Directory). Microsoft Network Policy Server has replaced IAS. On a Windows 2008 STANDARD Edition server, NPS has a 50 Client limit. A client is any device configured to authenticate with NPS. With the New SAN Architecture, with up to 40 MDS 9148's in a SAN, we will eclipse the number of supported NPS Clients. Windows 2008 Enterprise Edition server is required for NPS to support more than 50 Clients.

A server running Windows 2008 Enterprise Edition is required for NPS to support more than 50 Clients. Installing NPS on every DCNM server is no longer a requirement. NPS can be installed on two 2008 Enterprise Edition servers per region. All DCNM's and switches in the region can use these NPS servers for authentication.

The Data Center Network Manager Server can authenticate users via RADIUS protocol to Microsoft Network Policy Server (NPS), formerly known as Internet Authentication Service ("IAS"). NPS will accept user authentication requests from DCNM Client, Device Manager and SSH and pass it on to Active Directory. Please see **Section 5.7 and Section 7.1** for step-by-step instructions on how to configure NPS and Active Directory.

5. Management Server Build

Before upgrading or uninstalling Data Center Network Manager or Device Manager, make sure any instances of these applications have been shut down. If you are upgrading DCNM Server, be sure the previous installation of the database is running. Do NOT shutdown any of the DCNM services. Do NOT uninstall the previous version. The upgrade process will ask if you want to use an existing PostgreSQL database.

The installer detects your current version of DCNM and provides the option to upgrade. **GDSE recommends upgrading**, as this will preserve maps, enclosure names and local Fabric Manager Users.

Note: If you choose to uninstall the previous version of Data Center Network Manager software for a fresh install, uninstall the TPM package and uninstall DCNM from "Add Remove Programs".

5.1. Java Runtime Environment

Data Center Network Manager 6.3.2 installs Java Runtime Environment ("JRE"). JRE version 1.7.

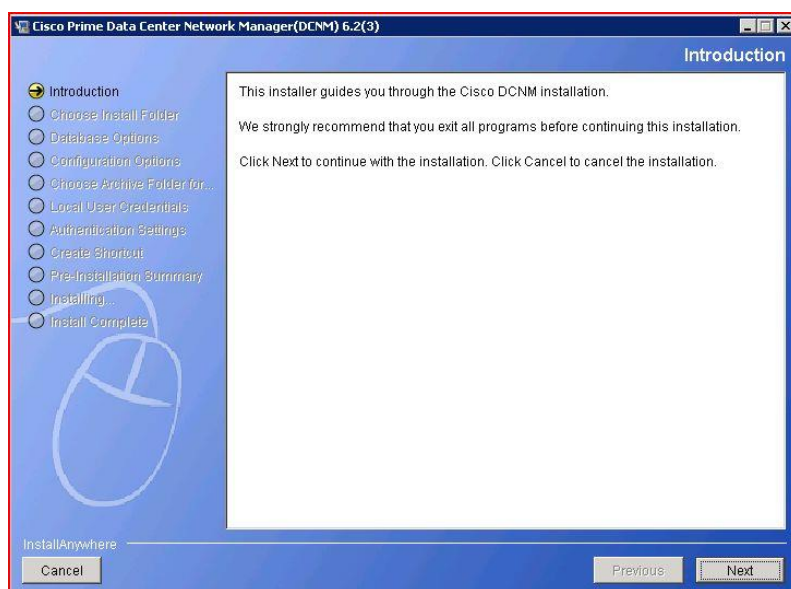
5.2. Install DCNM Server Components

These installation steps are for new installs of DCNM 6.3.2 on a Windows 2008 64-bit Server (only), **TPM package will install to C:\Cisco_DCNM_6.3.2.**

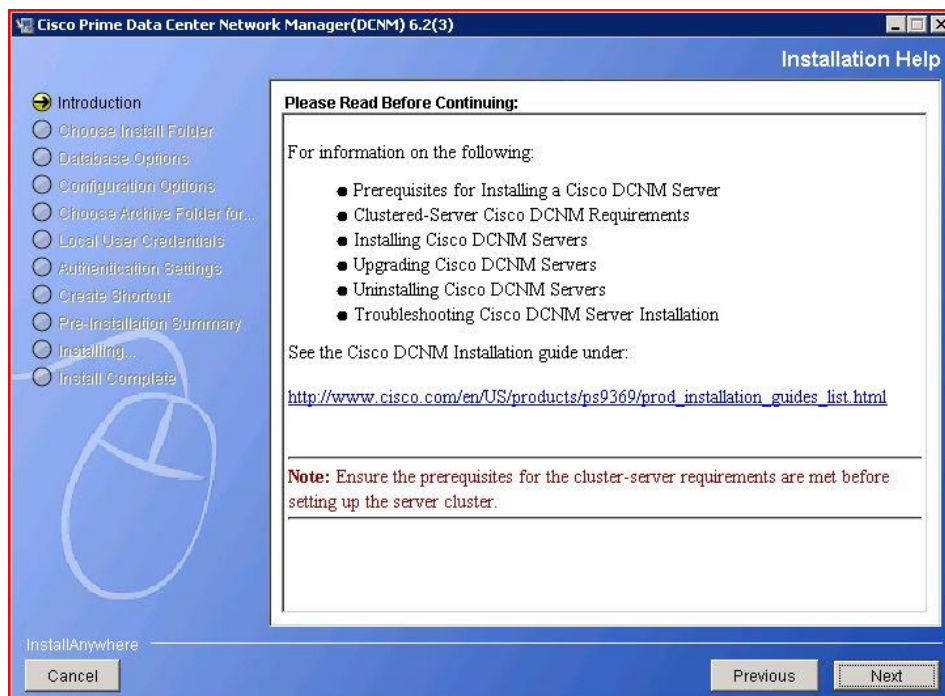
Windows 2008 TPM package: **CITI_WIN_2K8_DataCenterNetMgr_632_00**

5.2.1. Installing DCNM Server

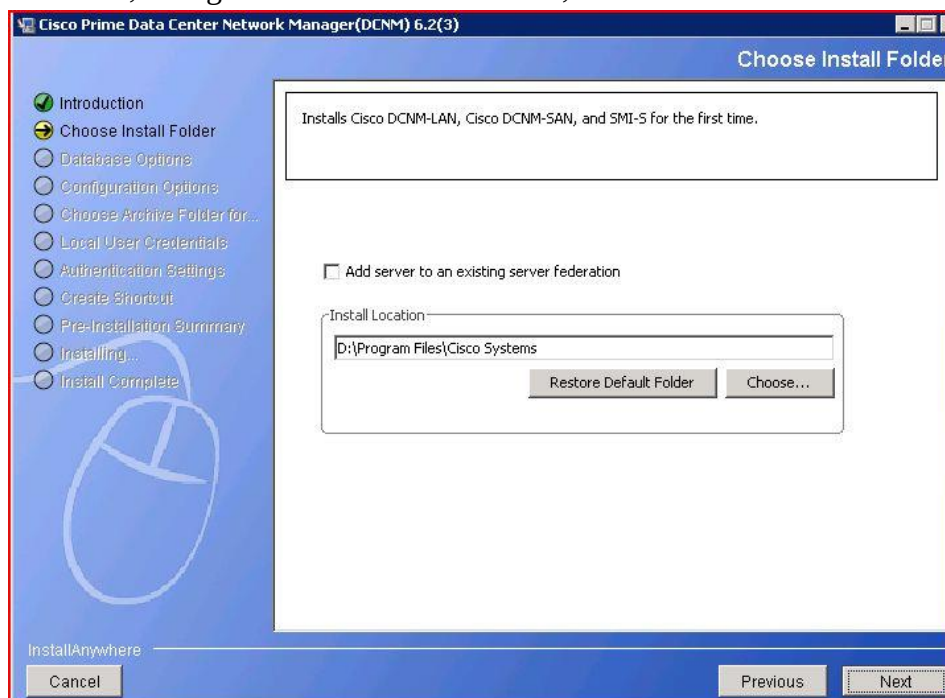
- Install DCNM Server, DCNM Client and Device Manager before upgrading NX-OS
 - Users installing DCNM Server must have full administrator privileges to create user accounts and start services
 - Installation must be performed via a “Console” (like VNC), or Remote Desktop with the console option (mstsc \console)
 - TFTP server is installed along with DCNM
 - **Adobe Flash 10** or higher is required for the DCNM Web Client
 - Make sure to review the [Cisco MDS NX-OS / DCNM Release Notes](#).
1. From the Windows 2008 server, launch TPM package:
CITI_WIN_2K8_DataCenterNetMgr_632_00
 2. Run the DCNM 6.3.2 install executable (**dcnm-installer-x64-windows.6.3.2.exe**) from C:\Cisco_DCNM_6.3.2.
 3. Click “Next”



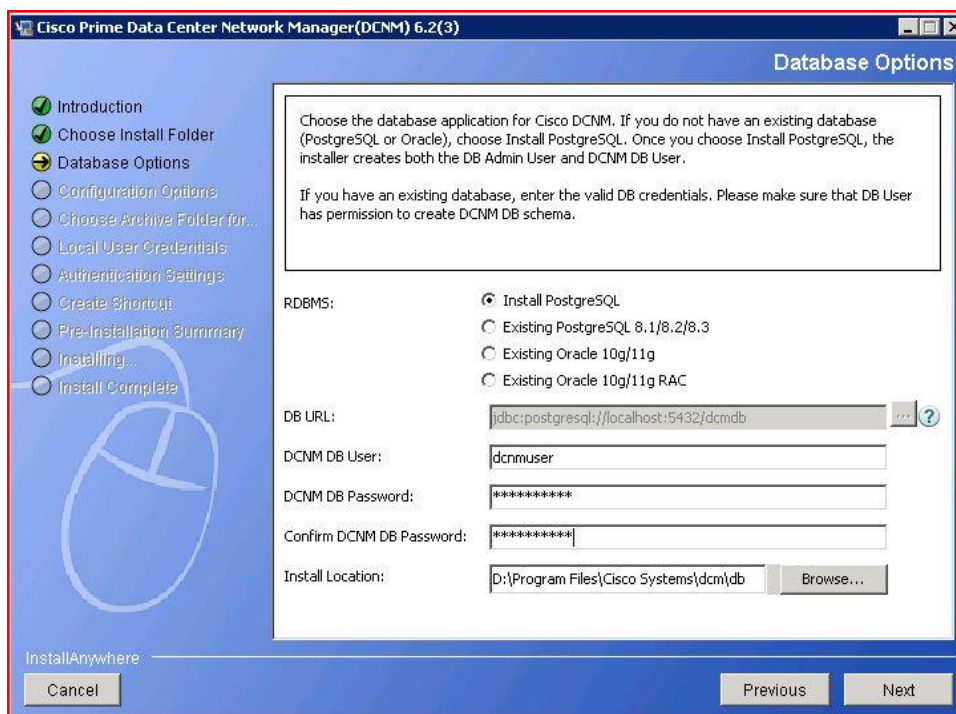
Click Next



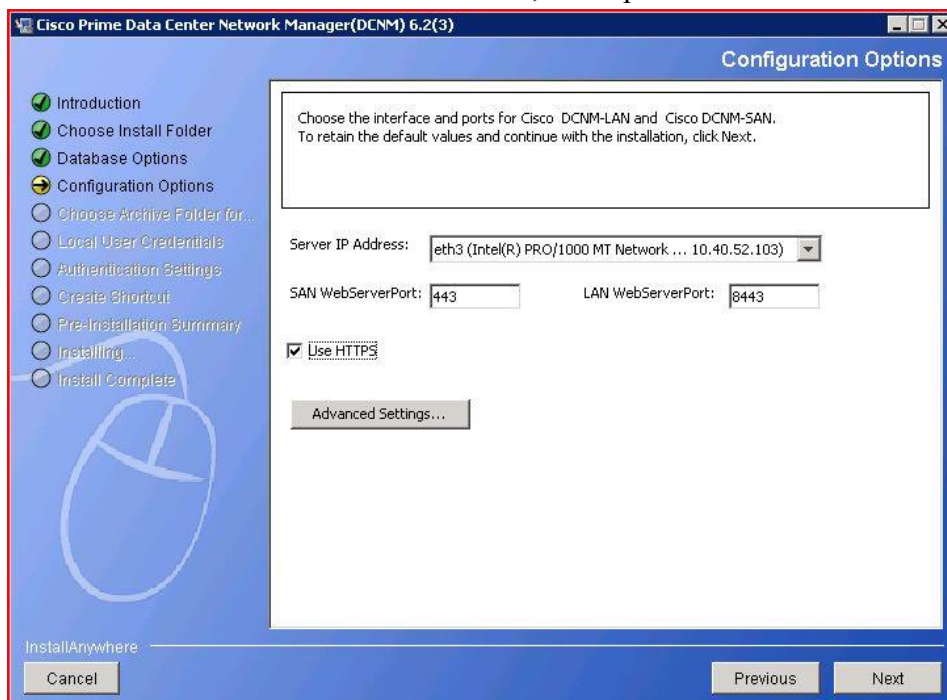
4. If desired, change the install location to D:\, Click “Next”



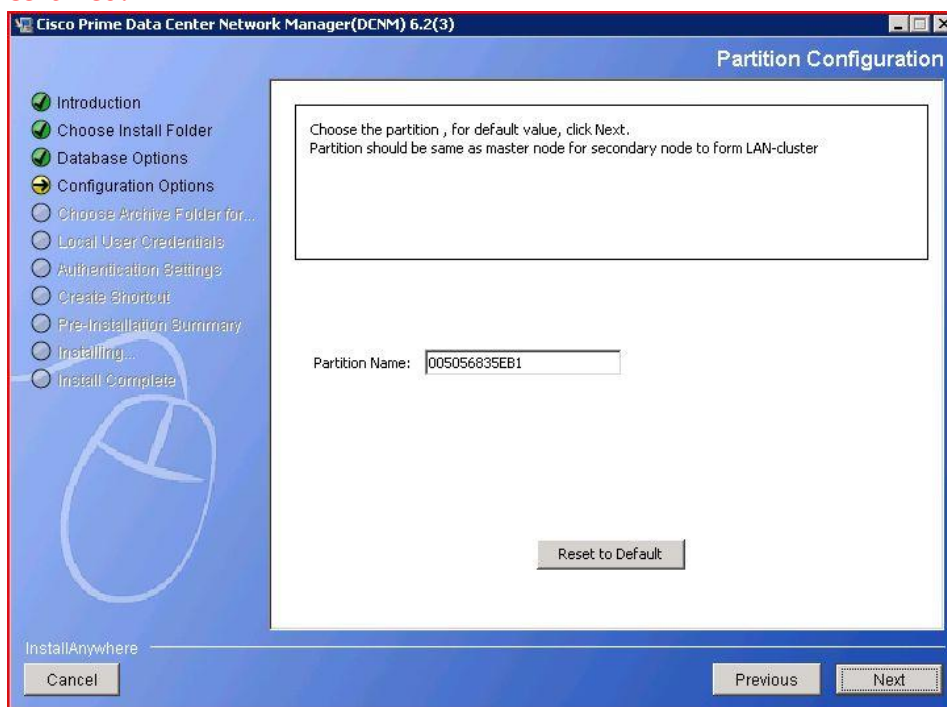
5. Select “**Install PostgreSQL**” radio button for a new install or “**Existing PostgreSQL**” for an upgrade. Enter the DCNM DB password and confirm it. If desired, verify D:\ is selected as the install location. Click “Next”



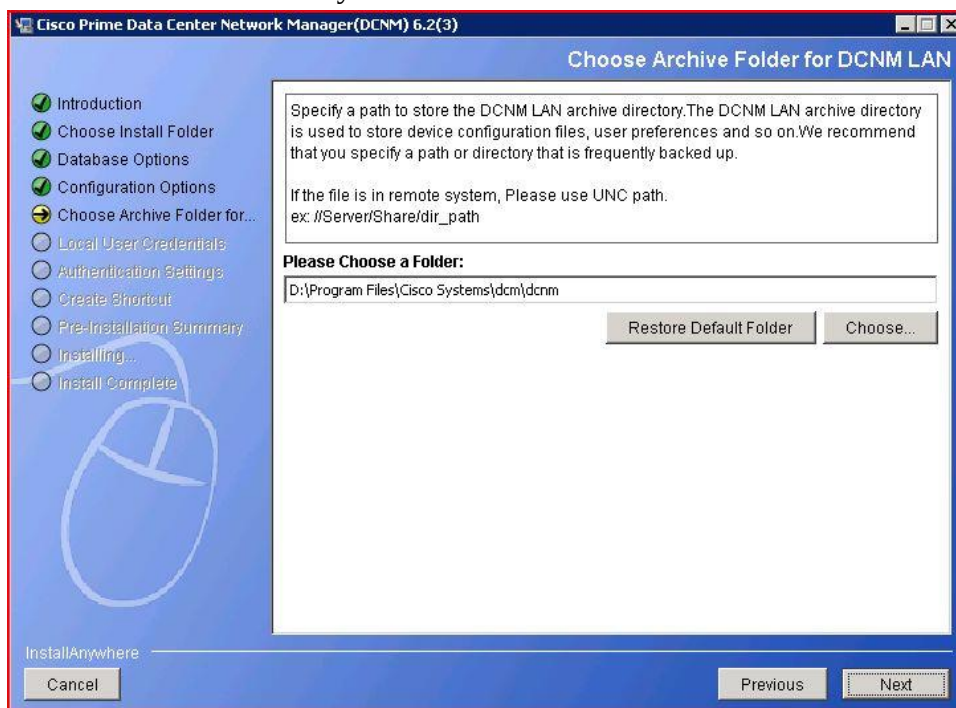
6. Click on the dropdown for **Server IP Address**. Select the Ethernet NIC. Select the checkbox to “**Use HTTPS Web Server**”, leave port 443 and click “Next”.



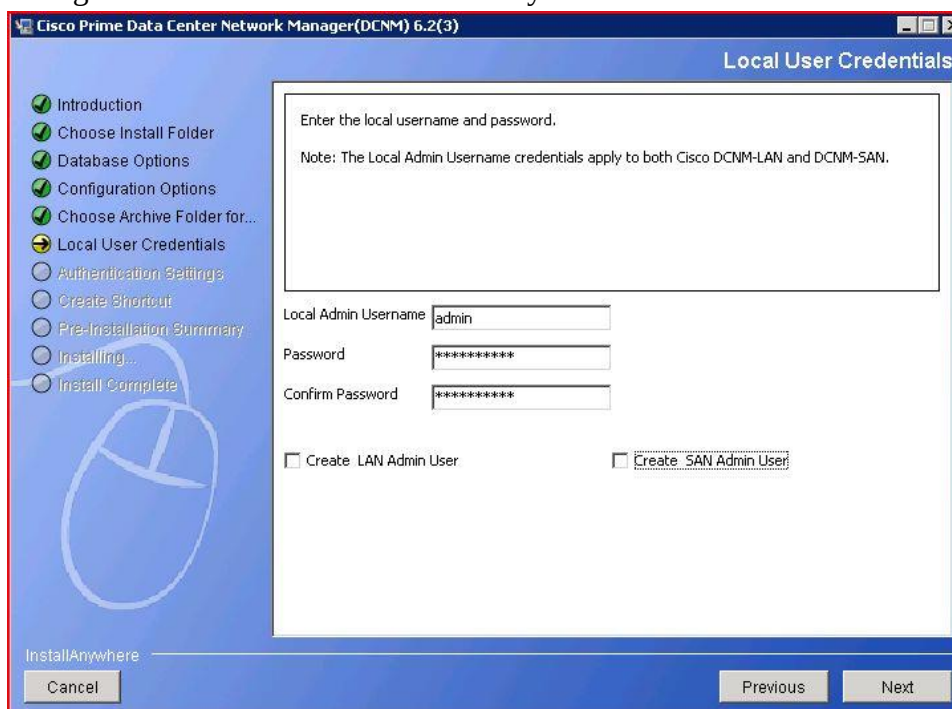
7. Leave the default value. **This is the MAC address of the server and it is used if installing in a Cluster (Federation) and for obtaining licensing. Federation was not certified.**



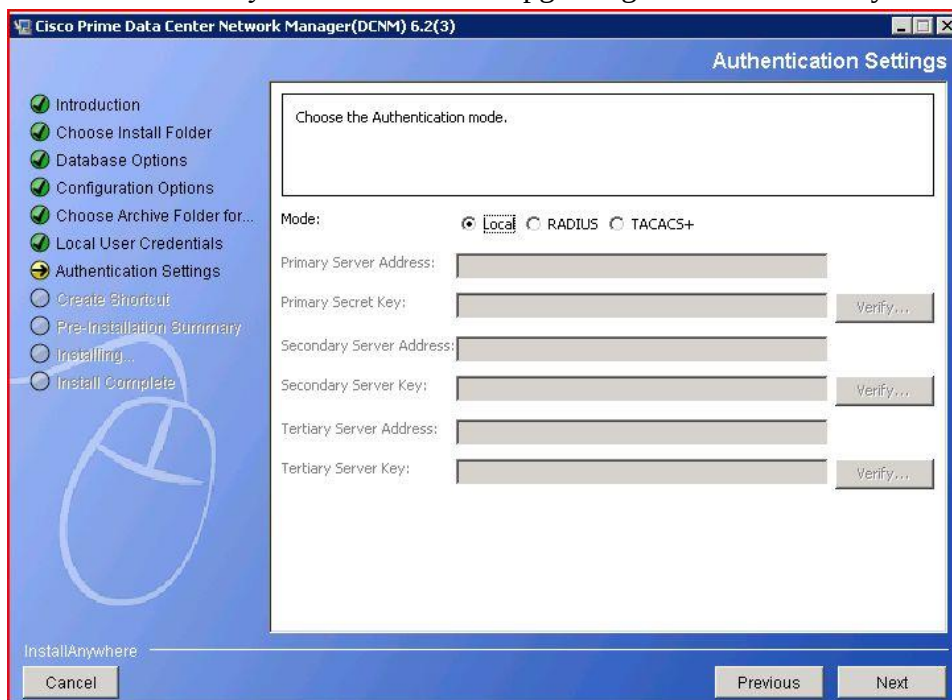
8. Leave the default directory and select Next.



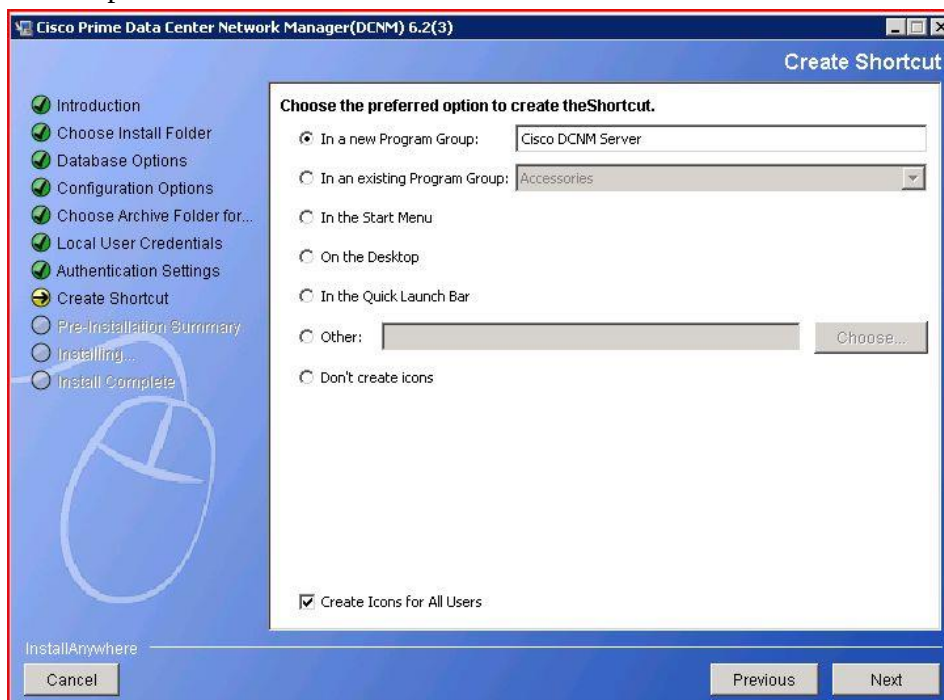
9. Enter the Local Admin Username and Password. This is temporary until DCNM is configured for RADIUS/Active Directory. Click “Next”.



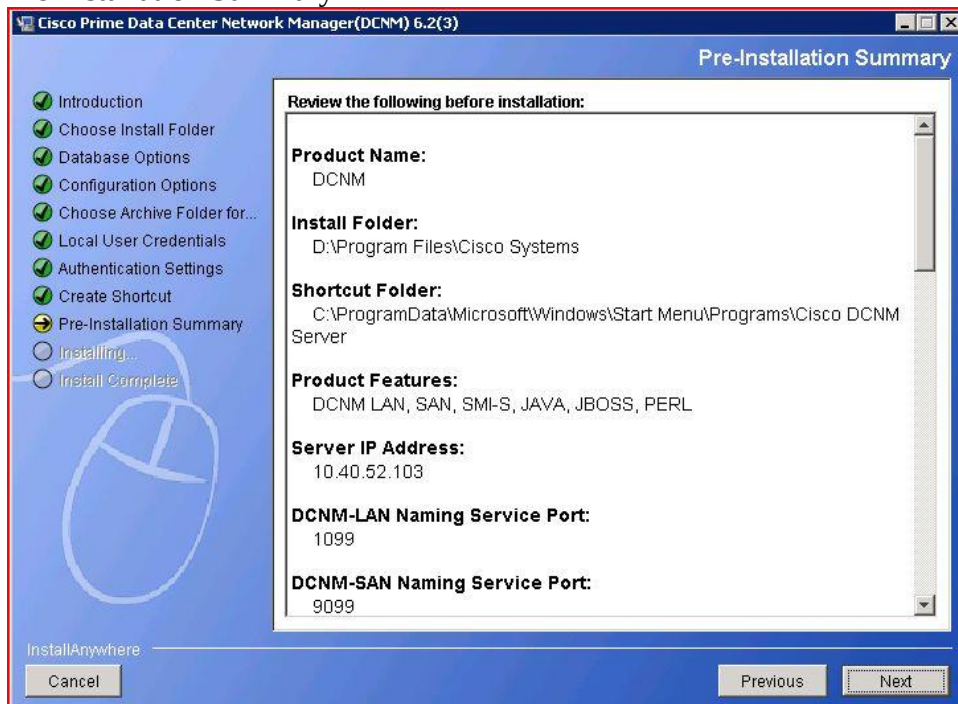
10. Click on the “Radius” radio button and enter the Primary and Secondary RADIUS servers and the “Secret Key”. Click “Next”. If upgrading this should already be filled in.



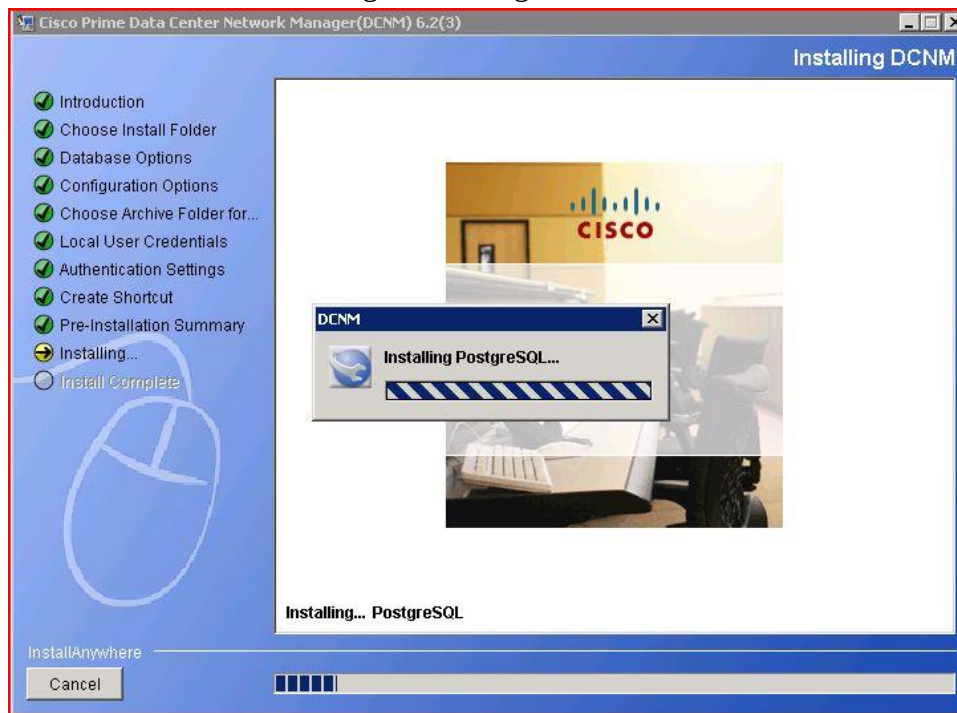
11. This step creates the shortcuts. Click “Next”.



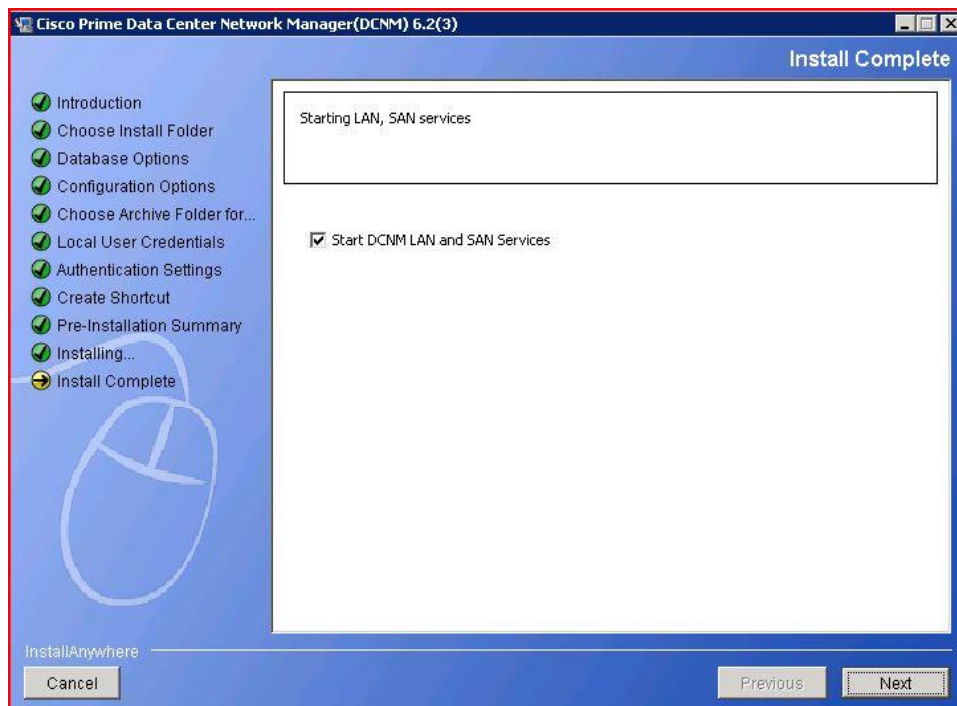
Pre-installation Summary



12. Data Center Network Manager 6.2.5 begins to install.



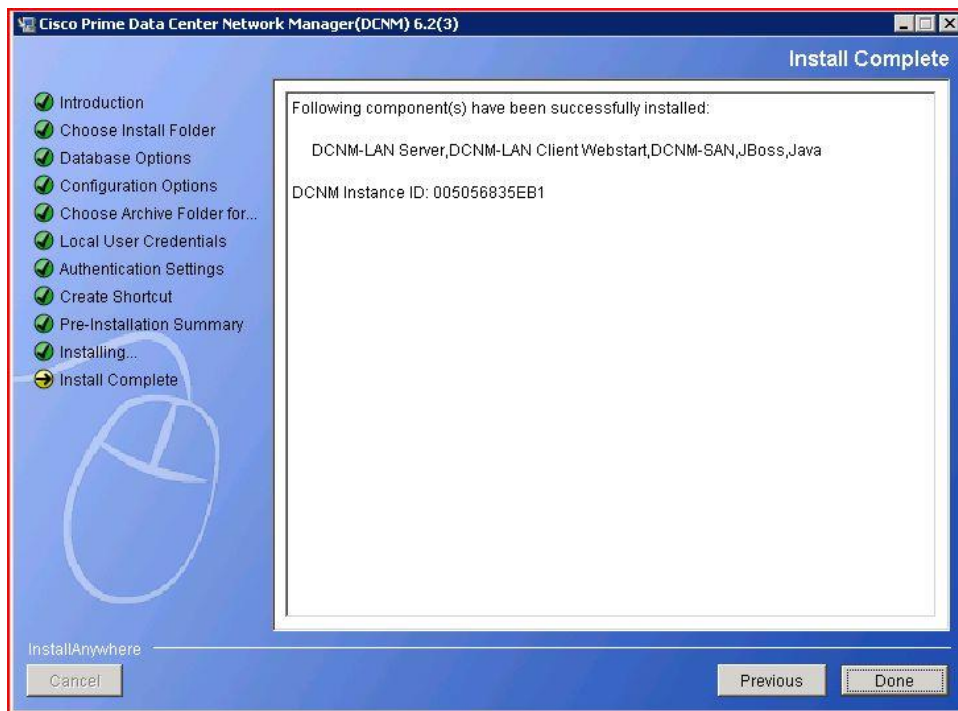
13. Select the checkbox to “Start DCNM-SAN Service” and click “Next”.



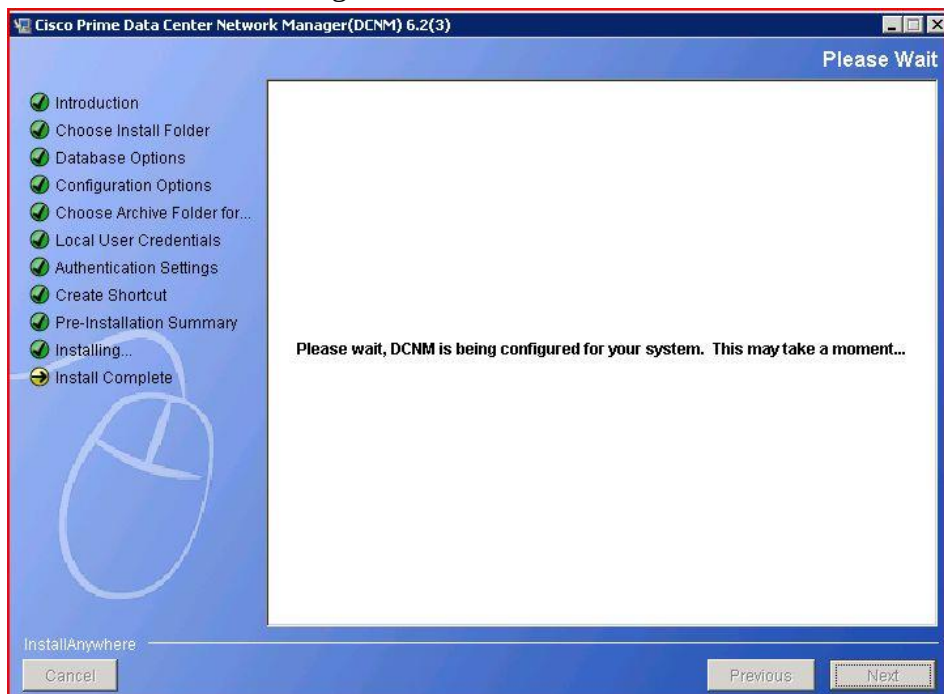
14.

15. DCNM-SAN server installation is complete, Click “Done”.

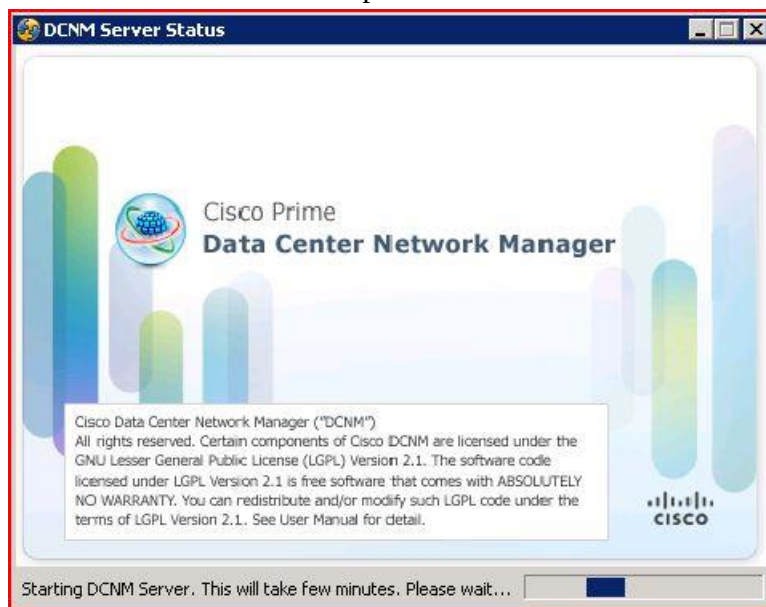
Note: DCNM Client and Device Manager still need to be installed. They are installed from the DCNM Web Client.



DCNM finishes the configuration.

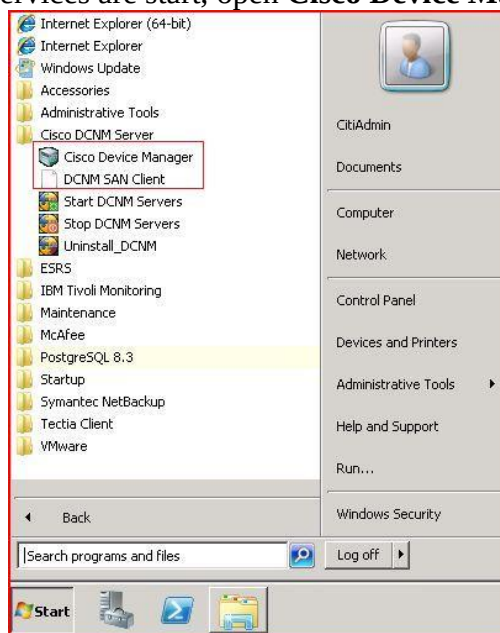


Cisco DCNM service startup.



5.2.2. *Device Manager and DCNM Client Installed*

DCNM Client and Device Manager 6.3.2 are installed when the DCNM Server is installed. On the DCNM Server, go to “*Start/All Programs/Cisco DCNM Server*”, click on “*Start DCNM Servers*”. Once services are start, open **Cisco Device Manager** or **DCNM SAN Client**.

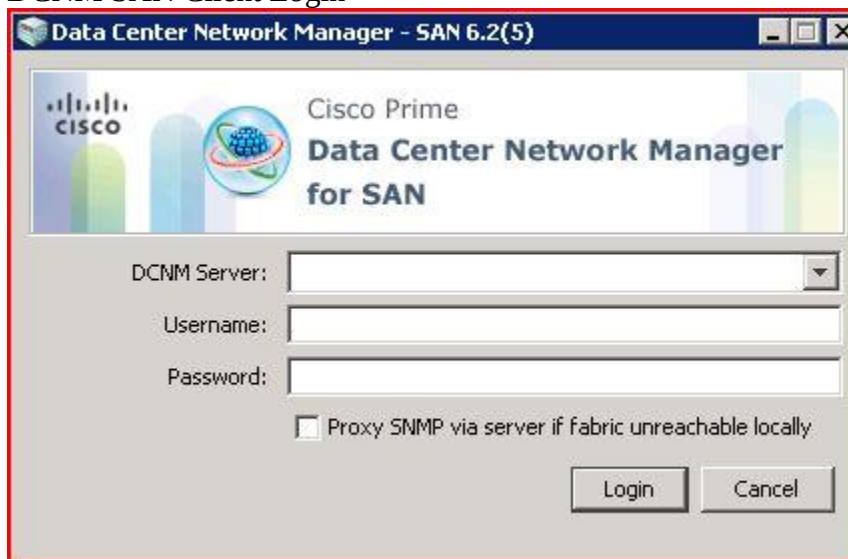


Device Manager Login



The dialog box titled "Device Manager 6.2(5) - Open" features the Cisco logo at the top. Below the logo are three input fields: "Device Name:" with a dropdown arrow, "User Name:", and "Password:". At the bottom, there are three buttons: "Open", "Options >>", and "Close".

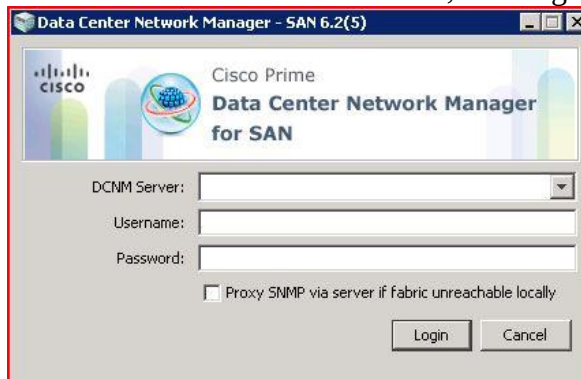
DCNM SAN Client Login



The dialog box titled "Data Center Network Manager - SAN 6.2(5)" displays the Cisco Prime logo and the text "Data Center Network Manager for SAN". It includes three input fields: "DCNM Server:" with a dropdown arrow, "Username:", and "Password:". Below these fields is a checkbox labeled "Proxy SNMP via server if fabric unreachable locally". At the bottom right, there are "Login" and "Cancel" buttons.

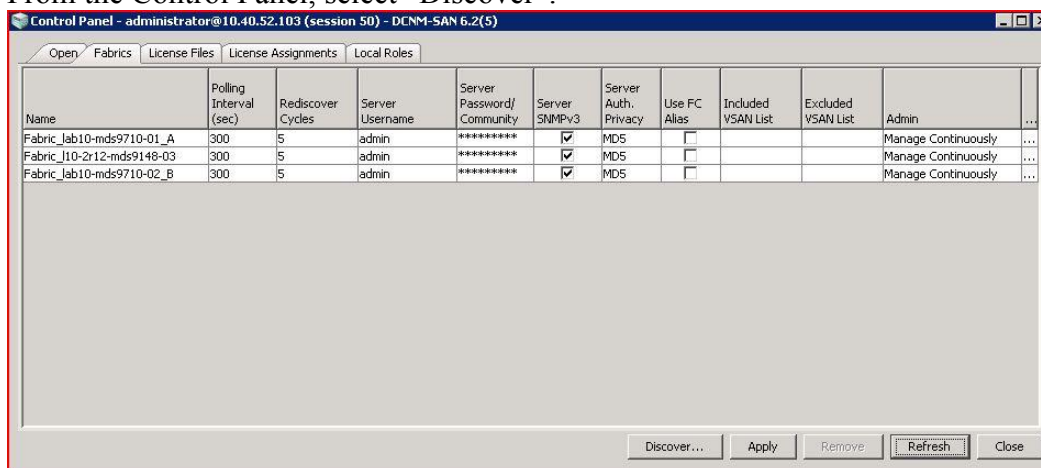
5.2.3. Discover SAN Fabric

3. Enter IP address of DCNM Server, then login with your ID and Password.

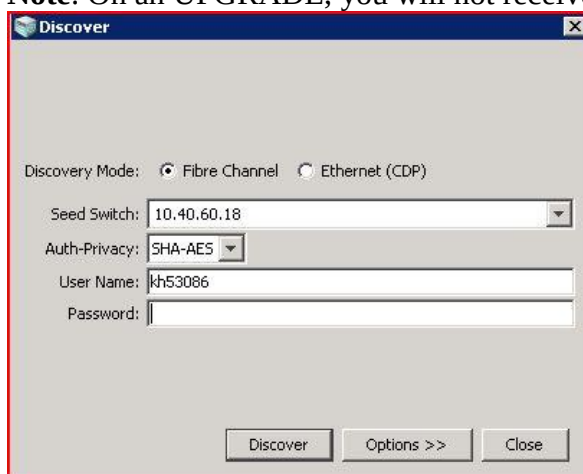


This is a duplicate of the "Data Center Network Manager - SAN 6.2(5)" login dialog box shown above. It contains the same fields for "DCNM Server:", "Username:", "Password:", and the "Proxy SNMP" checkbox, along with "Login" and "Cancel" buttons.

4. From the Control Panel, select “Discover”.



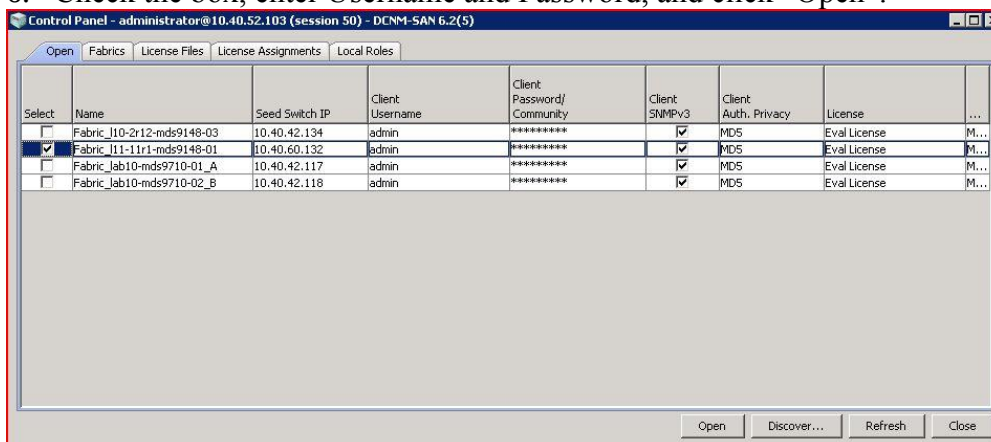
5. Enter the Seed Switch IP address, Admin ID and password of the switch. Click “Discover”.
If authenticating to **Active Directory**, use an Active Directory ID/Password/**SHA-AES**.
Note: On an UPGRADE, you will not receive this dialog box. Skip to next step.



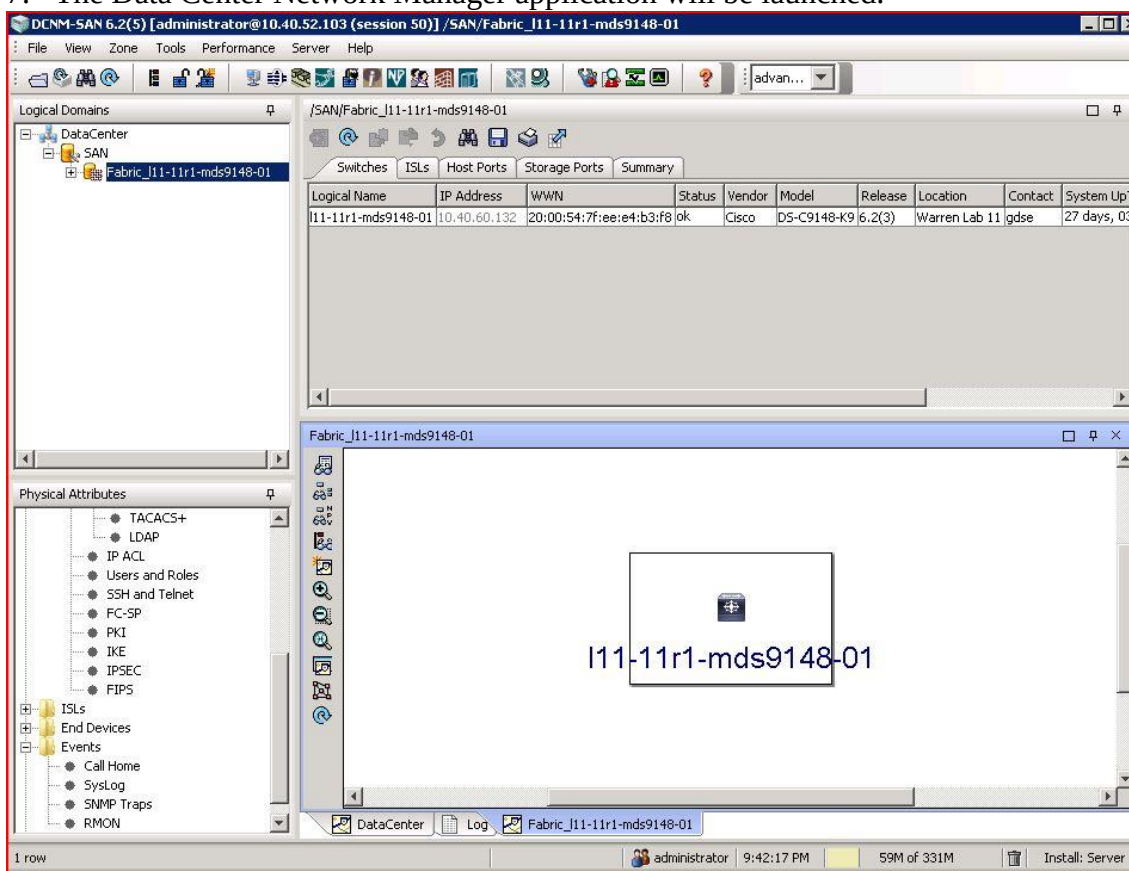
Switch will be discovered.



6. Check the box, enter Username and Password, and click “Open”.



7. The Data Center Network Manager application will be launched.



5.3. Install SSH Client

Install Tectia Client version 6.2.1 (or the latest version) from TPM packages:

CITI_WIN_TectiaSSHClient_621_03

This will install SSH client on the server.

5.4. Install SFTP Server

Install Tectia Server version 6.2.1 (or the latest version) from TPM packages:

CITI_WIN_TectiaSSHServer_621_04

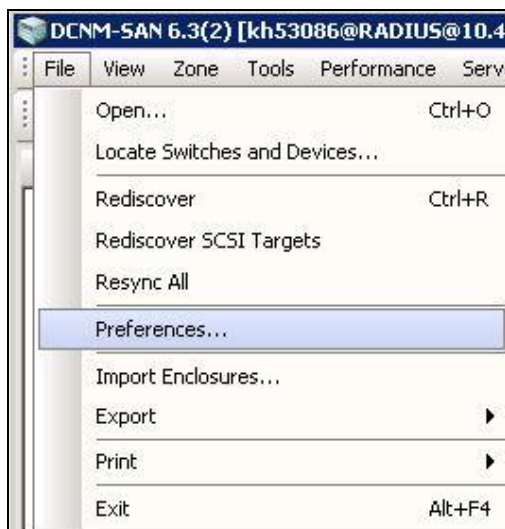
This will install the SSH server (w/SFTP) that can be accessed from the switch for exchanging firmware, configuration, script and license files.

Cancel the request to reboot the server. We will reboot once we are finished with other configuration.

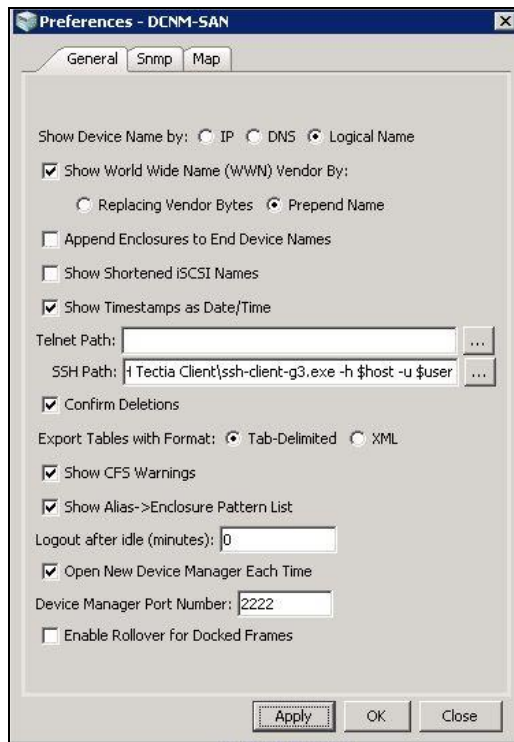
5.5. Configure DCNM with Citi SSH

Data Center Network Manager allows you to right click on a device on the map to start a CLI session to the device. This is a very convenient feature. Since Telnet is not applicable at Citi, SSH must be configured.

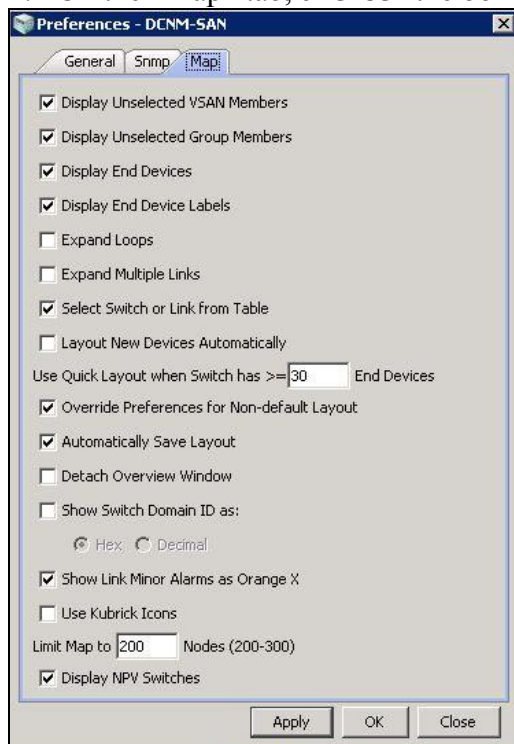
1. Log in to Data Center Network Manager, click on File > Preferences



2. On the "General" tab, remove (blank out) the path in "Telnet Path:" Telnet is disabled on the switches by default.
Enter the SSH Path:
C:\Program Files (x86)\SSH Communications Security\SSH Tectia\SSH Tectia Client\ssh-client-g3 -h \$host -u \$user
3. Check the box to "**Open New Device Manager Each Time**".



4. On the “Map” tab, uncheck the box “Use Kubrick Icons”, to show switch icons.



Note: This configuration is stored in the user profile. As users are added to Data Center Network Manager, each user must follow the above procedure to enable SSH from the GUI.

5.6. Configure Call-Home

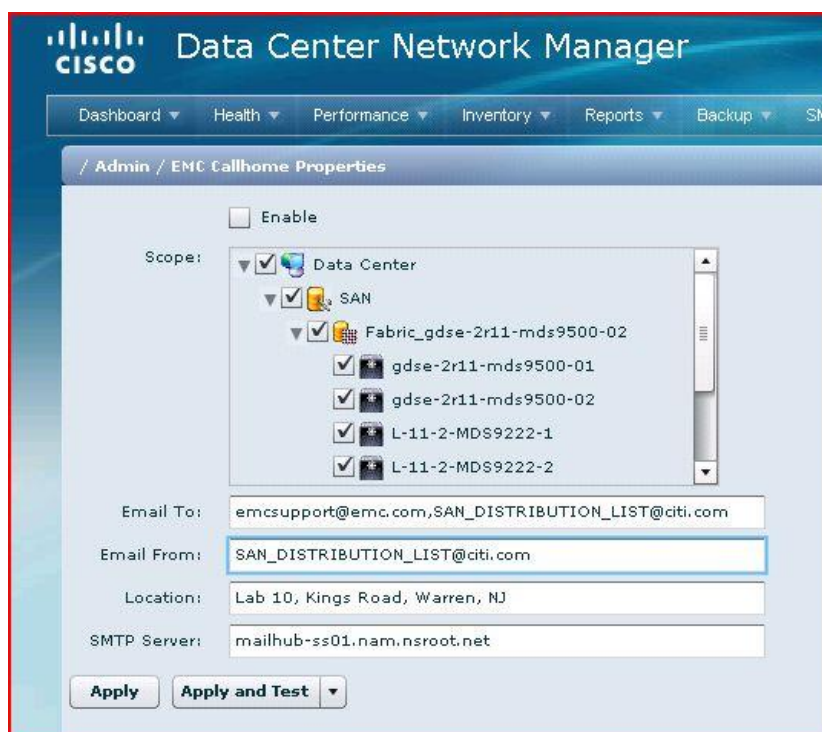
5.6.1. Call-Home to EMC

When the MDS switches are supported by EMC, the Data Center Network Manager Server should be configured to send fault alerts to EMC support center. DCNM will be set up to relay email to a Citi mail relay server. Configuration is **no longer performed** via the **server.properties** files.

1. Using Internet Explorer, browse to https://dcnm_server_ip_address, log in with an SOEID and password. Select “**Admin**”, then click on “**EMC Callhome**”.



2. Enable callhome to EMC by checking the “**Enable**” box. Expand the SAN and deselect any switches not supported by EMC. Enter mail information:
 Email to: **emcsupport@emc.com,santeam@citi.com** (comma separated, no spaces)
 Email from: **santeam@citi.com**
 Location: **street address of SAN site**
 SMTP Server: **Citi SMTP relay server. Obtain from Citi SMTP team.**



Note: For Call-Home to EMC to work, DCNM must be configured to monitor fabrics continuously. GDSE recommends using the admin ID to monitor the fabrics. If at any time the password of the admin account is changed, the monitor continuously configuration must be repeated.

5.6.2. Call-Home to HDS

When the MDS switches are supported by HDS, the following configuration should be used to enable call-home to HDS support center. HDS provides free software called “Hi-Track” to monitor the Cisco MDS switches. This software uses read-only SNMP v1 to periodically run a health check on the switches being monitored. Fault reports are collected into a file and periodically sent to the HDS support center by using HTTPS transport. The support center reviews the fault report and tasks customer support engineers in the field.

Note: Completely uninstall previous version of Hi-Track, before installing new version.

GDSE has certified version 7.1 of Hi-Track monitor. This software is available via TPM, Package ID: **CITI_WIN_2K8R2_Hitrack_71_00**. This package will copy the install programs to C:\Hi-Track_v7.1.

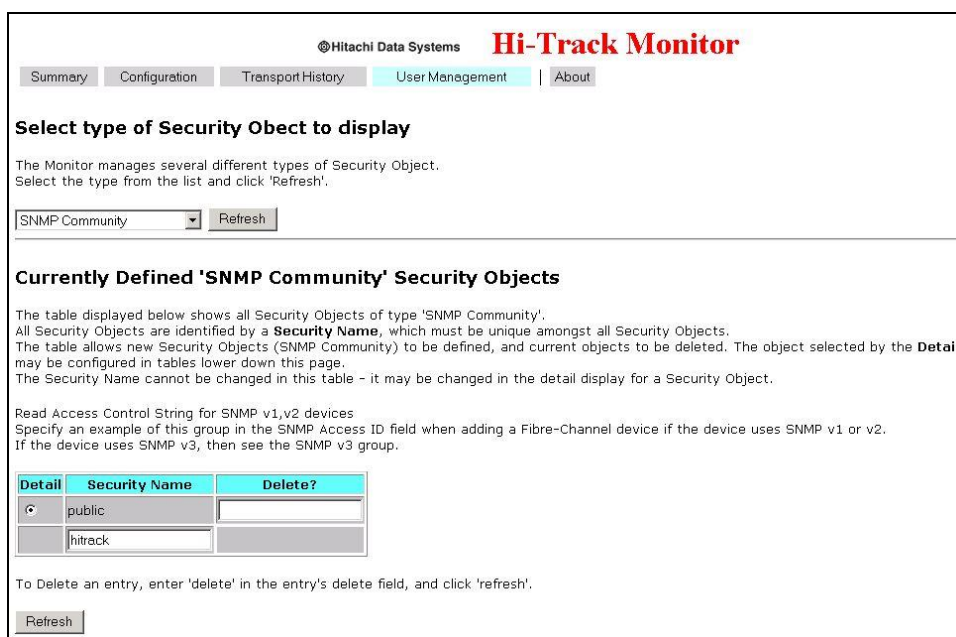
1. CheckSpecial.cmd – this will perform a pre-install check and at the end, run the install (HTinst.exe)
2. HTinst.exe

Double click on CheckSpecial.cmd to start the installation. Select all default options during the install.

Please have HDS support person assist you with this configuration. You will need several pieces of information from HDS before you can complete the configuration.

Browse to <http://127.0.0.1:6696> on the Management Server. Select “Administrator” user ID and password “hds” to logon.

1. After you install Hi-Track v7.1, launch the Hi-Track web portal from the icon on the desktop and login (administrator / hds).
Click on the User Management tab. To create the community string to be used to poll the switches, select “SNMP Community” from the dropdown. Enter “hitrack” and click on Refresh button.



©Hitachi Data Systems **Hi-Track Monitor**

Summary Configuration Transport History **User Management** About

Select type of Security Object to display

The Monitor manages several different types of Security Object.
Select the type from the list and click 'Refresh'.

SNMP Community Refresh

Currently Defined 'SNMP Community' Security Objects

The table displayed below shows all Security Objects of type 'SNMP Community'.
All Security Objects are identified by a **Security Name**, which must be unique amongst all Security Objects.
The table allows new Security Objects (SNMP Community) to be defined, and current objects to be deleted. The object selected by the **Detail** may be configured in tables lower down this page.
The Security Name cannot be changed in this table - it may be changed in the detail display for a Security Object.

Read Access Control String for SNMP v1,v2 devices:
Specify an example of this group in the SNMP Access ID field when adding a Fibre-Channel device if the device uses SNMP v1 or v2.
If the device uses SNMP v3, then see the SNMP v3 group.

Detail	Security Name	Delete?
☒	public	
☐	hitrack	

To Delete an entry, enter 'delete' in the entry's delete field, and click 'refresh'.

Refresh

When completed, it will look like this.

Hitachi Data Systems **Hi-Track Monitor**

Summary Configuration Transport History **User Management** | About

Read Access Control String for SNMP v1,v2 devices
Specify an example of this group in the SNMP Access ID field when adding a Fibre-Channel device if the device uses S
If the device uses SNMP v3, then see the SNMP v3 group.

Detail	Security Name	Delete?
☒	hitrack	
☐	public	
	-Add New User Here-	

To Delete an entry, enter 'delete' in the entry's delete field, and click 'refresh'.

Detail for SNMP Community 'hitrack'

The **Security Name** is used to display this object in all selection lists.
The **Community ID** parameter will be used during communication with the device.
By default, Security Name will be equal to Community ID..

Security Name:

Community ID.:

- Click on the Configuration tab, then Base. Enter site ID, Scan Interval, SNMP Timeout and change the daily report to 04:00. The rest of the settings for Base are default. The 2nd screenshot is for email notification and is located below the device monitoring (on the same screen). Configure it for your regional email systems.

Hitachi Data Systems **Hi-Track Monitor**

Summary **Configuration** Transport History User Management | About

Configuration

Base Transport Agents Device Polling Local TCP/IP Debug/Trace Backup Timezone

This page displays the Hi-Track Monitor configuration settings.
Most configuration changes are immediate. Other changes require a restart to make the changes current. See each table for details.

Device Monitoring

Changes to entries in this table do not require a restart.

[Help on this table's entries](#)

Name	Value	Default	Min	Max	Units
Site ID	R054665				
Scan Interval	360	150	60	3600	Seconds
Max SNMP Poll Period		600	3	3600	Seconds
SNMP Timeout	3	9	1	60	Seconds
Daily Report	04:00	06:30	00:01	23:59	Hours:Minutes

Email notification setup.

Configuration

Base Transport Agents Device Polling Local TCP/IP Debug/Trace Backup Timezone

The Sender's Email Address may be set as follows :-

- Leave Blank - the Sender's address will be 'Hi-Track@domainName', where domainName is the local TC device. This is the preferred option.
- Define name without domainName - If a name without a '@' character is entered, then that name will 'inputName@domainName'.
- Define full sender's name - If the entered name contains the '@' character, then this will be used unmodified option with your mail service administrator for security reasons.

The HELO/EHLO parameter should be left blank. Hi-Track will use the name of the local host. If this is not a value here.

This feature may be tested by clicking this 'Test Email' button at the bottom of this page. The Test Email button does not implement any configuration changes from this form. Only 'Email Limit Count' emails will be sent in any 'Email Limit Time' minute period. Any additional emails will be disabled.

name	value
eMail Server	mailhub-na.wlb.nam.nsroot.net Local Interface: eth0
User List	0
Sender's Email Address	kevin.hobaugh@citi.com
SSL Mode	None Authentication Mode User/Password
SMTP User	
SMTP Password	
HELO/EHLO parameter	
Subject Line	

[Help on Mail Subject Line Data](#)

Submit Reset

- Under Configuration, click on Transport Agents. Enter the information as shown.

There are two possible location/user ID combinations to use. The location/user ID determines whether the data will end up on the ROW (San Diego) Hi-Track Server or on the European Hi-Track server.

HDS **North America** Hi-Track Server.

Location: **ushtinet01.hds.com** (or **ushtinet02.hds.com** for the alternate location)

User: **ht_http_row**

Password: **htpw0425**

HDS **Europe** Hi-Track Server.

Location: **ushtinet01.hds.com** (or **ushtinet02.hds.com** for the alternate location)

User: **ht_http_eu**

Password: **htpw0425**

Use your regions webproxy (no password required for webproxy, it just puts asterisks in the field.


Hi-Track Monitor

Summary
Configuration
Transport History
User Management
About

Configuration

Base
Transport Agents
Device Polling
Local TCP/IP
Debug/Trace
Backup
Timezone

Index	Move to Top?	Enabled ?	Type	Destination
1	☐	yes	HTTPS	ushtinet02.hds.com:443/ht_http_row
2	☐	yes	HTTPS	ushtinet01.hds.com:443/ht_http_row

The Transport Agents will be called in the order shown.
 Transport Agents that are not enabled will not be called.
 You may change the order by moving one agent to the top of the list.
 The order will be updated just after midnight each day by moving the first entry to the bottom of the list, and all d

Detail configuration for HTTP(s) Agent selected in list above.

HDS Host:	ushtinet02.hds.com
Local Interface:	-any-
Port:	443
UserName:	ht_http_row
Password:	
Proxy Type:	HTTP Tunnel
Proxy Host or IP:	webproxy.wlb2.nam.nsr
Proxy Port:	8080
Proxy Username:	
Proxy Password:	
Reconnect For Each File ?	☐
Enabled ?	☒
Delete ?	

- Under Configuration, click on Device Polling. Scroll down to Cisco Switch or Director and change the field from “1” to “4”. Click on Modify.


Hi-Track Monitor

Summary | Configuration | Transport History | User Management | About

Configuration

Base	Transport Agents	Device Polling	Local TCP/IP	Debug/Trace	Backup	Timezone
Hitachi Compute Blade Server		symphony	1	☐		
Hitachi Compute Blade I/O Expansion Unit (IOEU)		cbioexp	1	☐		
Hitachi CB 500		cb500	1	☐		
Hitachi CB 2500		cb2500	1	☐		
HDI, HCO, HNAS F		hdi	1	☐		
Hitachi CR220 Server		cr220	1	☐		
Hitachi CR xM (CR 2x0H/S)		cr2x0hs	1	☐		
Hitachi Enterprise RAID		usp	1	☐		
Hitachi Scale-Out Platform (SOP)		hsop	1	☐		
Hitachi UCP Director		ucpdir	1	☐		
QuantaPlex T41S-2U Server		quanta2u	1	☐		
Hitachi Protection Platform (HPP)		hpp	1	☐		
Benning UPS Manager		benning	1	☐		
Brocade Switch or Director		brocade	1	☐		
Cisco Switch or Director		cisco	4	☐		100 minutes
McData Switch or Director		mcd	1	☐		
QLogic Switch		qlogic	1	☐		
Qlogic ISR Router		qisr	1	☐		

Modify | Reset

- To accommodate the large number of devices in our SAN, add the following parameter to C:\hds\HitDFmon\HitDFmon.config to increase the SNMP operations limit.
SnmpOpLimit = 50000
 Save the file and restart the HiTrack service.

6. To add devices to monitor, click on Summary. Click on “Item”. You can select Cisco switch from the dropdown.

©Hitachi Data Systems **Hi-Track Monitor**

Summary Configuration Transport History User Management About

Refresh Page Created: 2014/10/31 13:13:23

Device Error	Comms. Error	Device Okay	Not Monitored	Total Devices	Refresh	Devices / Page
☒ 0	☒ 0	☒ 4	☒ 0	4	60 Secs	40

Devices Okay

Item	Name	Location	Group	Type	Model	Serial	Status	Last Communication	Site ID	IP Address 1	IP Address 2
1	2R12-MDS9710-01	283 KING GEORGE ROAD, Warren, NJ 07059		Cisco	DS-C9710	JAF1802AFDE	D 87 Warnings	2014/10/31 13:10:10	R054665	10.40.42.117	
2	2R12-MDS9710-02	283 KING GEORGE ROAD, Warren, NJ 07059		Cisco	DS-C9710	JAF1801ARFH	D 83 Warnings	2014/10/31 13:10:52	R054665	10.40.42.118	
3	L-11-2-MDS9222-1	283 King George Rd, Warren, NJ, 07059		Cisco	DS-C9222I-K9	FOX1201GBCS	D 4 Warnings	2014/10/31 13:11:25	R054665	10.40.60.35	
4	L-11-2-MDS9222-2	283 King George Rd, Warren, NJ, 07059		Cisco	DS-C9222I-K9	FOX1201GBBQ	D 9 Warnings	2014/10/31 13:11:58	R054665	10.40.60.34	

Not Monitored

Item	Name	Location	Group	Type	Model	Serial	Status	Last Communication	Site ID	IP Address 1	IP Address 2
------	------	----------	-------	------	-------	--------	--------	--------------------	---------	--------------	--------------

Click Item heading to add a new item.
Click Item number to edit or delete item.
Or use the boxes in the Item column to selected Devices.

Click ▲ (ascending order) or ▼ (descending) in heading to sort that column. (current order is shown with ▲ or ▼).
Click D in status entry for detailed information.

Enter switch information here.

©Hitachi Data Systems **Hi-Track Monitor**

Summary Configuration Transport History User Management About

Add Cisco Switch or Director

Select Device Type:	Cisco Switch or Director	
Name:	2R12-MDS9710-01	
Location:	283 KING GEORGE ROAD, Warren, NJ 07059	
Group:		
Site ID:	R054665	
IP Address or Name:	10.40.42.117	Local Interface: -any-
SNMP Access ID:	hitrack	
Comms Error Reporting?:	Default	
Enabled?:	☒	
Trace?:	☐	

Add Modify Delete Reset

7. Test Hi-Track: Make sure that the added devices are showing “Okay” status on the summary page. Now click on the “Request Report” button on the “Transport History” page. This will create report files that should be transported to the HDS server. After a few minutes, the transport history will show that the report files have been successfully transmitted to HDS. “Request Report” button is at the bottom of the page.


Hi-Track Monitor

Summary
Configuration
Transport History
User Management
About

2014/11/16	04:00:07	HTTPS	ushtinet02.hds.com:443/ht_http_row	SEND OK	Successful	Periodic	04:00:0
2014/11/16	04:00:07	HTTPS	ushtinet02.hds.com:443/ht_http_row	SEND OK	File Transfer Successful	cisco Periodic	2014/11 04:00:0
2014/11/16	04:00:05	HTTPS	ushtinet02.hds.com:443/ht_http_row	SEND OK	File Transfer Successful	cisco Periodic	2014/11 04:00:0
2014/11/16	04:00:04	HTTPS	ushtinet02.hds.com:443/ht_http_row	SEND OK	File Transfer Successful	cisco Periodic	2014/11 04:00:0
2014/11/16	04:00:03	HTTPS	ushtinet02.hds.com:443/ht_http_row	SEND OK	File Transfer Successful	cisco Periodic	2014/11 04:00:0
2014/11/16	04:00:01	base	base	Delete Log Entries	7 Entries older than 60 hours removed		

Request Daily Report

Press the 'Request Report' Button to generate a Daily Report.
The requested report will not alter the generation of reports at the configured time.

Request Report

Note that the 'Daily Report' is sent to a Hi-Track Center machine and is not visible to users of this system.

5.7. Configure DCNM to authenticate to Active Directory

A separate server running Windows 2008 Enterprise Edition is required for NPS to support more than 50 Clients. With the New SAN Architecture (up to 40 MDS 9148's) in a SAN, we will eclipse the number of support NPS Clients. Installing NPS on every DCNM server is no longer a requirement.

The Data Center Network Manager Server can authenticate users via RADIUS protocol to Microsoft Network Policy Server (NPS), formerly known as Internet Authentication Service ("IAS"). NPS will accept user authentication requests from DCNM Client, Device Manager and SSH and pass it on to Active Directory. Please see Section [Interactive Authentication \(NPS/Active Directory\)](#) for step-by-step instructions on how to configure NPS and Active Directory.

NOTE: The following configuration should **ONLY** be done after the instructions in Section [Interactive Authentication \(NPS/Active Directory\)](#) have been executed.

1. Using Internet Explorer, browse to https://dcnm_server_ip_address, log in with an SOEID and password. Select "Admin", click on "Remote AAA".



From the AAA Properties window, configure DCNM to authenticate to Radius (NPS).
Click the “**Radius**” radio button
Enter the Primary and Secondary (if applicable) Radius server information

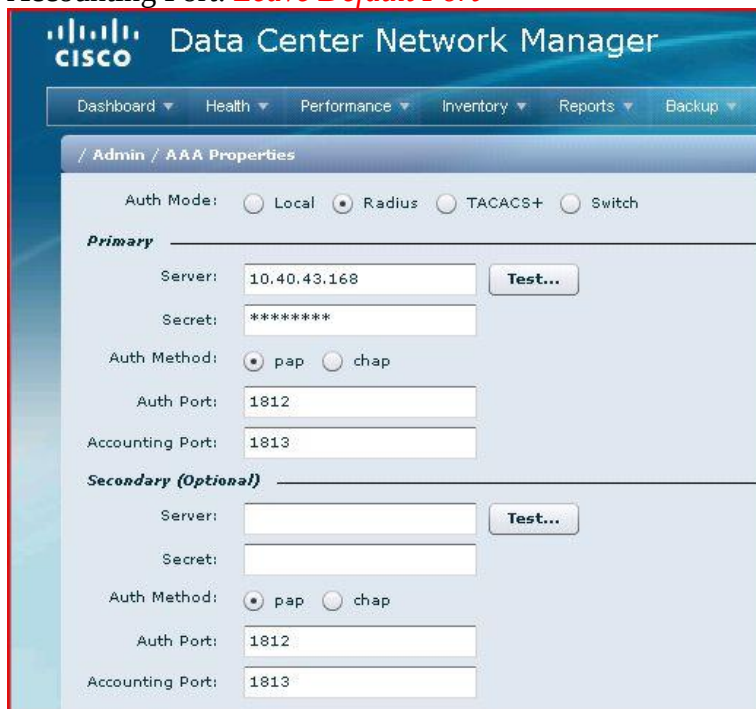
Server IP address: *IP address of the NPS Server (primary and secondary)*

Shared Secret: *cisco123*

Auth Method: Click “**pap**” radio button.

Auth Port: *Leave Default Port*

Accounting Port: *Leave Default Port*



2. Click “**Apply**” at the bottom of the screen.
3. From each switch run the following commands to setup switch authentication with Primary and Secondary Radius / Active Directory.

```
switch# config
switch(config)# radius-server host 10.40.43.200 key cisco123
switch(config)# aaa group server radius radius-group1
switch(config-radius)# server 10.40.43.200
switch(config-radius)# exit
switch(config)# radius-server host 10.40.43.168 key cisco123
switch(config)# aaa group server radius radius-group1
switch(config-radius)# server 10.40.43.168
switch(config-radius)# exit
switch(config)# aaa authentication login default group radius-group1
```

The following command will provide local (switch) authentication in the event that the Primary and Secondary NPS server are not available.

NOTE: This will be used for the “**admin**” ID. For ease of use, the password of the “**admin**” ID on the switch should match the password of the “**admin**” ID configured in Active Directory.

```
switch(config)# aaa authentication login default group radius-group1 local
switch(config)# aaa authentication login console local
switch(config)# exit
```

5.7.1. Back Out DCNM authentication to Active Directory

If NPS was configured per the previous section, if NPS is down, or incorrectly configured; authentication will revert to Local authentication. If there is a need to back out Active Directory authentication, follow these steps:

1. From each switch run the following commands to remove authentication with Radius / Active Directory.

```
switch# config
switch(config)# aaa group server radius radius-group1
switch(config-radius)# no server 10.40.43.200 (NPS server IP address)
switch(config-radius)# no server 10.40.43.168 (secondary NPS server IP address)
switch(config-radius)# exit
switch(config)# no radius-server host 10.40.43.200 (NPS server IP address)
switch(config)# no radius-server host 10.40.43.168 (secondary NPS server IP address)
switch(config)# no radius-server key cisco123
switch(config)# no aaa authentication login default group radius-group1
switch(config)# no aaa group server radius radius-group1
switch(config)# exit
```

- Using Internet Explorer, browse to https://dcnm_server_ip_address, log in with an SOEID and password. Select “**Admin**”, click on “**Remote AAA**”.



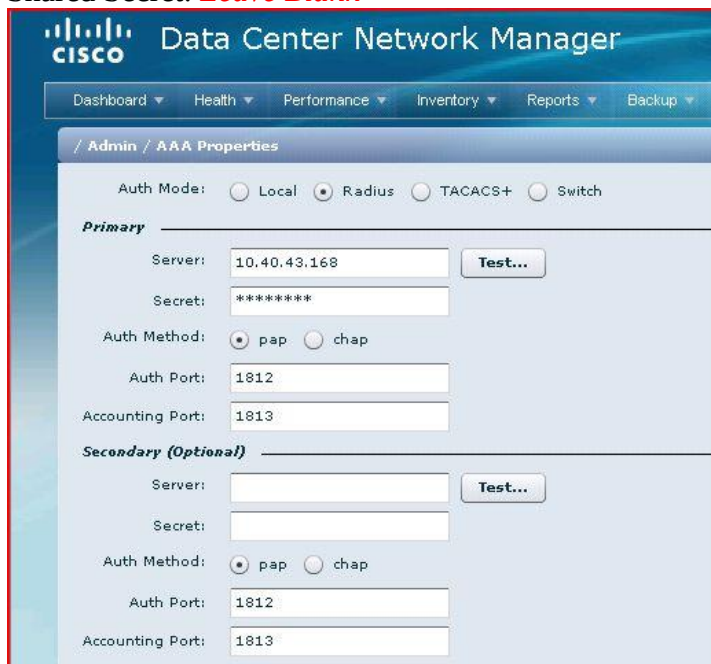
From the AAA Properties window, configure DCNM authentication.

Click the “**Local**” radio button

Enter the Primary and Secondary (if applicable) Radius server information

Server IP address: *Leave Blank*

Shared Secret: *Leave Blank*



- Click “**Apply**” at the bottom of the screen.

5.8. Management Server Access Control

Only authorized Citi storage and security management personnel should be authorized to log on to the Management Server. Please check with your SA on how to configure the server to support this. One way to accomplish this is to: (1) create a local group (2) assign this group the right to log on locally (3) add authorized storage administrators to this the group and (4) revoke the right to log on locally from all other groups and users.

5.9. Reboot The Server

Reboot the server for the changes above to take effect.

5.10. Downgrade to previous DCNM version

Since DCNM 6.3.2 is required to manage the MDS 9710 directors and NX-OS 6.2x or higher a downgrade to DCNM 5.2.1 is not an option.

6. Switch Configuration Steps

6.1. Step 1: Design VSAN IDs and Domain IDs

It is important to design VSAN ID and Domain IDs in such a way that future applications such as migrations between VSANs (fabrics) can be supported without significant configuration change. The goal is to try to avoid using AFID and NAT with IVR, and the simplest way to achieve that is to keep VSAN IDs and Domain IDs unique across the region. However this is not practical for large regions such as North America because there are only 239 domain IDs.

Problem	Cisco's Solution	Challenges with Solution
Overlapping VSAN IDs	Autonomous Fabric ID (AFID)	Reduces total number of VSANs allowed in the fabric (not a show stopper); additional configuration required
Overlapping Domain IDs	Network Address Translation (NAT)	Introduces limitations (no showstoppers); additional configuration required

It should be noted that IVR will only be used for migration between VSANs, not for BAU provisioning and replication tasks. Host to storage connections, as well as replicating end points should be members of the same VSAN.

Because the frequency of migrations within datacenter would be much higher than across datacenters **unique domain IDs should be maintained within each datacenter**. Also, because VSAN IDs provide a large range, 2 – 4093, **VSAN IDs should be unique across a region**.

Domain IDs are managed per VSAN. The IDs you reserve or assign to a switch for one VSAN has no bearing on other VSANs hosted by the switch.

Because there are only 239 domain IDs, domain IDs should be conserved. Because Fabric A and Fabric B will never be connected via IVR, **same domain IDs should be used for these fabrics**. Further, to keep things simple, each switch should be allocated the **same domain ID for every fabric**.

Blocks of domain IDs should be reserved for each VSAN (fabric) within the datacenter. Because the largest fabric (see fabric design section in this document) can have 42 switches, **a block of 42 domain IDs should be reserved for each fabric**.

The **MDS allows you to configure the reserved range of domain IDs per fabric**. This configuration will prevent an Operator from mistakenly assigning a domain ID outside the reserved range to a newly added switch. This configuration has been included in the Template.

Fabric A and Fabric B should be assigned different VSAN IDs. This will add another layer of protection when A and B fabrics are inadvertently merged. A range of **even numbered IDs should be reserved for Fabric A, and odd numbered IDs for fabric B per SAN**. **VSAN IDs 4002-4093 should not be used**; these should be reserved for transit VSANs for use with IVR.

Sample allocation of VSAN and Domain IDs:

SAN 1, Datacenter 1

VSAN IDs	VSAN Name	Reserved Domain IDs
1	Default	Don't care
2	Fabric_A	1-52 (51 & 52 reserve for Cores)
3	Fabric_B	1-52 (51 & 52 reserve for Cores)
4,6,8,10,12	Additional 'A' fabrics for future use	1-52 (51 & 52 reserve for Cores)
5,7,9,11,13	Additional 'B' fabrics for future use	1-52 (51 & 52 reserve for Cores)

SAN 2, Datacenter 1

VSAN ID	VSAN Name	Domain IDs
1	Default	Don't care
14	Fabric_A	1-52 (51 & 52 reserve for Cores)
15	Fabric_B	1-52 (51 & 52 reserve for Cores)
16,18,20,22,24	Additional 'A' fabrics for future use	1-52 (51 & 52 reserve for Cores)
17,19,21,23,25	Additional 'B' fabrics for future use	1-52 (51 & 52 reserve for Cores)

SAN 1, Datacenter 2

VSAN ID	VSAN Name	Domain IDs
1	Default	Don't care
26	Fabric_A	1-52 (51 & 52 reserve for Cores)
27	Fabric_B	1-52 (51 & 52 reserve for Cores)
28,30,32,34,36	Additional 'A' fabrics for future use	1-52 (51 & 52 reserve for Cores)
29,31,33,35,37	Additional 'B' fabrics for future use	1-52 (51 & 52 reserve for Cores)

SAN 2, Datacenter 2

VSAN ID	VSAN Name	Domain IDs
1	Default	Don't care
38	Fabric_A	1-52 (51 & 52 reserve for Cores)
39	Fabric_B	1-52 (51 & 52 reserve for Cores)
40,42,44,46,48	Additional 'A' fabrics for future use	1-52 (51 & 52 reserve for Cores)
41,43,45,47,49	Additional 'B' fabrics for future use	1-52 (51 & 52 reserve for Cores)

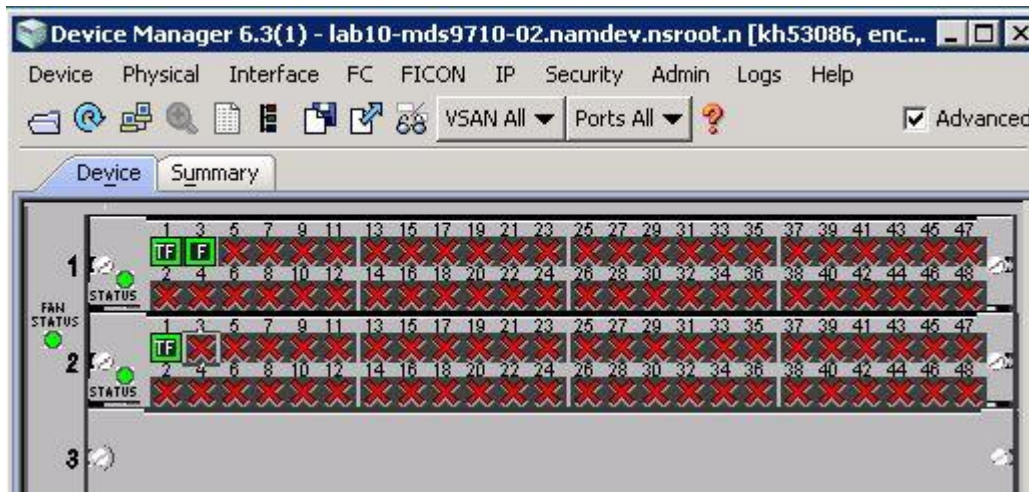
Because VSAN 1 will not be used for production, and because there will not be any IVR application for VSAN 1 in the future, there is no need to plan for domain IDs for VSAN 1. Domain IDs for VSAN 1 will be assigned dynamically by the principle switch.

6.1.1. Step 1a: Migrations and Domain IDs (NPV)

If you'll be connecting a new SAN to an existing SAN for migration purposes, verify that the new SAN Domain ID's won't be duplicates of the existing SAN switch Domain ID's. If so, adjust the Domain ID of the switch in the new SAN. This will help prevent segmentation when the existing and new SAN attempt to merge.

With the larger number of Host Edge switches (up to 88), **NPV is required** to be enabled on the MDS 9148 Host Edge Switches (NPIV and F-Port Trunking on the Core MDS 9710). The MDS 9148's will look like an N-Port (Node Port) to the Core Directors. Thus the edge switches DO NOT REQUIRE DOMAIN IDs. This will assist in management and migrations to these larger fabrics.

Core Switch ISLs will be Trunked F-Ports to the NPV enabled MDS 9148 Host Edge switches.



The NPV enabled MDS 9148 Host Edge switches will have Trunked Node Ports ISLs to the Core Directors.



6.2. Step 2: Naming Standard

Switch names	Max length is 32 characters, must start with a letter, not supported ~ ! @ # % & * () = + [] { } \ ; ' : " , . / < > ? _
Example:	Country Code (<Country>) Site Identifier (<Site>) Vendor Identifier (see below) SAN Usage Identifier; D=Disk, T=Tape, B=Both SAN Number Identifier (01-99) SAN Fabric Identifier; A or B side Usage Identifier; S=Storage Edge, C=Core, E=Host Edge SAN Member Sequence Number (001-199) CC S V H NN F U NNN Vendor Identifier: B = Brocade C = Cisco usucd01as001 (us / u-SWDC / c-Cisco / d-Disk / 01-SAN01 / a-FabricA / s-Storage / 001-Switch001)
VSAN names	Max length is 32 characters, No special character limit
Example:	Country Code (<Country> See Appendix A) Site Identifier (<Site> See Appendix A) Vendor Identifier (see below) SAN Usage Identifier; D=Disk, T=Tape, B=Both SAN Number Identifier (01-99) SAN Fabric Identifier; A or B side CC S V H NN P usucd01a (US / U-SWDC / d-Disk / 01-SAN01 / a-FabricA)
Zone names	Max length is 64 characters, must start with a letter, not supported ~ ! @ # % & * () = + [] { } \ ; ' : " , . / < > ?
Zoneset names	Max length is 64 characters, must start with a letter, not supported ~ ` ! @ # % & * () = + [] { } \ ; ' : " , . / < > ?
Device Alias	Max length is 64 characters, must start with a letter, not supported ~ ` ! @

names	# % & * () = + [] { } \ ; ' : " , . / < > ?
-------	---

Device alias and not FC alias names should be used for zoning. To make it easy to track a logged out HBA to a switch port, the device alias may include the switch name and port number, unless such information is being tracked in another system such as a spreadsheet or SANScreen.

6.3. Step 3: Customize Configuration Template

Use the commands outlined in the Configuration Template from [Appendix C](#) as a guide to configure your switches. Change the text marked in **red** to suit the specific switch and site that is being configured. The commands can be entered individually or scripted if you prefer.

6.3.1. Configuration Items in the template

- Banner
- Logging
- Time zone and automatic DST
- Roles and distribution via CFS
 - role name storage_admin
 - role name vendor
 - role name script
 - role name facility
- SSH access
- NTP synchronization
- IP Access Control List: Protect switch from unauthorized access
- SNMP TRAPs
- Management interface
- IP/Default Gateway
- VSANs
- Domain IDs
- Interfaces
- Device alias'

- Zoning related information
- Port channel (ISL)
- Authentication to NPS via RADIUS
- Enable NPIV to support HP C Class Blade Center

6.4. Step 4: Power Up and First Login

Connect the two console connections and configure the terminal server to operate the lines at 9600 baud, 8 databits, 1 stop bit and no parity. Use telnet to terminal server and connect to the console port on the supervisor in the lower numbered slot (the supervisor in the lower numbered slot will become the active supervisor). Power up the switch. When prompted, configure a new CISS complaint password for the “admin” user, and enter “no” when asked “Would you like to enter the basic configuration dialog (yes/no)”. Now logon as “admin”.

6.5. Step 5: Configure IP Address & Default Gateway

Configure IP address, subnet mask and default gateway by issuing the following commands. Replace the text in red with your own addresses.

```
conf
interface mgmt0
  switchport speed 1000
  ip address 10.40.42.108 255.255.255.0
exit
ip default-gateway 10.40.42.2
exit
```

6.6. Step 6: Upgrade NX-OS to CSBE Certified Version

The new SAN architecture allows up to 42 edge MDS 9148's per VSAN. An upgrade of NX-OS using CLI would be very time consuming. Going to “Tools/Install/Software” from DCNM allows you to upgrade multiple MDS 9148's at once. DCNM does not limit the number switches that can be concurrently upgraded, but Cisco recommends 10 concurrent upgrades if the images are being transferred and 20 concurrently if the images have been pre-staged on the switches. See [Section 19](#) for instructions on using DCNM to perform the NX-OS upgrade.

Upgrade MDS 9710 via DCNM or command line.

The following command will show the NX-OS version:

```
Switch# show version
```

Using your Cisco Connection Online (“CCO”) account, or with help from vendor support, download the correct System and Kickstart NX-OS images from Cisco’s website to your home directory³ on the Management Server. Now copy both files to switch bootflash filesystem using the following command on the switch:

```
Switch# copy sftp://MgmtServerIP/home/SystemImageFileName bootflash:SystemImageFileName
```

```
Switch# copy sftp://MgmtServerIP/home/KickStartImageFileName bootflash:KickStartImageFileName
```

Start the upgrade (or downgrade) process with this command:

```
Switch# install all system bootflash:SystemImageFileName kickstart bootflash:KickStartImageFileName
```

Examples:

```
Switch# copy sftp://10.40.43.168/home/m9500-sf2ek9-kickstart-mz.x.x.x.bin bootflash: m9500-sf2ek9-kickstart-mz.x.x.x.bin
```

```
Switch# copy sftp://10.40.43.168/home/m9500-sf2ek9-mz.x.x.x.bin bootflash: m9500-sf2ek9-mz.x.x.x.bin
```

```
Switch# install all system bootflash: m9500-sf2ek9-mz.x.x.x.bin kickstart bootflash: m9500-sf2ek9-kickstart-mz.x.x.x.bin
```

The system will be now be upgraded (or downgraded). Please note that there is a Supervisor switchover during the upgrade so you will have to connect to the console of the other Supervisor to carry out rest of the configuration.

³ This is the directory that the Tectia server makes accessible via SFTP. If you are logged in to the Management Server as “im12345” SOE ID, the home directory is “C:\Documents and Settings\im12345”.

6.7. Step 7: Configuration Commands

The configuration commands can be run individually or run via a script file. If you run from a script, you'll need to save the commands to a text file and copy the file to the switch.

Example:

```
copy sftp://MgmtServerIP/home/scriptFileName bootflash:scriptFileName4
```

Run the configuration script:

```
run-script bootflash:scriptFileName
```

If there are errors reported at the end, “write erase” and “reload” the switch and start over from step 1, making sure that errors in the script are fixed.

6.8. Step 9: Obtain and Install Licensing

In DCNM 6.3.2 and NX-OS 6.2 (and above) switch licensing is handled in the DCNM SAN server via license pools. The switch licenses aren't tied to a specific chassis or device. They reside in a fabric pool on the DCNM server. The server pulls a license from the 'pool' for each switch in the fabric it finds. The licenses are purchase by switch type.

Cisco DCNM Server-Based Licenses

Platform	Electronic Part Number	Physical Part Numbers	Chassis Part Numbers
DCNM for SAN Advanced Edition for MDS 9100	L-DCNM-S-M91-K9=	DCNM-SAN-M91-K9=	DCNM-SAN-M91-K9
DCNM for SAN Advanced Edition for MDS 9200	L-DCNM-S-M92-K9=	DCNM-SAN-M92-K9=	DCNM-SAN-M92-K9
DCNM for SAN Advanced Edition for MDS 9500	L-DCNM-S-M95-K9=	DCNM-SAN-M95-K9=	DCNM-SAN-M95-K9
DCNM for SAN Advanced Edition for MDS 9700	L-DCNM-S-M97-K9=	DCNM-SAN-M97-K9=	DCNM-SAN-M97-K9

Purchases will need enough licenses to cover the switches being implemented.

NOTE: MDS 9148 switches have port activation licenses, based on the number of ports needed. All MDS 9148 switches should be ordered with ALL ports activated. Cisco, EMC and HDS understand that this is how Citi will always order these.

NOTE: See “[New Licensing Model for DCNM 6.3.1](#)” for more information on Licensing.

7. User IDs and Authentication

7.1. Interactive Authentication (NPS / Active Directory)

Although the switch and DCNM can host user IDs, it is advisable to authenticate users from an external system to follow the principle of separation of duties. External authentication system will also generally provide more compliant authentication by enforcing password complexity, password expiration, and user account expiration.

⁴ The “copy sftp” command requires an ID and Password, enter the SOEID and Password used to login to the DCNM server.

The Citi standard for authentication of users to hardware devices such as Cisco network devices is Cisco Access Control Server (“ACS”). Currently ACS is used for authentication of all Cisco Ethernet and IP devices globally. However, although the MDS switch and DCNM support the TACACS+ protocol, they do not additionally support the “ENIGMA” protocol, which is required by Citi’s implementation of ACS. ENIGMA permits relaying of authentication requests from the device to Safeword systems via ACS. This relaying is required because the authentication built into ACS is not fully compliant with CISS.

The solution outlined here will thus not use ACS, but rather use Windows Network Policy Server (formerly called Internet Authentication Service - “IAS”) to relay authentication requests from switch and DCNM to Active Directory. All user add, delete, modify, as well as entitlement operations, will occur within Active Directory. The benefits of this approach over local user IDs are:

- Because authentication is delegated to Active Directory, there will be full compliance with CISS authentication standards
- Users can use their SOEID to log on; MASTER ID compliance is automatically achieved
- There is separation of duties: Storage Operations will not control user IDs and entitlements
- Management of user IDs will be centralized

NPS (Network Policy Server) is the Radius component of the Windows 2008 Server operating system. No additional license is required to use NPS, although for the number of clients it will be authenticating at Citi (50 or more Clients), NPS will require **Windows 2008 Enterprise Edition**. The Citi Windows 2008 Server build process does not install NPS. It must be manually installed after the build is completed. Here is an overview of the installation and configuration process:

- ✓ Ask for Active Directory groups to be created
- ✓ Install the Primary NPS server on a **W2K8 Enterprise Edition Server**
- ✓ Install the Secondary NPS server on a second server
- ✓ Configure NPS
- ✓ Configure switches
- ✓ Configure DCNM

Here are detailed step-by-step instructions to accomplish the above.

7.1.1. Create Active Directory Security Groups

Ask your Active Directory administrator to create following Active Directory security groups. The Active Directory group names are only suggestions; the Active Directory administrator should formulate the names based on Active Directory conventions. Any existing groups can also be used instead of getting new ones created specifically for MDS.

Active Directory Security Group	Purpose: Maps to this role on the switch	Members
MDS_Storage_Admin	storage_admin	Storage Operations personnel
MDS_Network_Admin	network-admin	Select Storage Operations personnel
MDS_Vendor	vendor	“emc” and “hds” functional IDs ⁵
MDS_Facility	facility	Facility Operations personnel who will hook up hosts and storage to MDS

Note: See the Switch Configuration Template in the Appendix, for the commands to create the Roles and enable CFS on the switches. CFS will keep the switches and DCNM in sync.

7.1.1.1. Switch Roles

These are the switch roles that need to be configured on the switches. These are also listed in Appendix C: Switch Configuration.

NOTE: Storage Engineering prohibits the use of “**vsan policy deny**” in any role. This setting has been known to cause supervisor failover and even a switch reload when an application is polling an SNMP MIB on the switch.

7.1.1.1.1. Storage Admin

```
role name storage_admin
rule 1 permit config
rule 2 permit debug
rule 3 permit show
rule 4 permit exec
rule 5 deny config feature aaa
rule 6 deny config feature radius-server
rule 7 deny config feature ssh
rule 8 deny debug feature aaa
```

⁵ Please contact your BISO for instructions on how to get functional IDs approved and created. If it is not possible to have these functional IDs created on Active Directory, these should be created as local Windows IDs on the Management Server.

rule 9 deny config feature logging
rule 10 permit clear
rule 11 deny clear feature accounting
rule 12 deny clear feature logging

7.1.1.1.2. Vendor

role name vendor
rule 1 permit show
rule 2 permit exec feature attach
rule 3 permit clear
rule 4 permit debug
rule 5 permit exec feature undebg
rule 6 permit exec feature dir
rule 7 permit exec feature fcping ⚡ Omit, if switch is in NPV Mode
rule 8 permit exec feature fctrace ⚡ Omit, if switch is in NPV Mode
rule 9 permit exec feature terminal
rule 10 permit exec feature delete
rule 11 permit exec feature copy
rule 12 permit exec feature install
rule 13 permit exec feature ping

7.1.1.1.3. Script

role name script
rule 1 permit show
rule 2 permit exec feature attach
rule 3 permit clear
rule 4 permit debug
rule 5 permit exec feature undebg
rule 6 permit exec feature dir
rule 7 permit exec feature fcping ⚡ Omit, if switch is in NPV Mode
rule 8 permit exec feature fctrace ⚡ Omit, if switch is in NPV Mode
rule 9 permit exec feature terminal

7.1.1.1.4. Facility

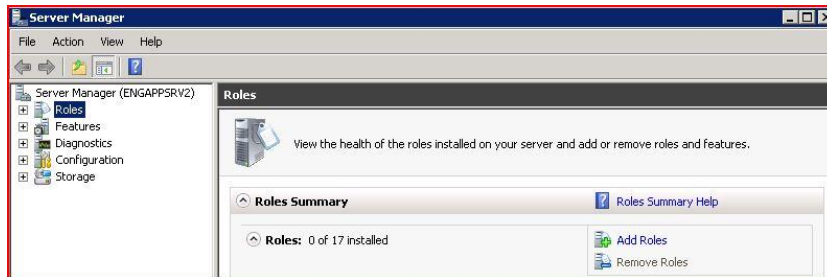
role name facility
rule 1 permit show
rule 2 permit exec feature system
rule 3 permit exec feature terminal

7.1.2. Install Windows Network Policy Server (“NPS”)

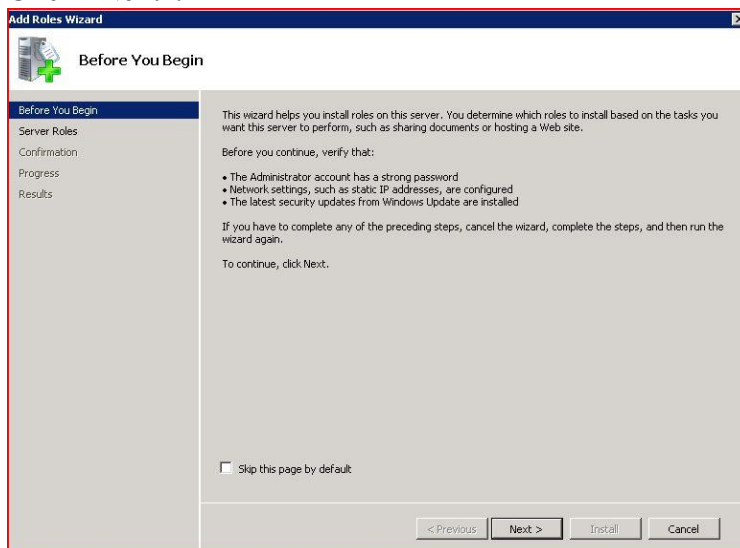
The following steps require Administrator rights on the Management Server.

Install NPS on a primary and secondary Windows 2008 Enterprise Edition Server. This can be on the DCNM server or another server, as long as it is running W2k8 Enterprise Edition.

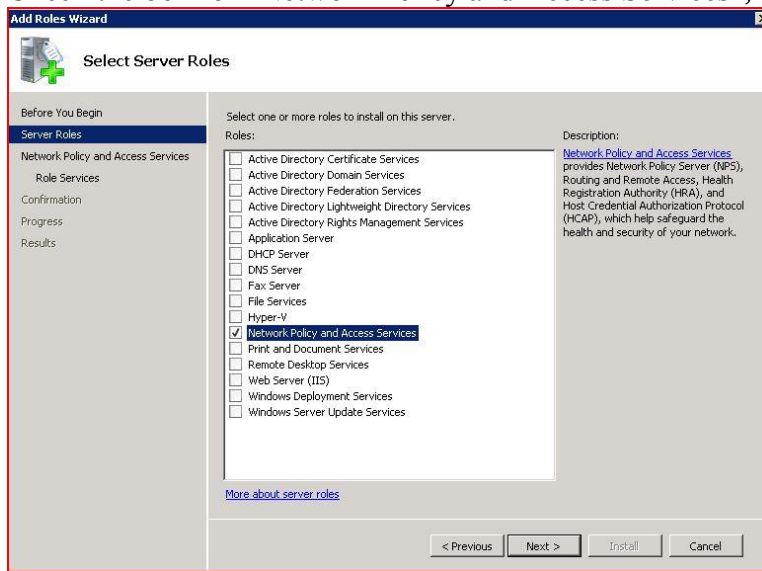
1. Go to Start/Administrative Tools/Server Manager.20
2. Click on “Add Roles”.



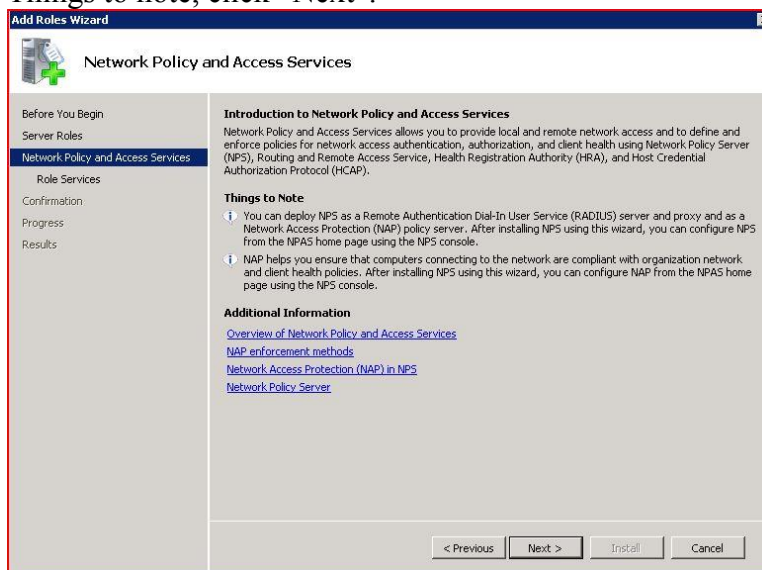
3. Click “Next”.



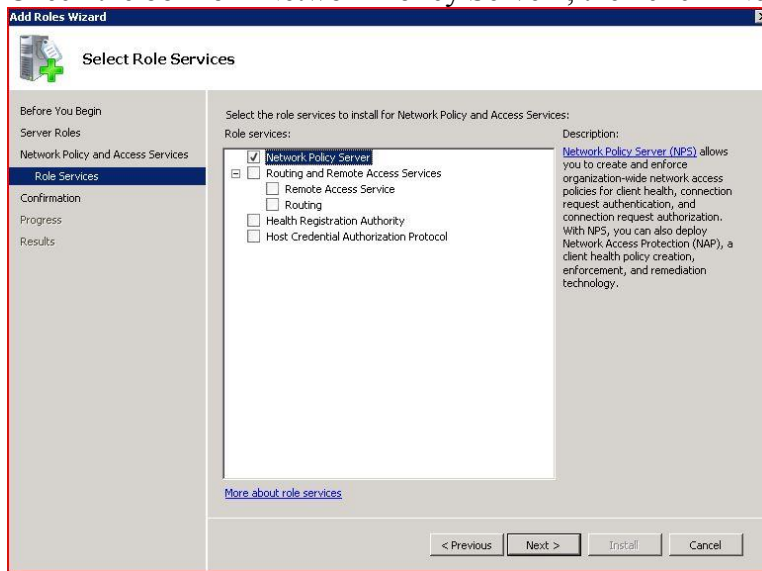
4. Check the box for “Network Policy and Access Services”, click “Next”.



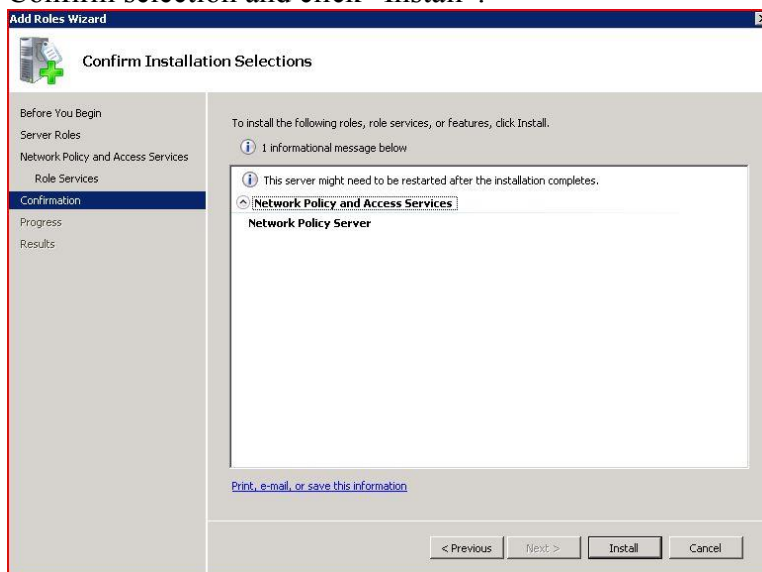
5. Things to note, click “Next”.



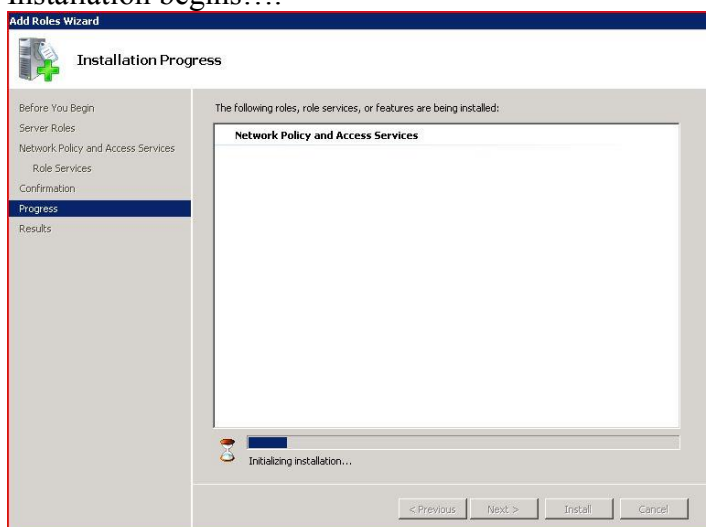
6. Check the box for “Network Policy Server”, then click “Next”.



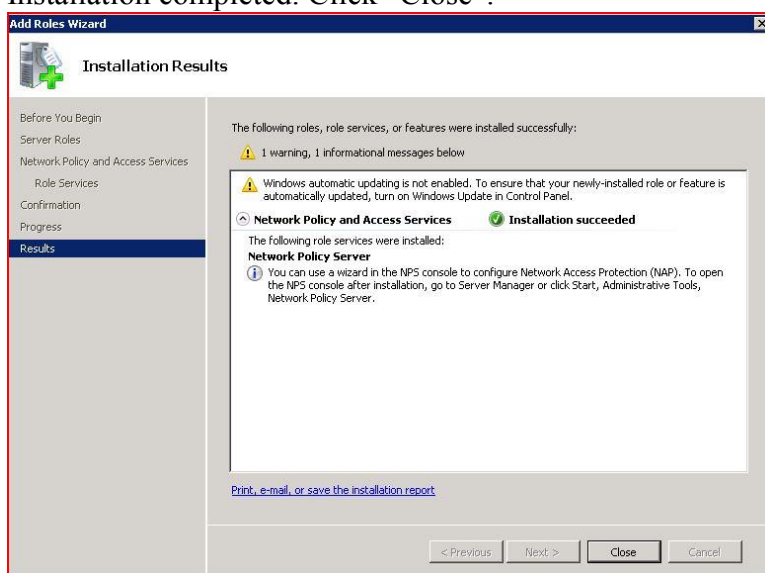
7. Confirm selection and click “Install”.



8. Installation begins....



Installation completed. Click “Close”.



7.1.3. Configure NPS

Step 1: Create Policies on the Primary NPS Server

IMPORTANT CHANGE TO NPS CONFIGURATION

Due to bug [CSCuo24658 - RADIUS login only assigned network-operator role](#) (noted in the NX-OS 6.2.x Release Notes), separate Network Policies will have to be created for each Role. One Network Policy for switches running NX-OS 6.2.x and one for switches running NX-OS 5.2.x. The difference is in the Cisco-AV-Pair definitions and an additional “Condition” setting for Client IPv4Addresses for authentication to NX-OS 6.2.x switches.

For switches running NX-OS 6.2.x:

Cisco-AV-Pair attribute values must be on separate lines.

```
shell:roles="storage_admin"
```

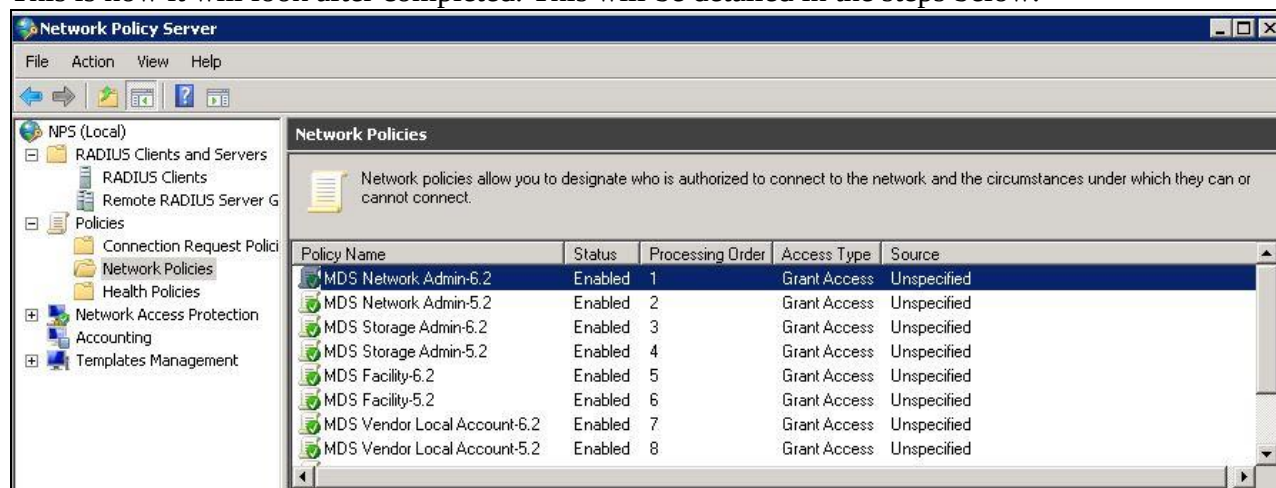
```
snmpv3:auth=SHA priv=AES-128
```

Client IPv4 Address

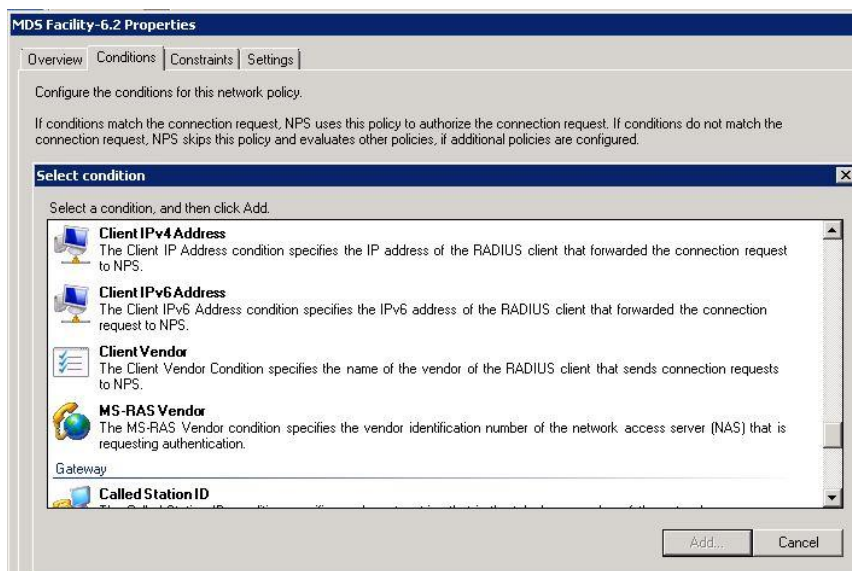
This will allow us to select the IP addresses of the Radius Client

Example: (10.40.42.117|118)|(10.40.52.103)|(10.40.42.144)

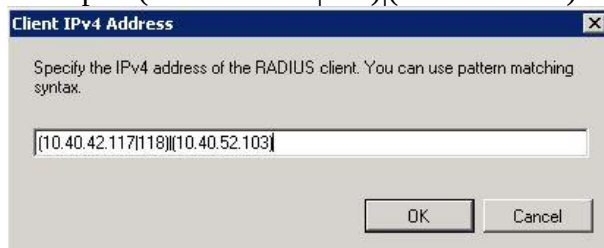
This is how it will look after completed. This will be detailed in the steps below.



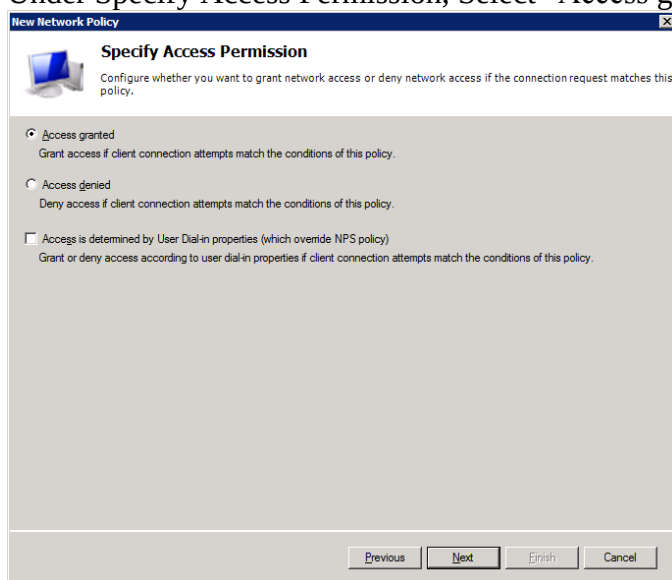
- From Start Menu, select Programs, Administrative Tools and click on Network Policy Server.
- Expand Policies, Click on Network Policies
- Right click on Network Policies and click on New
- Enter Policy Name (Example: **MDS Storage Admin-6.2** or **MDS Storage Admin-5.2**), Click Next
- Under Specify Conditions, Select Add
- Select Windows Groups, Select Add
- Select Add Groups
- Find the AD User Group that corresponds with the Policy you are creating (Example: NAM\MDS_Storage_Admin) and add it
- Note: You may be asked to provide a user account in the domain where this group resides so that the group name can be validated. Any user account (domain administrator account is not required) can be provided.
- The group should now be listed in the Groups list.
- **For NX-OS 6.2 switches**, add this Network Policy Condition, “Client IPv4 Addresses”. Setting is not needed for NX-OS 5.2 switch Network Policies.
- Under Specify Conditions, Select Add. Select “Client IPv4 Addresses”. Click OK



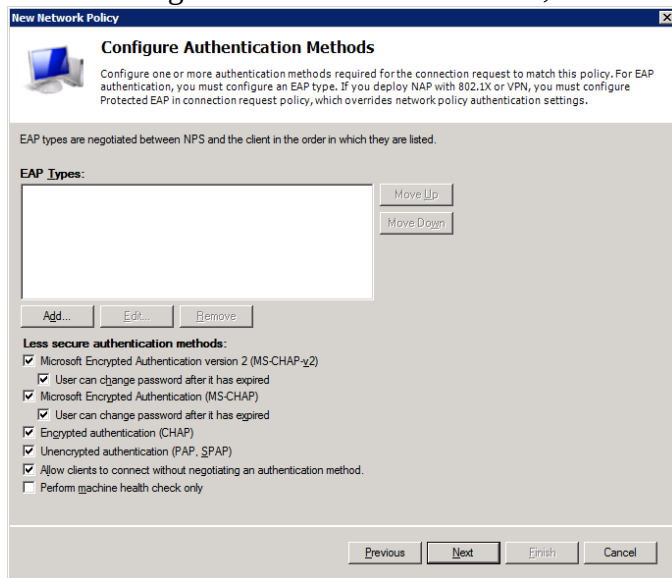
- Enter the IP addresses (Uses pattern matching syntax).
These will be the IP addresses of the MDS 9710 directors and DCNM servers.
Click OK, and then click Next.
Example: (10.40.42.117|118)|(10.40.52.103)



- Under Specify Access Permission, Select “Access granted” and click Next



- Under Configure Authentication Methods, check the following boxes and click Next



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Move Up
Move Down

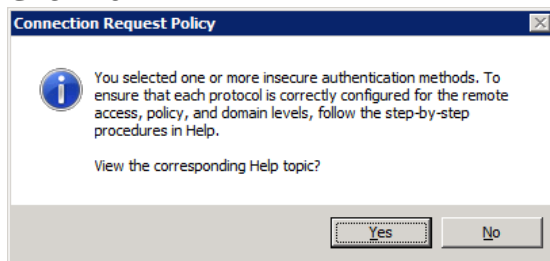
Add... Edit... Remove

Less secure authentication methods:

- ☒ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 - ☒ User can change password after it has expired
- ☒ Microsoft Encrypted Authentication (MS-CHAP)
 - ☒ User can change password after it has expired
- ☒ Encrypted authentication (CHAP)
- ☒ Unencrypted authentication (PAP, SPAP)
- ☒ Allow clients to connect without negotiating an authentication method.
- ☐ Perform machine health check only

Previous Next Finish Cancel

Click No



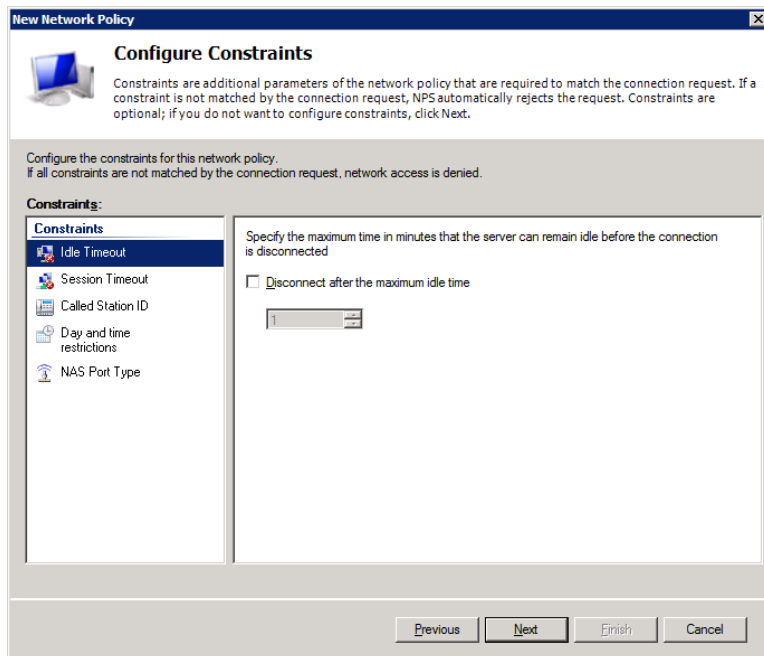
Connection Request Policy

i You selected one or more insecure authentication methods. To ensure that each protocol is correctly configured for the remote access, policy, and domain levels, follow the step-by-step procedures in Help.

View the corresponding Help topic?

Yes No

- Click Next



New Network Policy

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Constraints

- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

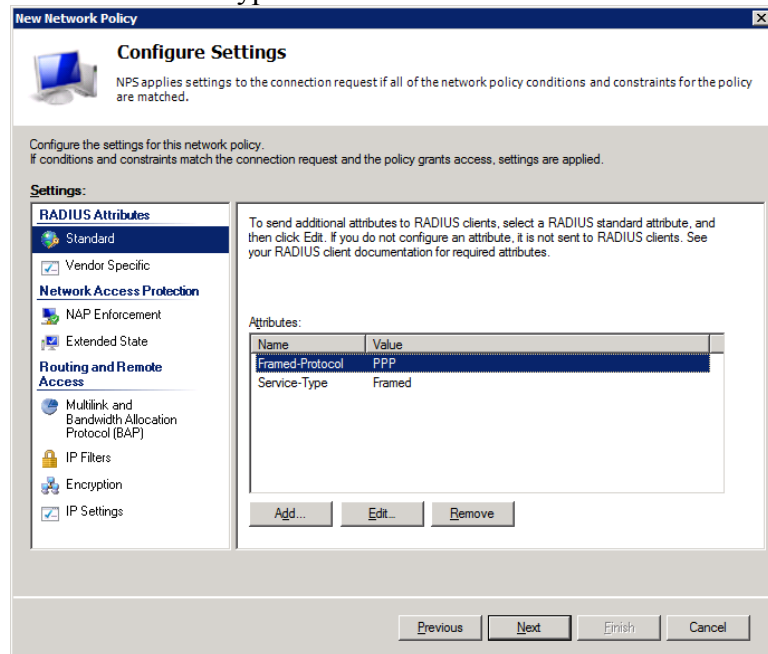
Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

☐ Disconnect after the maximum idle time

Previous Next Finish Cancel

- Under Configure Settings, select “Standard” under RADIUS Attributes. Remove “Framed-Protocol”.

Select “Service-Type” and click on Edit



New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

- RADIUS Attributes**
 - ☒ Standard
 - ☐ Vendor Specific
- Network Access Protection**
 - ☐ NAP Enforcement
 - ☐ Extended State
- Routing and Remote Access**
 - ☐ Multilink and Bandwidth Allocation Protocol (BAP)
 - ☐ IP Filters
 - ☐ Encryption
 - ☒ IP Settings

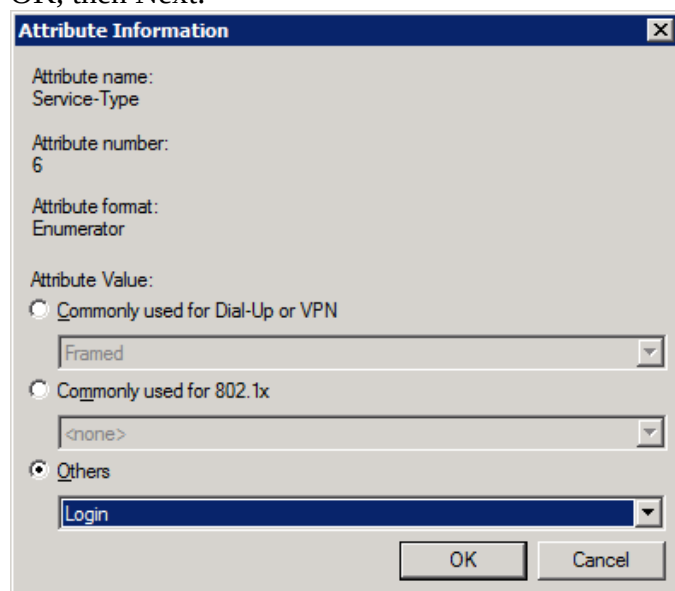
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

Add... Edit... Remove

Previous Next Finish Cancel

- Under Attribute Information, click on the “Others” radio button and select “Login”. Click OK, then Next.



Attribute Information

Attribute name:
Service-Type

Attribute number:
6

Attribute format:
Enumerator

Attribute Value:

☐ Commonly used for Dial-Up or VPN
Framed

☐ Commonly used for 802.1x
<none>

☒ Others
Login

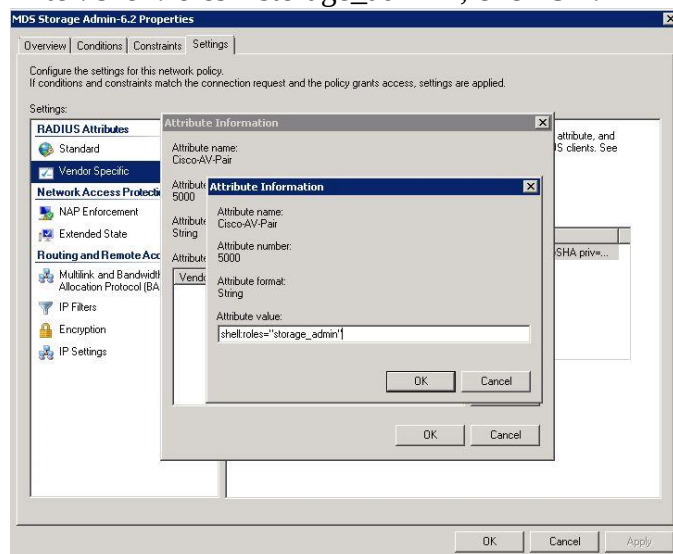
OK Cancel

- **For NX-OS 6.2 Policies**

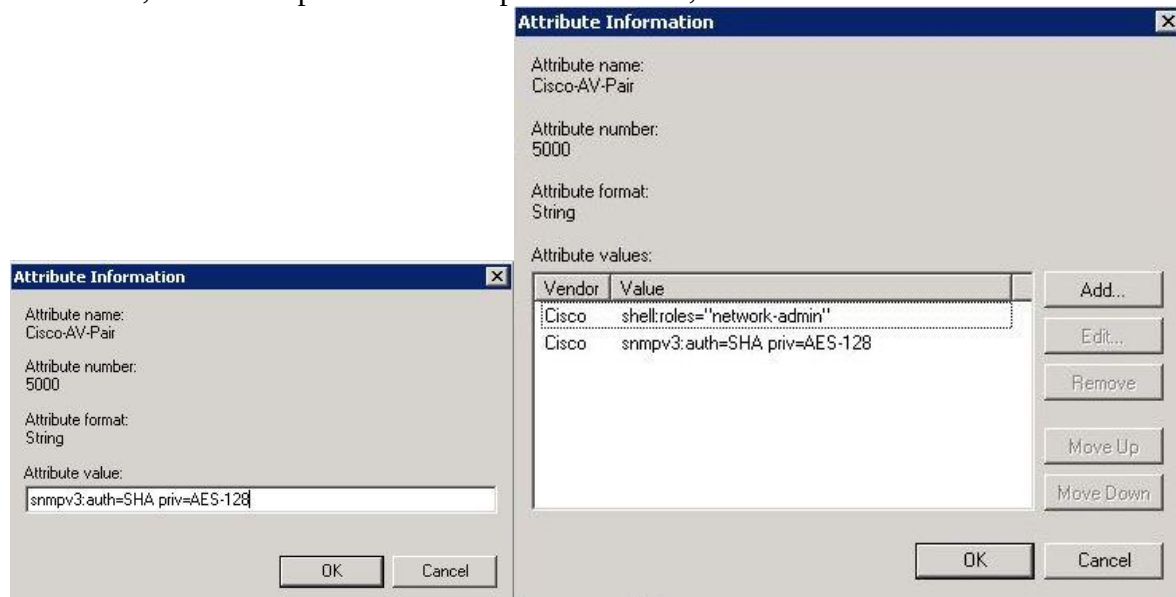
Under Configure Settings, select “Vendor Specific” under RADIUS Attributes.

Click on Add; Select; Select Vendor Cisco; Select Cisco-AV-Pair on the list and click “Add”; click “Add” on the attribute information screen. Shell:roles and snmpv3 need to be on separate lines.

Enter: shell:roles="storage_admin", click OK.

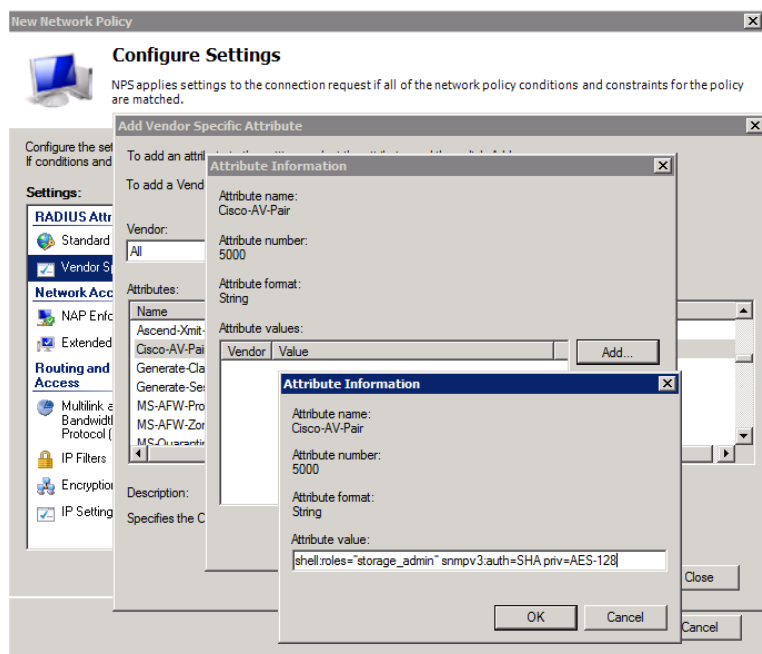


Click Add, Enter: snmpv3:auth=SHA priv=AES-128, click OK.

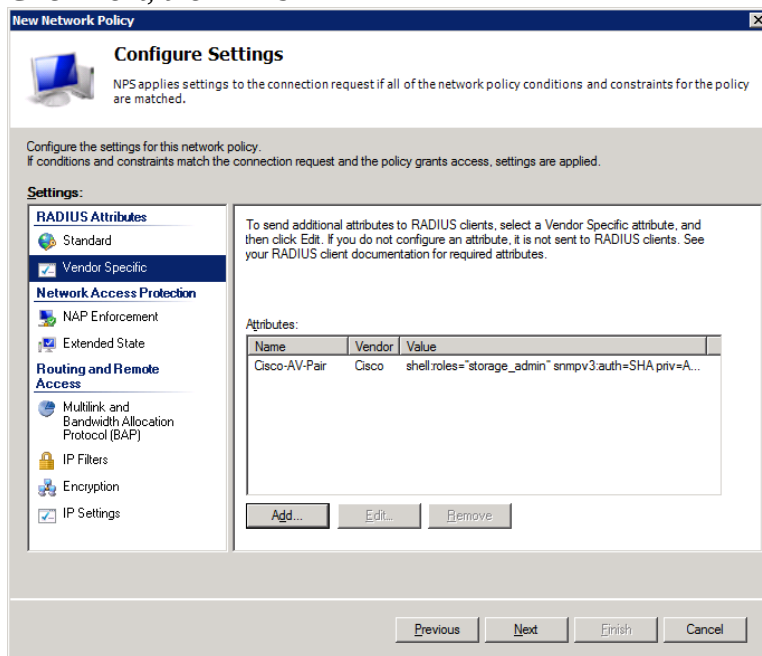


- **For NX-OS 5.2 Policies**

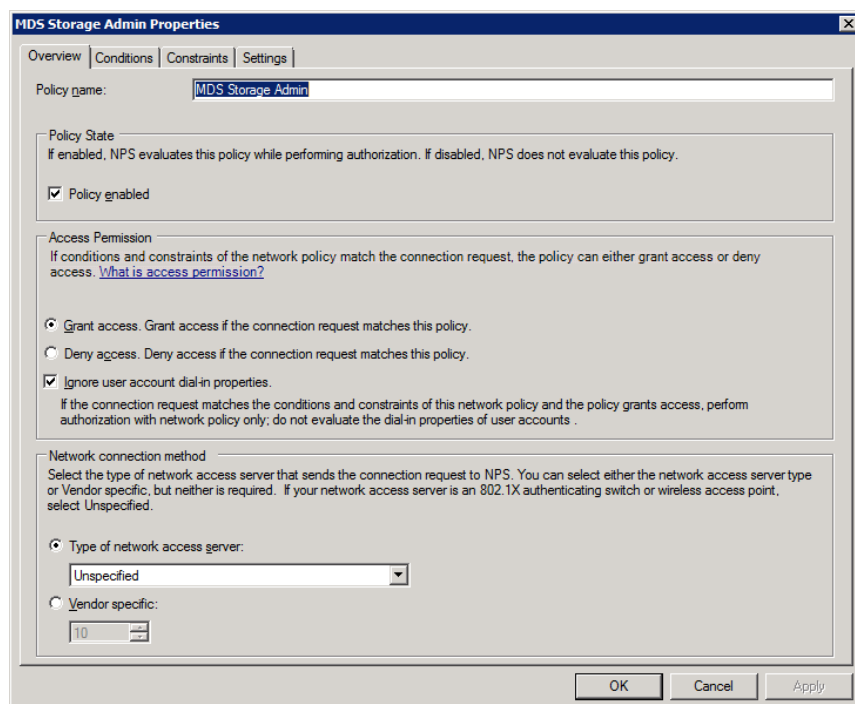
On the Attribute Information setting, enter shell:roles and snmpv3 on one line.
 shell:roles="network-admin" snmpv3:auth=SHA priv=AES-128, click OK, OK, Close.
 Click Next.



- Click Next, then Finish



- Once all of the Network Policies are configured. Double-click on each policy and check the “Ignore-User-Dialin-Properties”. Click OK



MDS Storage Admin Properties

Overview | Conditions | Constraints | Settings

Policy name: MDS Storage Admin

Policy State
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

☒ Policy enabled

Access Permission
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. [What is access permission?](#)

☒ Grant access. Grant access if the connection request matches this policy.
☐ Deny access. Deny access if the connection request matches this policy.

☒ Ignore user account dial-in properties.
 If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts.

Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

☒ Type of network access server:
 Unspecified

☐ Vendor specific:
 10

OK Cancel Apply

Step 2: Create the remaining policies, one for each group defined on the switch

Use the instructions from the previous step to create the remaining policies.

Policy Name	Active Directory Group	CISCO-AV-PAIR
MDS Storage Admin	MDS_Storage_Admin	shell:roles="storage_admin" snmpv3:auth=SHA priv=AES-128
MDS Vendor	MDS_Vendor - Only set this Policy up if functional IDs are allowed in Active Directory	shell:roles="vendor" snmpv3:auth=SHA priv=AES-128
MDS Facility	MDS_Facility	shell:roles="facility" snmpv3:auth=SHA priv=AES-128
MDS Network Admin	MDS_Network_Admin	shell:roles="network-admin" snmpv3:auth=SHA priv=AES-128
MDS Vendor Local Account (instructions in the next step)	Local Windows Auth – Only set this Policy up if functional IDs are not allowed in Active Directory	shell:roles="vendor" snmpv3:auth=SHA priv=AES-128

Step 3: Configure Local Windows NPS Policy – For Windows authentication of the vendor Local Functional ID's

This step should only be performed for the vendor ID, if it cannot be added to Active Directory.

These ID's will be created locally on the Primary and Secondary IAS Servers.

- On the server that has NPS installed, have the SA create a local windows group called “Vendor”
- Create a local user (example: emc2008)
 - Set ID to “User cannot change password” and “Password never expires”
- Add vendor ID to the Vendor group
- Use the same process from the previous step, create a 6.2 and a 5.2 policy. Only difference is under Conditions, add the local Vendor group
Example: `servername\vendor`.
- Add Cisco-AV-Pair
`shell:roles="vendor" snmpv3:auth=SHA priv=AES-128`

Step 4: Configure NPS: Add Clients

Each MDS switch and DCNM Server (Management Server) has to be added as a client.

- Right click on RADIUS Clients and click on New Radius Client
- Enter the switch/server name for Friendly name
- Enter the IP Address of the switch/server
- Enter a **shared secret** for the client. This is an arbitrary string without spaces. Make a note of the secret because you will have to configure the same secret on the switch/server.
- Click on the Advanced tab and verify that Vendor name has RADIUS Standard (this is selected by default)
- Click OK

Repeat the above procedure for all switches and Management Servers.

Step 5: Create Secondary NPS instance

A secondary NPS Server needs to be configured, in case the primary fails.

To transfer the configured remote access policies from the Primary NPS server to the Secondary NPS Server, perform this procedure:

- NPS should already be installed on the Secondary NPS Server.
- Any **Local IDs** and **Groups** that were created on the Primary NPS Server will need to be created on the Secondary Server (same ID and passwords)
- On the Primary NPS server, right click on NPS(local) and select “Export Configuration” and save the XML file.

- Copy the XML file to the Secondary NPS server.
- On the Secondary NPS server, right click on NPS(local) and select “Import Configuration”, select the XML file to import.
- **NOTE:** If you use this procedure for a site that uses a different SHARED SECRET, then you’ll need to modify the SHARED SECRET of copied policies.
- After completion, modify the Network Policies for the Local user group “Vendor” to change to the appropriate “servername”.

Step 6: Configure Data Center Network Manager

Please see Section 5.7: [Configure DCNM to Authenticate to Active Directory](#).

Step 7: Configure Switch

Please see the configuration template in [Appendix C](#). Search for “Authenticate to NPS via RADIUS” section.

The authentication configuration is now complete.

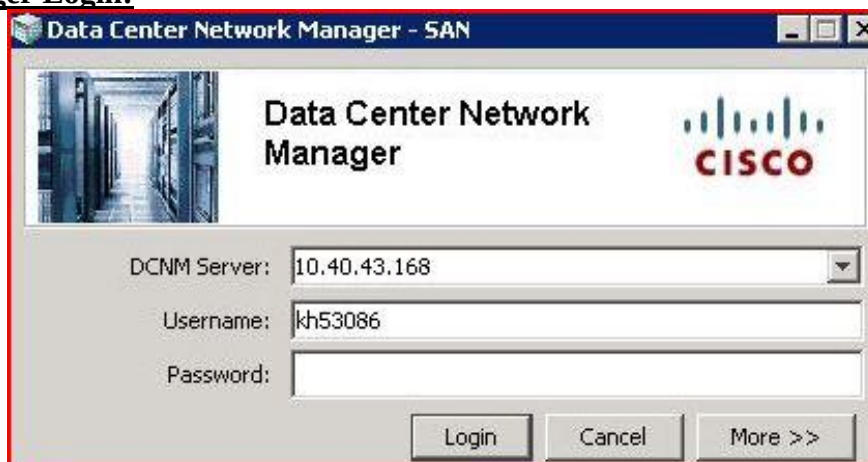
7.2. Cryptography (SHA / AES)

MD5 authentication has been marked as EOL by ISTG. **SHA** and **AES** are now the approved cryptographic algorithms. By default, DCNM and Device Manager use MD5. The previous section contains information on configuring NPS(Radius) to force the use of SHA and AES.

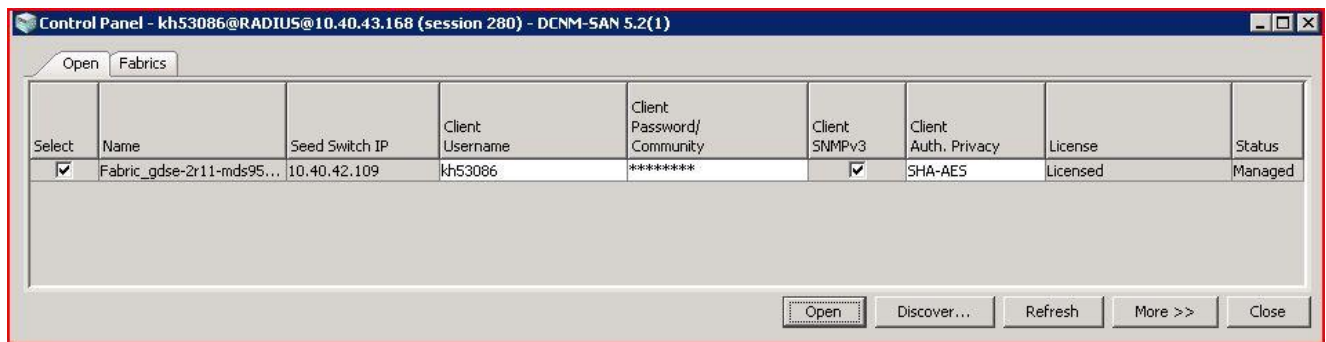
7.3. Storage Personnel Authentication

Data Center Network Manager Login:

From the DCNM Client
enter:
IP address: DCNM Server
IP
Enter User ID
Enter password
Click Login



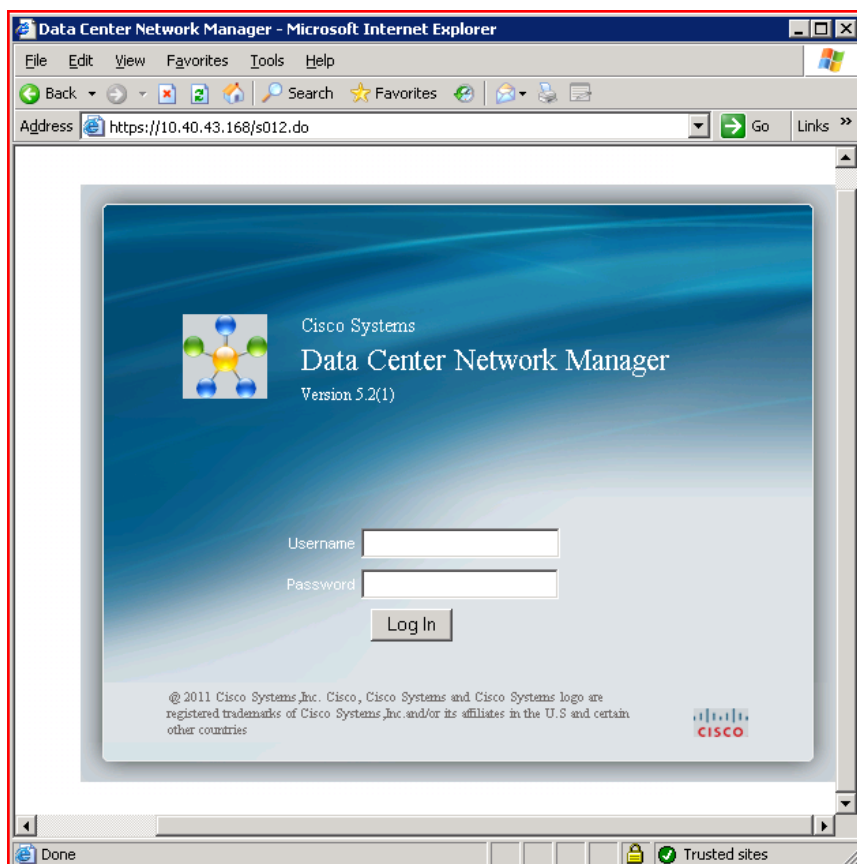
Click on the Client Auth-Privacy dropdown, select SHA-AES, and then click on Open.

**Device Manager Login:**

Click "Options" to expand selections
Enter switch IP address
Enter User ID.
Enter password
Check boxes: SNMPv3
Select Auth-Privacy: SHA and AES
Click Open

**Web Client (Performance Manager):**

Enter: <https://IP Address of DCNM Server>
Login with your soeid and password (Active Directory).



7.4. Vendor Authentication

The vendor will connect to the Cisco switches using SSH, only. If functional IDs are not allowed in Active Directory, the vendor will authenticate with a functional ID on the local Windows DCNM server. When logging into the switches via SSH, the vendor will have to enter their ID as *DCNMservername\vendorID* to connect to the switch.

The vendor will need to update their site maintenance documentation. Storage Management will communicate this information to EMC, for each Data Center Network Manager Server instance.

- Cisco switch IP addresses
- DCNM Server
- EMC functional user ID \ Password

Note: Entering *DCNMservername\soeid* is not a requirement for Citi personnel. They will be authenticated by Active Directory and can enter the ID as *soeid*, without *DCNMservername*.

7.5. Purpose of Network-Admin Role

The default “admin” user ID on the switch is a member of the Network-Admin role, which has full privileges on the switch. This ID cannot be deleted. The password for “admin” should be stored in

a safe place. Some select Storage Operations personnel should also be made members of the Active Directory group that corresponds to the network-admin group.

These IDs should not be used for BAU tasks, but for the following exceptional situations:

- NPS/Active Directory is down or incorrectly configured and you are unable to log on.
 - If the switches were configured per Section [Configure DCNM to authenticate to Active Directory](#) to allow local authentication as the secondary authentication mechanism, you can use the “admin” ID to log on to a switch via SSH. *Depending on the length of the outage, you can execute the “[Back Out of Active Directory](#)”. This would enable the use of DCNM in this situation.*
 - Or, you can use the “admin” ID to log on via the console port (Terminal Server) and reset the configuration
- The management interface is not accessible due to:
 - Bad IP ACL entry
 - Incorrect IP address, mask or default gateway
 - The physical Ethernet interface has failed

In such cases the switch can be accessed via the console port by using the “admin” ID.

- Existing role definitions need to be modified. A user with network-admin privileges can make these changes.
- New roles need to be added. A user with network-admin privileges can add new roles.
- Non-interactive authentication users (see following section) need to be created locally on the switch. A user with network-admin privileges can create such users.

7.6. Non-Interactive Authentication

Scripts that do not alter switch configuration, such as those that will report user entitlements or backup switch configuration, can use non-interactive, public/private key based authentication. Scripts that will make changes to the configuration, should be started and monitored by an Operator and therefore should continue to use interactive authentication. Under no circumstances should usernames and passwords be coded in the script.

One or more user accounts can be created for scripts that will use public/private key based authentication. From a security assessment perspective, these user accounts will be treated as functional IDs with read only privileges. The following illustrates how the key pair can be generated and associated with a user account on the switch.

Note: Throughout the following discussion it will be assumed that user ID “im12345” is logged on to the Management Server. Paths will change if a different user is logged on.

Step1: Generate keys by using SSH utilities on the Management Server

```
ssh-keygen2 -t rsa -P key
```

This will generate two files under the “c:\documents and settings\im12345\application data\ssh\userkeys:

key: file containing private key

key.pub: file containing public key

Step 2: Copy the public key file to the switch bootflash: by using SFTP from the switch

You will need to copy the key.pub file to the user’s home directory to be able to access it from sftp on the switch. The home directory for user “im12345” is “c:\documents and settings\im12345”.

```
Switch# copy sftp://MgmtSvrIP/home/key.pub bootflash:key.pub
```

Step 3: Associate the public key with a user account on the switch

! Enter configuration mode
config

! Create a new user called scriptuser
username scriptuser

! Associate the public key just copied to this user
username scriptuser sshkey file bootflash:key.pub

! Do not forget to give limited privileges to this user⁶
username scriptuser role script

! Exit config mode
exit

! Delete the public key file
delete bootflash:key.pub

! Save
copy run start

Step 4: Test the account by logging on to the switch

```
ssh2 scriptuser@switch.citi.com
```

⁶ Please see Template for a definition of the role “script”

You should be logged in without being asked for a user ID or password.

Use the `-v` switch with `ssh2` command line to troubleshoot any problems.

Note: To run `scriptuser` from a UNIX platform, the `key.pub` file can be copied from the Windows DCNM Server to a UNIX server. The “`dos2unix`” command can be run to convert the file to a UNIX format.

7.7. Functional IDs

The Citi Information Security Standards (CISS) require that each user must be identified with a unique user ID. However, certain operations on information systems might require the use of IDs not directly associated with an individual. Additionally, applications might also require the use of these types of IDs for support, batch/internal processes, or other reasons. These IDs are referred to as “functional IDs”. The table below will assist Operations in determining the ID characteristics and when the passwords need to be changed.

Reference Documentation:

<http://www.citigroup.net/informationsecurity/itispolstd.htm>

Application	Account	Interactive/Non-Interactive	Privileged/Non-Privileged	Password Change Frequency
Cisco MDS Switch	admin	Interactive	Privileged	6 Months
Cisco MDS Script Access	scriptuser	Non-Interactive	Non-Privileged	N/A - Private/public key
Cisco MDS Vendor Access	emc, hds	Interactive	Non-Privileged	12 Months
Cisco DCNM	admin	Interactive	Privileged	6 Months
PostgreSQL Database	postgres	Non-Interactive	Non-Privileged	Password changes are not required

8. Audit Trail Management (SEMS)

The MDS switch captures all security and system administration events in an internal log that can be accessed through CLI or Device Manager. The switch is also capable of sending these events to external system(s) via the SYSLOG protocol as they occur. Since SEMS has replaced eTrust Audit, the process to collect audit events has been improved and is simpler, using their SEMS Syslog server.

All possible messages that the MDS can produce are documented in this guide:

http://www.cisco.com/en/US/docs/switches/datacenter/sw/system_messages/reference/sl_nx-os.pdf

Audit logs should be periodically reviewed by the Storage Operations team to meet the following objectives:

1. Identify and investigate attempts to gain unauthorized access to the switch
2. Reconcile changes
3. Investigate root cause of a security incidence (forensic analysis)

Step 1: Contact SEMS Operations

Contact SEMS team by emailing the GSOC team (SEMS Operations) at *CTI Global SOC SDM, specify that you are requesting SEMS audit logging for Cisco switches in your region. They will provide you with the target SEMS Syslog server and SEMS team member to work with.

Step 2: Configure the Switch to Use NTP Time

In order for the date and time stamp on the log events to be accurate and consistent with other systems, the switch should be configured to synchronize its clock with one or more Citi NTP servers. NTP servers in every region are listed here

http://catercollaboration.citigroup.net/domains/networks/Services/Shared%20Documents/NTP/NTP_design_RFP.doc (Refer to Appendix C)

See switch configuration template in [Appendix C](#) for commands needed to configure NTP.

Step 3: Configure Cisco SAN switches to forward events to SEMS connector (Syslog)

Use the Syslog server information provided by the SEMS team to configure the switches. See switch configuration template in [Appendix C](#) for commands needed for configuring logging.

8.1. SEMS Include List

Field to be included	flexString1
Global Filter	All lines with keyword "update:"
Note	Please note the ":" in the filter
Additional filters	Sample Message
:configure terminal	update:165.203.68.61@pts/17:rg96417:configure terminal ; zoneset name TOR_SAN2A vsan 72 ; zone name cmodfswasu1-hb0-a (SUCCESS)"
:Activation	update:snmp_65211_169.193.166.52:sn78586:Activation of zoneset ecd13b-active attempted on VSAN 29
:Added	update:snmp_63918_169.193.192.161:sm20316:Added attr-group toruat01-hb0-a-attr-group to zone toruat01-hb0-a on VSAN 70
	update:snmp_65475_169.193.192.161:sm20316:Added member [WWN: 50:06:01:60:47:20:26:bd ID: 1] to zone TORPRD01-hb0-a on VSAN 70
	update:snmp_61734_153.40.137.170:dn65671:Added flow stat 9 Entity 22 sid 10035 did 30036 ffffff VSAN 21 module 0
	update:snmp_65202_153.40.137.169:bk19197:Added zone nacswdvhsbv005-hb1-a to zoneset ucd08a_Fab_A on VSAN 44
	update:snmp_65475_169.193.192.161:sm20316:Added member [WWN: 50:06:01:60:47:20:26:bd ID: 1] to zone TORPRD01-hb0-a on VSAN 70
:added	update:159.17.206.9@pts/17:kh64535:added user:hds to the role:vendor
:adding	update:153.40.137.170@pts/17:ss42300:adding to trunking membership of port-channel 13: 11
:assigned	%\$VSAN 97%\$ update:165.203.108.34@pts/17:rg96417:assigned vsan:97 to interface:fc3/6
:Attribute	update:snmp_57448_153.40.137.169:rr69576:Attribute group cpbswxcwsud1-hb5-b-attr-group is created on VSAN 3
:Broadcast	update:169.193.192.161@pts/0:kh64535:Broadcast zoning policy is set to disable on VSAN 2922
:device-alias	update:cfs_17534811:CLI/SNMPv3:ss42300@169.185.212.194:device-alias name catdb201-hb2-b pwwn 10:00:00:00:c9:54:00:2e"
:fcdomain	%\$VSAN 11%\$ update:153.40.137.170@pts/17:ss42300:fcdomain added allowed configured domain ID list 97-127.
	%\$VSAN 11%\$ update:153.40.137.170@pts/17:ss42300:fcdomain configured domain ID 118 as static.
:Install	update:169.193.192.163@pts/0:kh64535:Install all completed successfully.
:Interface	update:snmp_65175_159.17.206.9:kh64535:Interface fc10/6 description updated to USOUH056N6776-CL2H
:no	update:snmp_53324_169.193.192.160:CLI/SNMPv3:sy69578:no device-alias name nacmwdvhsbe006-hb3-a
	update:169.193.192.163(pts/0):gf89952:no shut:success
:removed	update:159.17.206.9@pts/17:kh64535:removed user:hds from role:network-admin
:Removed	update:snmp_65286_153.40.137.169:as23277:Removed member [WWN: 10:00:00:00:c9:84:10:b6 ID: 5] from zone gtsswdcesx44-hb0-a on VSAN 2
	update:153.40.137.170@pts/17:ss42300:Removed zone test_zoning from zoneset umd01b-active on VSAN 11
:Set	update:169.193.192.160@pts/17:kt16213:Set enhanced zoning mode attempted on VSAN 92
:system	update:169.193.233.89@pts/17:jr10806:system health external-loopback interface fc6/9 force (SUCCESS)
	update:172.24.226.65@pts/17:ap25883:system switchover (REDIRECT)
:updated	update:159.17.206.9@pts/17:kh64535:updated v3 user : hds
:vsan	%\$VSAN 95%\$ update:135.53.240.218@pts/17:ap25883:vsan:95 values updated name:exchange_gcd03b
:zone	update:150.110.105.98@pts/17:MT69094:zone copy active-zoneset full-zoneset vsan 17 (SUCCESS)
:Zone	update:snmp_51828_169.193.192.160:sy69578:Zone crptxdbsp701-hb1-b is created on VSAN 37
:Zoneset	update:169.193.233.89@pts/17:sp65064:Zoneset Exchange_GCD03B is removed on VSAN 95

9. Vendor Remote Access

Vendor Remote Access will be provided so that vendor specialists can remotely log in to the MDS switch to quickly troubleshoot any problems.

9.1. EMC Remote Access Registration

EMC includes support for MDS in their EMC Secure Remote Support Gateway ("ESRS") product. ESRS has already been certified by GDSE for remote support of other EMC products such as Symmetrix (see [EMC Secure Remote Support](#)). EMC Personnel will deploy the EMC Cisco MDS switches to the ESRS Gateway. ESRS has received approval from C3PAR.

9.2. HDS Remote Access Registration

HDS RACC (Remote Access Control Center) has replaced the unreliable VPN solution that was in place. HDS RACC is software that allows HDS support personnel remote connectivity to HDS-managed arrays and SAN switches. RACC uses proxy-server based sessions to HDS from Citi to allow HDS personnel to diagnose production issues in a timely manner. The RACC software runs

on the HDS storage SVP. HDS support personnel maintain the RACC software and the storage devices being managed by RACC. See the CSBE HDS documentation for more information.

10. Integration with ECC

EMC Control Center (“ECC”) is Citi standard SAN monitoring, reporting and provisioning software application. Please see

<http://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/ecc.aspx>.

Currently, only storage utilization reporting capabilities of ECC have been certified by GDSE. As such, there is no need to integrate the MDS with ECC at this time. Future releases of ECC from GDSE might require integration that will be addressed as a part of the ECC project.

11. Integration with SANScreen

SANScreen from NetApp is the Citi standard change monitoring and planning tool for SANs. Please see

<https://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/sanscreen.aspx>

MDS was successfully tested with the latest release of SANScreen version 6.1.2.5.

A read-only SNMP v3 community string must be created on all MDS switches that need to be monitored by SANScreen. Please see [Appendix C: Switch Configuration \(“Template”\)](#).

If Access Control Lists are on the switch, they must be modified to allow SNMP access from the server running SanScreen Acquisition Unit. Please see [Appendix C: Switch Configuration \(“Template”\)](#).

12. Integration with HPNA

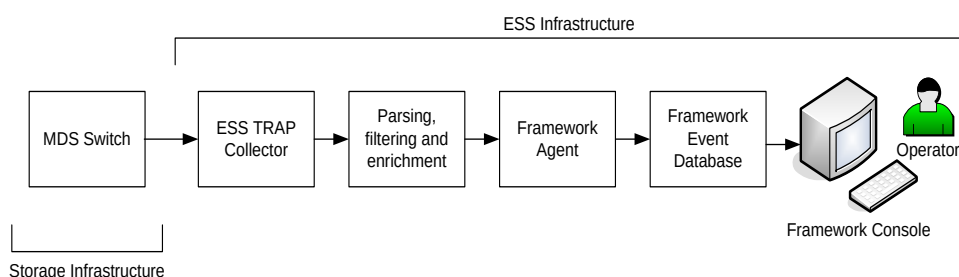
HPNA (HP Network Analyzer) is a tool used in the networking environment to gather switch information, including configurations. It’s used to validate that switches globally are configured the same. HPNA requires the switch name and IP address to be registered in Aperture or NetInfo.

Switch settings that HPNA is validating can be found in the SBCC Config Checklist on our Cisco MDS webpage:

<https://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/ciscomds.aspx>

13. Monitoring the Switch with ESS

The MDS switch should be monitored by Enterprise Systems Services (“ESS”). The switch will generate SNMP v2 TRAPS for select events, such as power supply failure, link failure, etc. The TRAPs will be received by an ESS TRAP collector server and the events posted to a text file. A script will then parse and filter the events.



The framework agent will then gather the processed events and report these to the console. The console will be monitored 24x7 by the Console Operator(s). A Process Control Manual (“PCM”) developed by Regional Storage Operations teams will direct the Console Operator to deal with alerts that show up on the console. Another PCM developed by Regional Storage Operations team will direct Storage Operator actions against all possible events.

13.1. Implementation Steps

- ✓ Storage Operations team will engage regional ESS engineering/integration teams:

Region	Framework	Owner
APPC	BMC Patrol	Jit-Soon Koh
Mexico	HP Openview, MOM	Alfonso Diaz Jimenez
EMEA	Tivoli, Ice	Sean Lonegran
Japan	Tivoli, Ice	Carl Pickin
NA	Tivoli, Ice, NetIQ, MOM, HP Openview	Roger Kutchaver

- ✓ Regional ESS engineering/integration team will:
 - Configure the TRAP collector server(s)
 - Create scripts to parse, filter, enrich and categorize TRAPS according to GDSE specifications contained in the following section
- ✓ Storage Operations will configure the Cisco MDS switches
- ✓ Storage Operations will test the system by triggering test TRAPs from MDS

13.2. TRAPS to Monitor

All the MIBs supported by Cisco MDS NX-OS 5.2.x software are in this file:

http://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/mds9000/sw/5_2/technical/reference/mibs_zip/mibs521.zip

All the MIBs supported by Cisco MDS NX-OS 6.2.x software are in this file:

http://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/mds9000/sw/6_2/technical/reference/mibs_zip/mibs621.zip

Cisco also provides an online MIB browser tool at:

<http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en>

GDSE has identified the following TRAPs for use within Citi:

Color Code	Category	Notification
	Critical	Tivoli/Generate Ticket
	Warning	Email Notification
	Informational	Informational/Clear

Enterprise ID of TRAP	Specific Type	Category	Description	Generate alert only if variable	Include in the Message ⁷	Variable Type
1.3.6.1.4.1.9.9.276	1		Link Down	N/A	Interface Name = 1.3.6.1.2.1.31.1.1.1.1	String
1.3.6.1.4.1.9.9.276	2		Link Up	N/A	Interface Name = 1.3.6.1.2.1.31.1.1.1.1	String
1.3.6.1.4.1.9.9.289.1.3	1		(E)ISL Port Down	1.3.6.1.4.1.9.9.289.1.1.3.1.1.* = 2 (down)	Cause = 1.3.6.1.4.1.9.9.289.1.1.3.1.3.*	String
1.3.6.1.4.1.9.9.289.1.3	2		(E)ISL Port Up	1.3.6.1.4.1.9.9.289.1.1.3.1.1.* = 1 (up)	Cause = 1.3.6.1.4.1.9.9.289.1.1.3.1.3.*	String
1.3.6.1.4.1.9.9.282.1.3	1		VSAN Status Change to DOWN	1.3.6.1.4.1.9.9.282.1.1.3.1.8.* = 2 (down)	VSAN ID = 1.3.6.1.4.1.9.9.282.1.1.4.*	Positive Integer, range 0 – 4099
1.3.6.1.4.1.9.9.302.1.3	1		VSAN Segmentation	N/A	VSAN ID = 1.3.6.1.4.1.9.9.282.1.1.4.*	Positive Integer, range 0 - 4099
1.3.6.1.4.1.9.9.302.1.3	3		Build Fabric (BF) or ReConfigure Fabric (RCF) Event	N/A	VSAN ID = 1.3.6.1.4.1.9.9.282.1.1.4.*	Positive Integer, range 0 – 4096
1.3.6.1.4.1.9.9.294.1.4	2		Zone Merge Failure	N/A	VSAN ID = 1.3.6.1.4.1.9.9.294.1.3.3.*	Positive Integer, range 0 – 4096
					Failure Reason = 1.3.6.1.4.1.9.9.294.1.3.6.*	1:other 2:zoningModeMismatch 3:qosNotEnabled 4:qosConflict 5:bcastNotEnabled 6:mergeCtrlMismatch 7:defZoneMismatch 8:qosAttrMissing 9:bcastAttrMissi

⁷ All messages should include the IP address and/or the DNS name of the switch sending the TRAP and the Description

						ng 10:rdonlyAttrMi ssing 11:memberMism atch 12:invPayloadFo rmat 13:sizeExceeded 14:unlicensedMe mber 15:nonInteropZo neset
1.3.6.1.4.1.9.9.91.2	1		Temperature exceeded threshold	N/A	Threshold temperature = 1.3.6.1.4.1.9.9.91.1.2.1.1.4.*	Positive Integer range 0-200
					Current Temperature = 1.3.6.1.4.1.9.9.91.1.1.1.1.4.*	Positive Integer range 0-200
1.3.6.1.4.1.9.9.117.2	6		Fan Tray Status	1.3.6.1.4.1.9.9.117.1.4.1.1.1.* ≠ 2	Fan tray status = 1.3.6.1.4.1.9.9.117.1.4.1.1.1.*	1 : unknown 2 : up 3 : down 4 : warning
1.3.6.1.4.1.9.9.117.2	2		Power Status	1.3.6.1.4.1.9.9.117.1.1.2.1.2.* ≠ 2	Power status = 1.3.6.1.4.1.9.9.117.1.1.2.1.2.*	1:offEnvOther 2:on 3:offAdmin 4:offDenied 5:offEnvPower 6:offEnvTemp 7:offEnvFan 8:failed 9:onButFanFail 10:offCooling 11:offConnector Rating 12:onButInlineP owerFail
1.3.6.1.4.1.9.9.117.2	1		Module Status	1.3.6.1.4.1.9.9.117.1.2.1.1.2.* ≠ 2	Module status = 1.3.6.1.4.1.9.9.117.1.2.1.1.2.*	1:unknown 2:ok 3:disabled 4:okButDiagFail ed 5:boot 6:selfTest 7:failed 8:missing 9:mismatchWith Parent 10:mismatchCon fig 11:diagFailed 12:dormant 13:outOfService Admin

						14:outOfService EnvTemp 15:poweredDown 16:poweredUp 17:powerDenied 18:powerCycled 19:okButPowerOverWarning 20:okButPowerOverCritical 21:syncInProgress
1.3.6.1.4.1.9.9.176.2	1		Supervisor Failover	N/A	Reason = 1.3.6.1.4.1.9.9.176.1.1.8.*	1:unsupported 2:none 3:notKnown 4:userInitiated 5:userForced 6:activeUnitFailed 7:activeUnitRemoved
1.3.6.1.2.1.16.29.2.0	1		hcRisingAlarm	N/A	Alarm Variable 1.3.6.1.2.1.16.29.1.1.1.3*	Integer
					Alarm Sample Type 1.3.6.1.2.1.16.29.1.1.1.4*	1:absoluteValue 2:deltaValue
					Alarm Absolute Value 1.3.6.1.2.1.16.29.1.1.1.5*	Integer
					Alarm Value Status 1.3.6.1.2.1.16.29.1.1.1.6*	1:valueNotAvailable 2:valuePositive 3:valueNegative
					Alarm Rising ThreshAbsValueLo 1.3.6.1.2.1.16.29.1.1.1.8*	Integer
					Alarm Rising ThreshAbsValueHi 1.3.6.1.2.1.16.29.1.1.1.9*	Integer
					Alarm Rising ThresholdValStatus 1.3.6.1.2.1.16.29.1.1.1.10*	1:valueNotAvailable 2:valuePositive 3:valueNegative
					Alarm Rising EventIndex 1.3.6.1.2.1.16.29.1.1.1.14*	Positive Integer 0 - 65535
1.3.6.1.2.1.16.29.2.0	2		hcFallingAlarm	N/A	Alarm Variable	Integer

					1.3.6.1.2.1.16.29.1.1.1.1.3*	
					Alarm Sample Type 1.3.6.1.2.1.16.29.1.1.1.1.4*	1:absoluteValue 2:deltaValue
					Alarm Absolute Value 1.3.6.1.2.1.16.29.1.1.1.1.5*	Integer
					Alarm Value Status 1.3.6.1.2.1.16.29.1.1.1.1.6*	1:valueNotAvailable 2:valuePositive 3:valueNegative
					Alarm Rising ThreshAbsValueLo 1.3.6.1.2.1.16.29.1.1.1.1.8*	Integer
					Alarm Rising ThreshAbsValueHi 1.3.6.1.2.1.16.29.1.1.1.1.9*	Integer
					Alarm Rising ThresholdValStatus 1.3.6.1.2.1.16.29.1.1.1.1.10*	1:valueNotAvailable 2:valuePositive 3:valueNegative
					Alarm Rising EventIndex 1.3.6.1.2.1.16.29.1.1.1.1.14*	Positive Integer 0 - 65535
1.3.6.1.6.3.1.1.5	3		LinkDown	N/A	Status = 1.3.6.1.2.1.2.2.1.8.*	1:up 2:down 3:testing 4:unknown 5:dormant 6:notPresent 7:lowerLayerDown
1.3.6.1.6.3.1.1.5	4		LinkUp	N/A	Status = 1.3.6.1.2.1.2.2.1.8.*	1:up 2:down 3:testing 4:unknown 5:dormant 6:notPresent 7:lowerLayerDown
1.3.6.1.4.1.9.9.706.0.1	1		SFP Transceiver Alarm	N/A	ifName 1.3.6.1.2.1.31.1.1.1.1.*	String
					cIfXcvrMonDigitalDiagTempAlarm 1.3.6.1.4.1.9.9.706.1.1*	1:highSet 2:lowSet 3:highClear 4:lowClear 5:normal
					cIfXcvrMonDigitalDi	1:highSet

			agTempWarning 1.3.6.1.4.1.9.9.706.1. 2*	2:lowSet 3:highClear 4:lowClear 5:normal
			cIfXcvrMonDigitalDi agVoltAlarm 1.3.6.1.4.1.9.9.706.1. 3*	1:highSet 2:lowSet 3:highClear 4:lowClear 5:normal
			cIfXcvrMonDigitalDi agVoltWarning 1.3.6.1.4.1.9.9.706.1. 4*	1:highSet 2:lowSet 3:highClear 4:lowClear 5:normal
			cIfXcvrMonDigitalDi agCurrAlarm 1.3.6.1.4.1.9.9.706.1. 5*	1:highSet 2:lowSet 3:highClear 4:lowClear 5:normal
			cIfXcvrMonDigitalDi agCurrWarning 1.3.6.1.4.1.9.9.706.1. 6*	1:highSet 2:lowSet 3:highClear 4:lowClear 5:normal
			cIfXcvrMonDigitalDi agRxPwrAlarm 1.3.6.1.4.1.9.9.706.1. 7*	1:highSet 2:lowSet 3:highClear 4:lowClear 5:normal
			cIfXcvrMonDigitalDi agRxPwrWarning 1.3.6.1.4.1.9.9.706.1. 8*	1:highSet 2:lowSet 3:highClear 4:lowClear 5:normal
			cIfXcvrMonDigitalDi agTxPwrAlarm 1.3.6.1.4.1.9.9.706.1. 9*	1:highSet 2:lowSet 3:highClear 4:lowClear 5:normal
			cIfXcvrMonDigitalDi agTxPwrWarning 1.3.6.1.4.1.9.9.706.1. 10*	1:highSet 2:lowSet 3:highClear 4:lowClear 5:normal
			cIfXcvrMonDigitalDi agTxFaultAlarm 1.3.6.1.4.1.9.9.706.1. 11*	1:highSet 2:lowSet 3:highClear 4:lowClear 5:normal

All other TRAPs should be filtered out.

13.3. Testing

The system should be tested during initial deployment and then annually to make sure that all components in the TRAP path are operational. NX-OS allows the following test TRAPs to be triggered from the CLI:

```
switch# test pfm snmp test-trap fan
switch# test pfm snmp test-trap powersupply
switch# test pfm snmp test-trap temp_sensor
```

The above commands are completely non-disruptive.

14. N_Port ID Virtualization (NPIV)

NPIV allows multiple hosts to connect to the SAN over the same physical port. This technology has been certified within Citi for connecting HP Blade System to the SAN. NPIV should be enabled on all MDS switches at the time of deployment (see Configuration Template in appendix D). To check whether NPIV is enabled, use the following command on the switch:

```
Switch# show run | include npiv
```

If the output of the command is

```
npiv enable
```

NPIV is enabled. Otherwise if the output is blank, NPIV can be enabled with the following non-disruptive command:

```
Switch (config)# npiv enable
```

15. Switch Backup and Restore Process

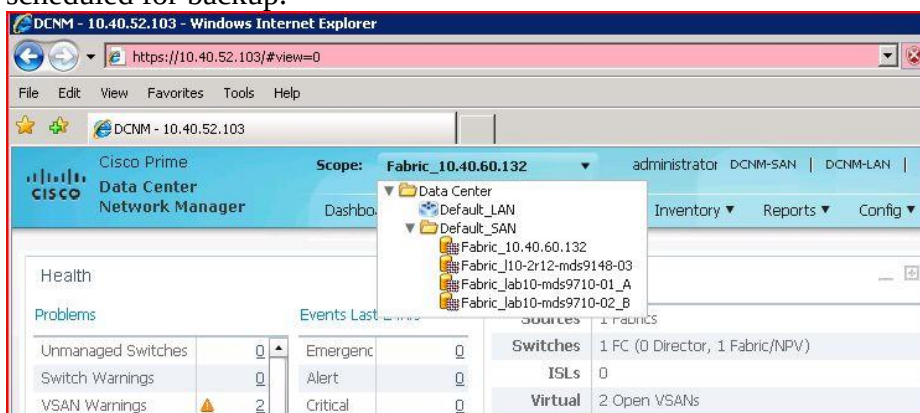
With the new SAN architecture of using MDS 9148's as the edge switches, the manual process of backing up switches with scripts and restoring them will be cumbersome. DCNM 6.3.1 and greater Web Client has greatly improved over past versions. Via the Web Client switches can be scheduled for backup on a daily or weekly basis. Restoring a failed switch is much simpler too.

Note: DCNM backup and restore requires DCNM SAN switch licensing. See [Section 20](#).

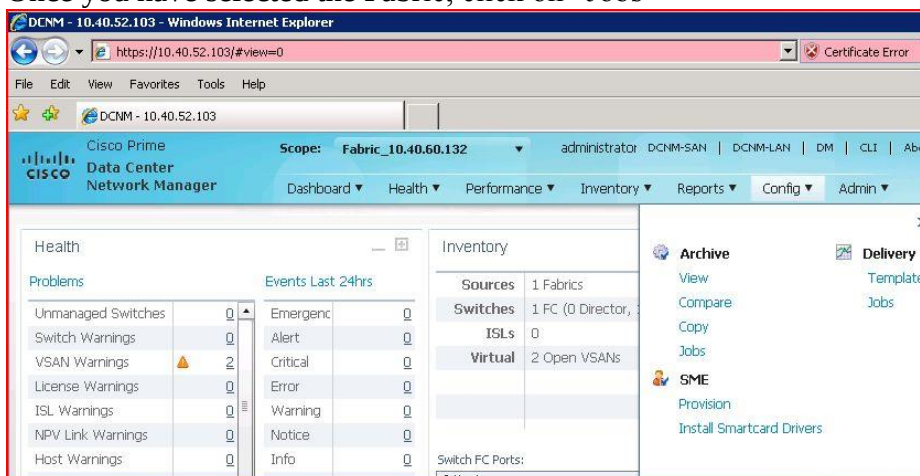
15.1. Switch Backup via DCNM Web Client

Schedule Automatic Switch Backups:

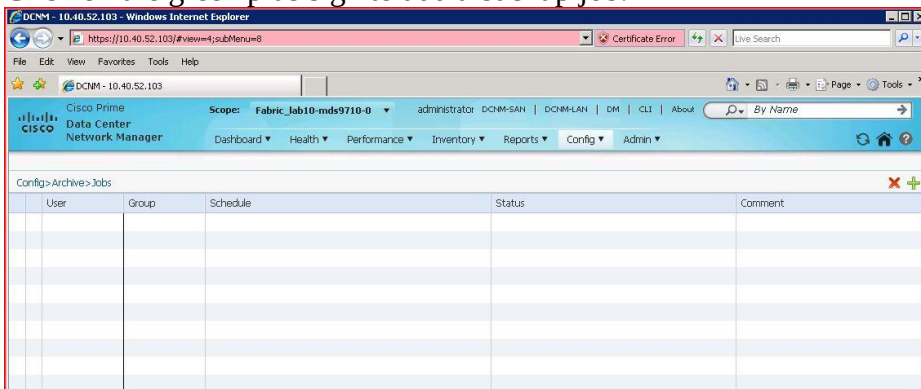
1. Log into the DCNM Web Client. Under “Scope:” use the dropdown to select the Fabric to be scheduled for backup.



2. Once you have selected the Fabric, click on “Jobs”



- Click on the green plus sign to add a backup job.



The “Create Config Archive Job” window will open. Select your backup schedule and select “Create”.



Create Config Archive Job

Repeat: ☐ Once ☐ Daily ☒ Weekly

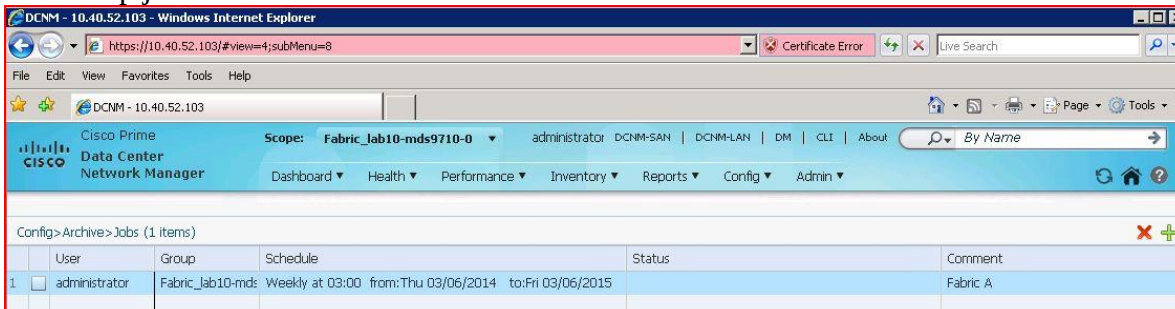
Start: 03/06/2014 03 : 00 pm

End: 03/06/2015

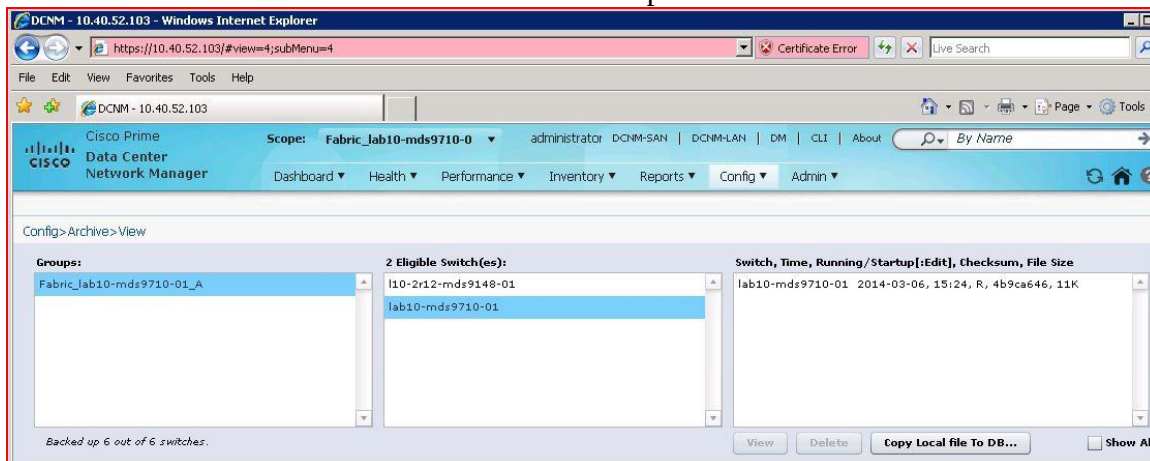
Comment: Fabric A

Create

- A backup job is scheduled to run



- Once the backup job has run, you can verify your backups by selecting the Fabric under “Scope”, then selecting “Config” and “View”.
Select the Fabric and each switch to see the backups for each.

**Note:**

- By default switch backups are kept for 90 days before they roll off (deleted).
- 1The switch config is backed up only if it has changed since the prior backup.

15.2. Switch Restore via DCNM Web Client

15.2.1. Prerequisite

- “Spare” switch(es) should be racked and powered up along with all the other new switches
- “Spare” switch(es) should have:
 - The generic admin password
 - IP / Default-Gateway configured on them
 - Current NX-OS version
 - Only IP connectivity, no fibre cables connected

Note: For MDS 9148 switches that will be running in NPV Mode, you'll need to discover the switch via DCNM, prior to enabling NPV. DCNM can't discover a switch in NPV mode, because an NPV mode switch can't be the “seed switch”. Instructions in the next section.

15.2.2. OPS – Restore from Backup

- The switch should have a cisco default config; no configuration was done on the switch other than setting the admin password and the IP address, IP mask and default IP gateway and current NX-OS version.
- Prior to restore, shutdown the Port-Channels to the failed switch from each Core switch. From CLI on the Core Switches, issue the following commands, substituting the appropriate port-channel number. This will prevent the switch from merging with the fabric, until the

zoneset is deactivated. Failure to shut these port-channels down can result in a failed merger and a segmented fabric.

In this example port-channel1 goes from Edge1 to Core1 and port-channel51 goes from Edge1 to Core2.

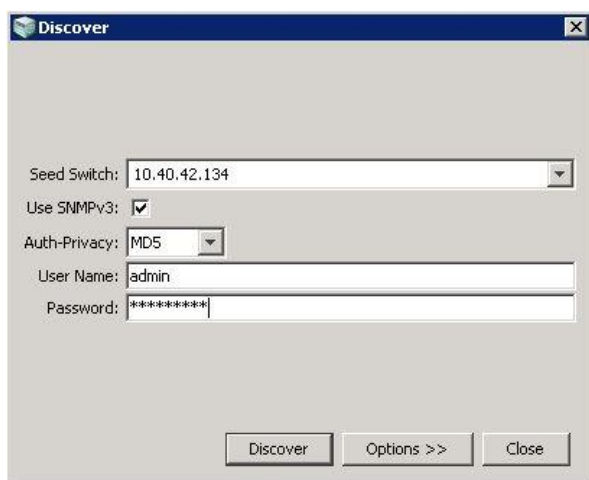
From Core 1:

```
Core1-switch# conf
Core1-switch(config)# interface port-channel 1
Core1-switch(config-if)# shut
Core1-switch(config-if)# exit
Core1-switch(config)#
```

From Core 2:

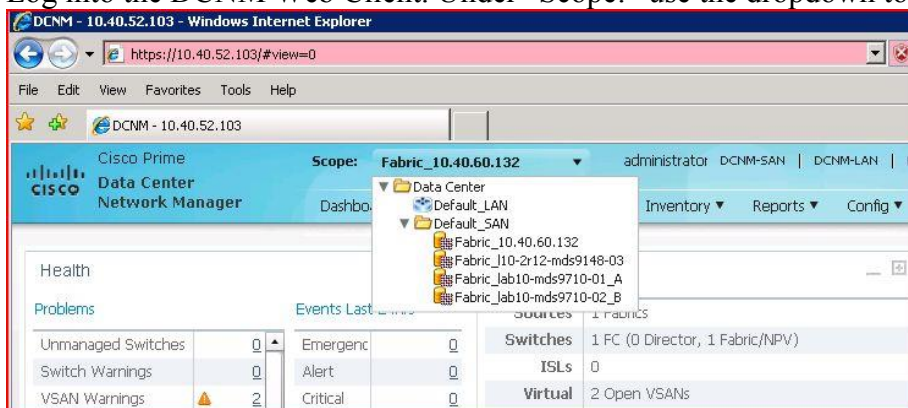
```
Core2-switch# config
Core2-switch(config)# interface port-channel 51
Core2-switch(config-if)# shut
Core2-switch(config-if)# exit
Core2-switch(config)#
```

3. From the DCNM SAN Client, **“Purge”** the failed switch, then discover the replacement switch with existing IP address, generic admin ID and password.



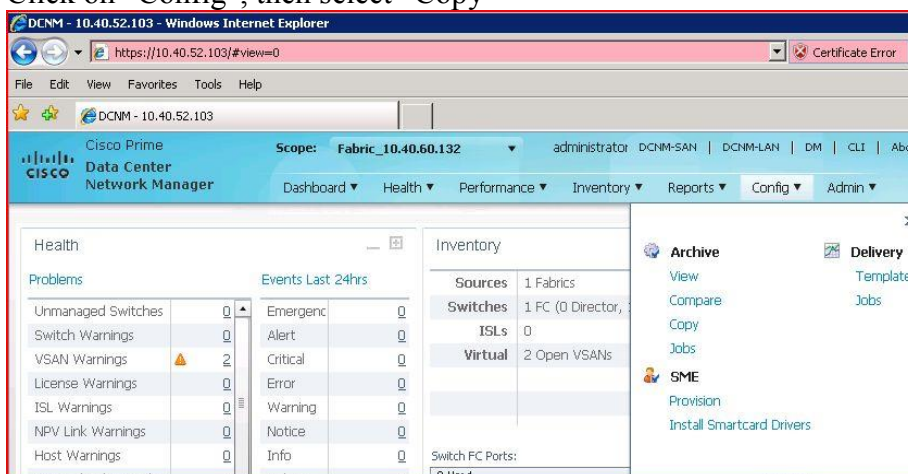
- a. After discovering a MDS 9148 switch that you want to run in **NPV mode**, log into the switch via CLI and enable NPV (“feature npv”). It will “erase” the config and perform a “reload”. The configuration will be lost, except for the IP configuration.

- Log into the DCNM Web Client. Under “Scope:” use the dropdown to select “Default SAN”.

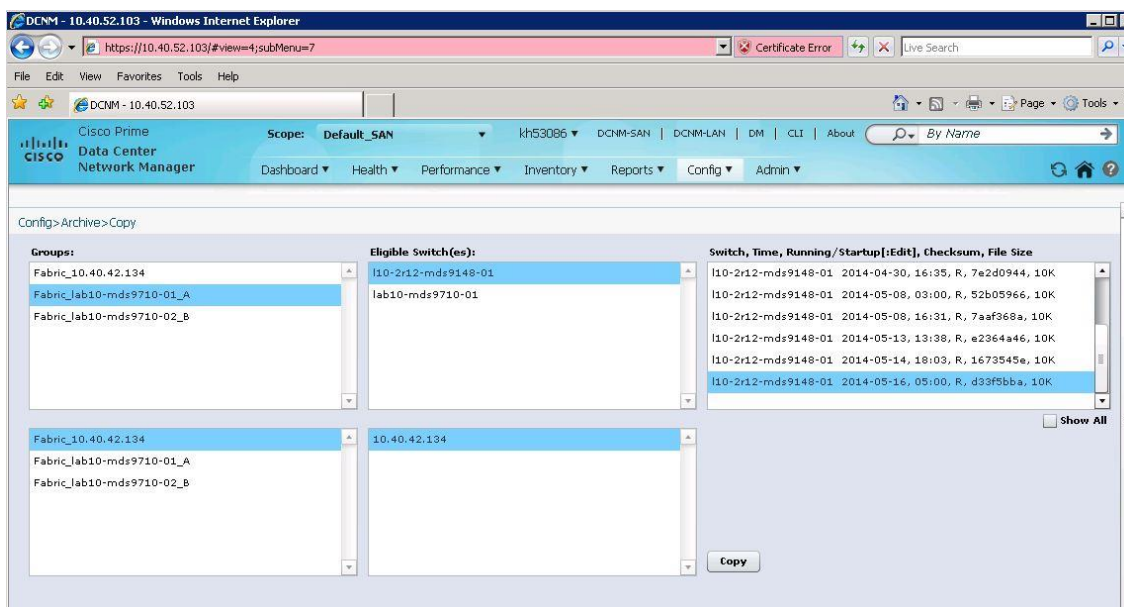


NOTE: It may take a few minutes for DCNM SAN Client to sync up with the DCNM Web Client. Or click on Admin, Data Sources. The switch should be discovered.

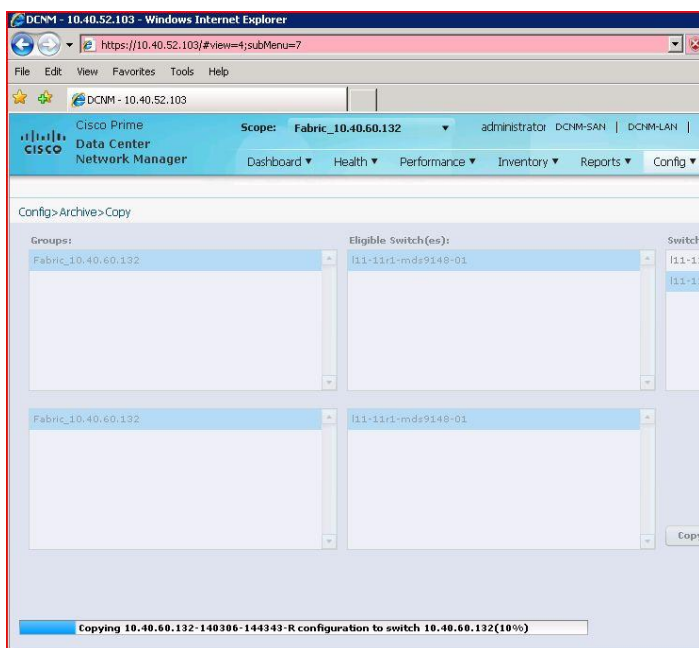
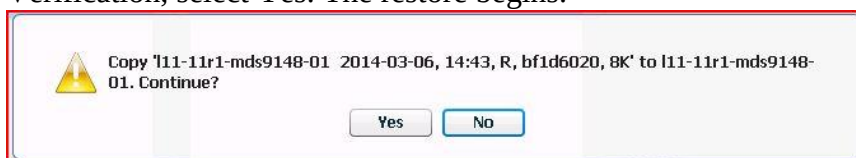
- Click on “Config”, then select “Copy”



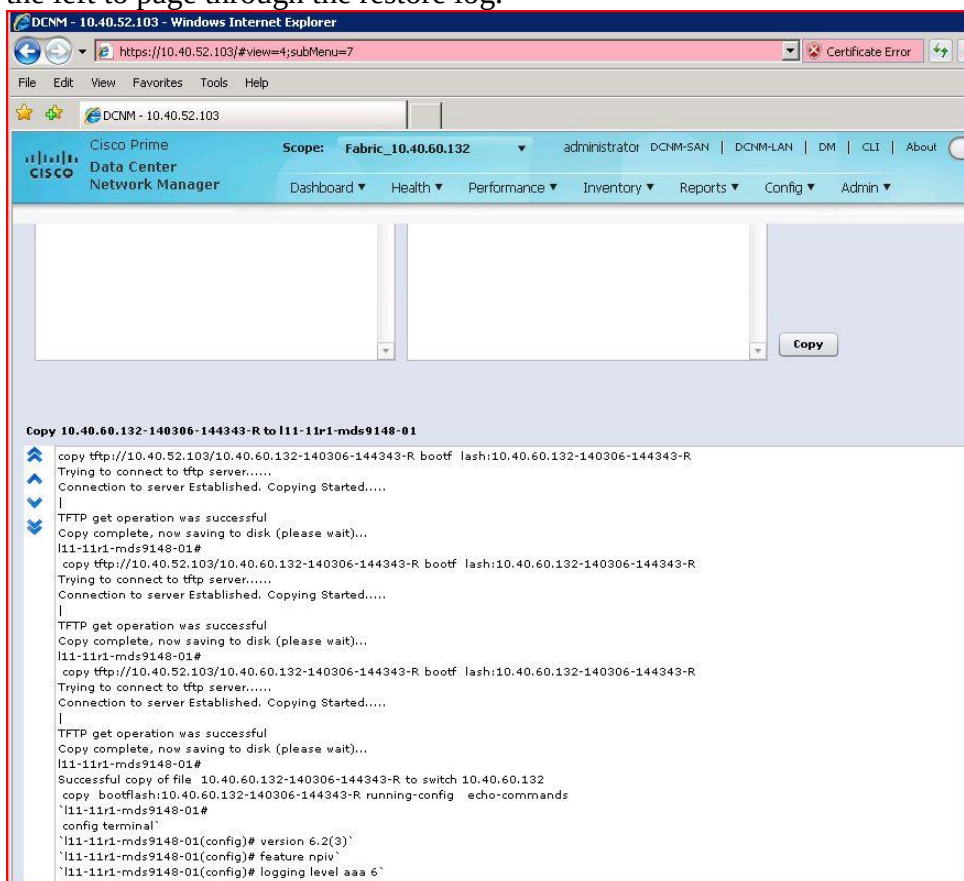
- Under Groups, select the Fabric name of the switch that failed.
Under Eligible Switches, select the switch name of the failed switch.
Under Switch, Time..., select the latest backup file for the failed switch to restore to the replacement switch.
On the next row, under Groups, select the replacement switch Fabric Name or switch IP.
Under Eligible Switches, select the replacement switch IP.
Select Copy (to copy the backup to the replacement switch)



7. Verification, select Yes. The restore begins.



8. When the restore is completed, the details are posted in the lower panel. Select the arrows to the left to page through the restore log.



9. The restore process restores the RADIUS encrypted key. You'll need to login into the switch with the admin ID and run the command to add the key.

```
conf
radius-server host radius-server-ip-address key ciscokeyname
radius commit
exit
```

10. Turn Spare switch over to Vendor to have it re-racked.

15.2.3. Vendor: (Replace failed switch with Spare)

1. **After the restore has been completed**, Ops will turn over to the vendor to replace the failed switch with the restored "spare" switch.
2. Power up the newly restored switch
3. Reconnect fibre channel cables to the appropriate ports (as they were in the failed switch)
4. Turn over to Ops to facilitate the switch merge to the existing fabric.

15.2.4. OPS: (Merge new *NPV* switch with fabric)

1. Since an NPV mode switch doesn't store Zoning, Device-Alias or Domain IDs, it is less likely to have problems merging with the Fabric.

From the Replacement (New) Edge switch:

Login to the Edge switch via SSH using SOEID/password

Bring the port-channels back up so the newly restored switch will merge with the existing fabric.

From the Core1 switch:

```
Core1-switch# config
Core1-switch(config)# interface port-channel x (port-channel from Core1 to failed switch)
Core1-switch(config-if)# no shut
Core1-switch(config-if)# exit
Core1-switch#
```

From the Core2 switch:

```
Core2-switch# config
Core2-switch(config)# interface port-channel x (port-channel from Core2 to failed switch)
Core2-switch(config-if)# no shut
Core2-switch(config-if)# exit
Core2-switch#
```

2. From the DCNM SAN Client, discover the newly restored switch with the original IP address of the failed switch and the admin ID and password that is used to manage the fabric. Check DCNM SAN Client to see if the restored switch merged with its fabric.

15.3. Management Server Backup and Recovery

Management Server stores:

- Topology Map (The map displays a graphical view of the fabric)
 - Enclosure names – The map ordinarily displays each HBA as a separate node. A server entity can be defined with multiple HBAs and labeled with the server name. This definition and label are stored on the Management Server
 - Layout – Operator can move elements on the map around to suit his tastes. The layout is stored on the Management Server.
- Performance data
 - The Performance Manager software component constantly gathers performance data from the switches. This data can be used to identify bottlenecks and trends that can help troubleshoot issues and plan for future growth. It is also an important tool to monitor front end oversubscription. The gathered data is stored on the Management Server.

This data is stored within “*InstallDirectory*:\Program Files\Cisco Systems\dcn” on the Management Server. This folder should be backed up on a nightly basis.

All switch configuration, zonesets, zones and device alias data is stored on every switch in the fabric, not on the Management Server. Because the CLI is a superset of the GUI, business as usual operations such as zoning can be carried out via CLI from another workstation even as the Management Server is being rebuilt.

16. Port Group Monitoring

Port-group-monitor is a command that allows you to monitor port groups that go above and below a configurable bandwidth threshold. When the traffic for a particular port group reaches 80 percent of the maximum supported bandwidth for that port group (rx and tx), NX-OS generates a syslog message that identifies individual port bandwidth (for rx and tx). A syslog message is generated for a rising threshold and for a falling threshold. When port group monitoring is enabled, monitoring occurs every ten seconds.

To enable the Port Group Monitor feature, use the port-group-monitor enable command. To disable this feature, use the no form of the command.

```
port-group-monitor enable
no port-group-monitor enable
```

Example:

```
switch(config)# port-group-monitor enable
switch(config)#
```

```
switch(config)# no port-group-monitor enable
switch(config)#
```

To activate the specified Port Group Monitor policy, use the `port-group-monitor activate` command. To deactivate the Port Group Monitor policy, use the `no` form of the command. The policy name is optional and not required.

```
port-group-monitor activate {name}
no port-group-monitor activate {name}
```

Example

```
switch(config)# port-group-monitor activate pgmon
switch(config)#
```

```
switch(config)# no port-group-monitor activate pgmon
switch(config)#
```

`show port-group-monitor` Displays Port Group Monitor information

```
switch# show port-group-monitor
```

```
-----
Port Group Monitor : enabled
-----
```

```
Policy Name : default
Admin status : Active
Oper status : Active
Port type   : All Port Groups
-----
```

```
Counter      Threshold Interval %ge Rising Threshold %ge Falling Threshold In Use
-----
RX Performance Delta    60    80          20          Yes
TX Performance Delta    60    80          20          Yes
-----
```

17. Port Monitoring

Port monitor helps to monitor the performance and the status of ports and generate alerts when problems occur. You can configure the thresholds for various counters and trigger an event when the values cross the threshold settings. The port-monitor functionality doesn't have the limitations that RMON possesses.

Enable / disable Port Monitoring

<code>port-monitor enable</code>	Enables (default) port monitoring.
<code>no port-monitor enable</code>	Disables port monitoring.

The following example shows how to activate a port monitor policy. By entering a policy name, it puts you in policy configuration mode.

<code>#config</code>	
----------------------	--

(config)# port-monitor name <i>polycname</i>	Specifies the policy name and enters the port monitoring policy configuration mode.
switch(config)# no port-monitor name <i>polycname</i>	Removes the policy
(config-port-monitor)# port-type access-port	Applies the policy to the access ports.
(config-port-monitor)# port-type trunks	Applies the policy to the trunk ports.
(config-port-monitor)# port-type all	Applies the policy to all ports.

Activate / deactivate the default port-monitor policy.

port-monitor activate	Activates the default port monitor policy
no port-monitor activate	Deactivates the default port monitor policy

17.1. Default Port Monitor Policy Settings

```
gdse-2r11-mds9500-01# show port-monitor
```

Port Monitor : disabled

Policy Name : default
Admin status : Not Active
Oper status : Not Active
Port type : All Ports

Counter	Threshold	Interval	Rising Threshold	event	Falling Threshold	event	Portguard
Link Loss	Delta	60	5	4	1	4	Not enabled
Sync Loss	Delta	60	5	4	1	4	Not enabled
Signal Loss	Delta	60	5	4	1	4	Not enabled
Invalid Words	Delta	60	1	4	0	4	Not enabled
Invalid CRC's	Delta	60	5	4	1	4	Not enabled
TX Discards	Delta	60	200	4	10	4	Not enabled
LR RX	Delta	60	5	4	1	4	Not enabled
LR TX	Delta	60	5	4	1	4	Not enabled
Timeout Discards	Delta	60	200	4	10	4	Not enabled
Credit Loss Reco	Delta	1	1	4	0	4	Not enabled
TX Credit Not Available	Delta	1	10	4	0	4	Not enabled
RX Datarate	Delta	60	80%	4	20%	4	Not enabled
TX Datarate	Delta	60	80%	4	20%	4	Not enabled

Policy Name : slowdrain
Admin status : Active
Oper status : Not Active
Port type : All Access Ports

Counter	Threshold	Interval	Rising Threshold	event	Falling Threshold	event	Portguard
Credit Loss Reco	Delta	1	1	4	0	4	Not enabled
TX Credit Not Available	Delta	1	10	4	0	4	Not enabled

See the Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide on the GDSE Cisco webpage.

17.2. Recommended Citi Port Monitor Policy Settings

CATE Storage Engineering worked with Cisco and Operations to come up with the following monitoring solution for the Cisco MDS switches. We recognize that our monitoring teams are currently overrun with alerts and we don't want to add more alerts unless they are truly useful alerts. There are three port-monitoring configurations based on the type of switch, 1) ISL Trunk Monitoring, 2) Storage Port Monitoring and 3) Host Port Monitoring.

Run commands as described below:		
Storage Edge Switch	pmon_storage	
Core Switch (ISLs Only)	pmon_eports	
Core Switch with storage (Core / Edge)	pmon_eports	pmon_storage
Host Edge Switch (NPV Enabled)	pmon_hosts	
Host Edge Switch (Non-NPV)	pmon_hosts	

17.2.1. ISL Trunk Monitoring (Core or Core/Storage Switches)

ISL trunks will be monitored from the Core switches. The following port-monitoring alerts will be enabled and they include Port-Guard. These will monitor the ISL trunk ports only. Port-Guard is enabled for pmon_eports configuration only.

Port Monitor Name: pmon_eports

Commands:

```

config t
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO

snmp-server host FQDN-SRM-Server traps version 1 public udp-port 2041
snmp-server enable traps rmon
! The SFP Transceiver should be monitored for High/Low Alarms/Warnings by enabling
! the following trap. High or Low readings can indicate an SFP, HBA or cable issue.
snmp-server enable traps link cisco-xcvr-mon-status-chg
snmp-server enable traps link cieLinkDown
snmp-server enable traps link linkDown
end

config t
logging level snmpd 3
port-monitor enable

no port-monitor activate default

```

```
no port-monitor activate slowdrain
no port-monitor activate e_ports
no port-monitor name e_ports
no port-monitor activate pmon_eports
no port-monitor name pmon_eports
```

```
port-monitor name pmon_eports
port-type trunk
```

```
monitor counter link-loss
monitor counter sync-loss
monitor counter signal-loss
monitor counter invalid-words
monitor counter invalid-crc
monitor counter tx-discards
monitor counter lr-rx
monitor counter lr-tx
monitor counter timeout-discards
monitor counter credit-loss-reco
monitor counter tx-credit-not-available
monitor counter rx-datarate
monitor counter tx-datarate
```

```
counter credit-loss-reco poll-interval 1 delta rising-threshold 1 event 4 falling-threshold 0 event 4
counter tx-credit-not-available poll-interval 1 delta rising-threshold 10 event 4 falling-threshold 0 event 4
```

```
counter link-loss poll-interval 60 delta rising-threshold 3 event 4 falling-threshold 0 event 4 portguard
errordisable
```

```
counter sync-loss poll-interval 60 delta rising-threshold 3 event 4 falling-threshold 0 event 4 portguard
errordisable
```

```
counter signal-loss poll-interval 60 delta rising-threshold 3 event 4 falling-threshold 0 event 4 portguard
errordisable
```

```
counter invalid-crc poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4 portguard
errordisable
```

```
counter invalid-words poll-interval 60 delta rising-threshold 10 event 4 falling-threshold 0 event 4
portguard errordisable
```

```
counter rx-datarate poll-interval 60 delta rising-threshold 80 event 4 falling-threshold 50 event 4
counter tx-datarate poll-interval 60 delta rising-threshold 90 event 4 falling-threshold 50 event 4
```

```
counter tx-discards poll-interval 60 delta rising-threshold 100 event 4 falling-threshold 10 event 4
counter lr-rx poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4
counter lr-tx poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4
counter timeout-discards poll-interval 60 delta rising-threshold 100 event 4 falling-threshold 10 event 4
```

```
exit
port-monitor activate pmon_eports
end
```

Result:

Policy Name : pmon_eports							
Admin status : Active							
Oper status : Active							
Port type : All Trunk Ports							
Counter	Threshold	Interval	Rising Threshold	event	Falling Threshold	event	PMON Portguard
Link Loss	Delta	60	3	4	0	4	Error Disable
Sync Loss	Delta	60	3	4	0	4	Error Disable
Signal Loss	Delta	60	3	4	0	4	Error Disable
Invalid Words	Delta	60	10	4	0	4	Error Disable
Invalid CRC's	Delta	60	5	4	0	4	Error Disable
TX Discards	Delta	60	100	4	10	4	Not enabled
LR RX	Delta	60	5	4	0	4	Not enabled
LR TX	Delta	60	5	4	0	4	Not enabled
Timeout Discards	Delta	60	100	4	10	4	Not enabled
Credit Loss Reco	Delta	1	1	4	0	4	Not enabled
TX Credit Not Available	Delta	1	10	4	0	4	Not enabled
RX Datarate	Delta	60	80%	4	50%	4	Not enabled
TX Datarate	Delta	60	90%	4	50%	4	Not enabled

17.2.2. Storage Port Monitoring (Storage or Core/Storage Edge Switch)

Storage ports will be monitored from the Core switches in a 2-Tier SAN design or from the Storage Edges on 3-Tier SAN. The following port-monitoring alerts will be enabled.

Note: Due to concerns with the number of alerts that might be generated, “Tx-datarate” and “Rx-datarate” will not be monitored at this time.

Port Monitor Name: pmon_storage

Commands:

```

config t
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO

snmp-server host FQDN-SRM-Server traps version 1 public udp-port 2041
snmp-server enable traps rmon
! The SFP Transceiver should be monitored for High/Low Alarms/Warnings by enabling
! the following trap. High or Low readings can indicate an SFP, HBA or cable issue.
snmp-server enable traps link cisco-xcvr-mon-status-chg
snmp-server enable traps link cieLinkDown
snmp-server enable traps link linkDown
end

```

```

config t

```

```
logging level snmpd 3
port-monitor enable
```

```
no port-monitor activate default
no port-monitor activate slowdrain
no port-monitor activate pmon_storage
no port-monitor name pmon_storage
```

```
port-monitor name pmon_storage
port-type access-port
```

```
monitor counter link-loss
monitor counter sync-loss
monitor counter signal-loss
monitor counter invalid-words
monitor counter invalid-crc
monitor counter tx-discards
monitor counter lr-rx
monitor counter lr-tx
monitor counter timeout-discards
monitor counter credit-loss-reco
monitor counter tx-credit-not-available
no monitor counter rx-datarate
no monitor counter tx-datarate
```

```
counter credit-loss-reco poll-interval 1 delta rising-threshold 1 event 4 falling-threshold 0 event 4
counter tx-credit-not-available poll-interval 1 delta rising-threshold 10 event 4 falling-threshold 0 event 4
```

```
counter link-loss poll-interval 60 delta rising-threshold 3 event 4 falling-threshold 0 event 4
counter sync-loss poll-interval 60 delta rising-threshold 3 event 4 falling-threshold 0 event 4
counter signal-loss poll-interval 60 delta rising-threshold 3 event 4 falling-threshold 0 event 4
counter invalid-crc poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4
counter invalid-words poll-interval 60 delta rising-threshold 10 event 4 falling-threshold 0 event 4
```

```
counter tx-discards poll-interval 60 delta rising-threshold 100 event 4 falling-threshold 10 event 4
counter lr-rx poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4
counter lr-tx poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4
counter timeout-discards poll-interval 60 delta rising-threshold 100 event 4 falling-threshold 10 event 4
```

```
exit
port-monitor activate pmon_storage
end
```

Result:

Policy Name : pmon_storage								
Admin status : Active								
Oper status : Active								
Port type : All Access Ports								
Counter	Threshold	Interval	Rising Threshold	event	Falling Threshold	event	PMON	Portguard
Link Loss	Delta	60	3	4	0	4	Not enabled	
Sync Loss	Delta	60	3	4	0	4	Not enabled	
Signal Loss	Delta	60	3	4	0	4	Not enabled	
Invalid Words	Delta	60	10	4	0	4	Not enabled	
Invalid CRC's	Delta	60	5	4	0	4	Not enabled	
TX Discards	Delta	60	100	4	10	4	Not enabled	
LR RX	Delta	60	5	4	0	4	Not enabled	
LR TX	Delta	60	5	4	0	4	Not enabled	
Timeout Discards	Delta	60	100	4	10	4	Not enabled	
Credit Loss Reco	Delta	1	1	4	0	4	Not enabled	
TX Credit Not Available	Delta	1	10	4	0	4	Not enabled	
RX Datarate	Delta	60	80%	4	50%	4	Not enabled	
TX Datarate	Delta	60	90%	4	50%	4	Not enabled	

17.2.3. Host Port Monitoring (Host Edge Switch)

Host ports will be monitored from the Host Edge switches. The following port-monitoring alerts will be enabled.

Note: Due to concerns with the number of alerts that might be generated, “Invalid Transmission Words”, “Tx-datarate” and “Rx-datarate” will not be monitored at this time.

Port Monitor Name: pmon_hosts

Commands:

```

config t
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO

snmp-server host FQDN-SRM-Server traps version 1 public udp-port 2041
snmp-server enable traps rmon
! The SFP Transceiver should be monitored for High/Low Alarms/Warnings by enabling
! the following trap. High or Low readings can indicate an SFP, HBA or cable issue.
snmp-server enable traps link cisco-xcvr-mon-status-chg
no snmp-server enable traps link cieLinkDown
no snmp-server enable traps link linkDown
end

config t
logging level snmpd 3
port-monitor enable

```

```
no port-monitor activate default
no port-monitor activate slowdrain
no port-monitor activate pmon_hosts
no port-monitor name pmon_hosts
```

```
port-monitor name pmon_hosts
port-type access-port
```

```
monitor counter link-loss
monitor counter sync-loss
monitor counter signal-loss
no monitor counter invalid-words
monitor counter invalid-crc
monitor counter tx-discards
monitor counter lr-rx
monitor counter lr-tx
monitor counter timeout-discards
monitor counter credit-loss-reco
monitor counter tx-credit-not-available
no monitor counter rx-datarate
no monitor counter tx-datarate
```

```
counter credit-loss-reco poll-interval 1 delta rising-threshold 1 event 4 falling-threshold 0 event 4
counter tx-credit-not-available poll-interval 1 delta rising-threshold 10 event 4 falling-threshold 0 event 4
```

```
counter link-loss poll-interval 60 delta rising-threshold 3 event 4 falling-threshold 0 event 4
counter sync-loss poll-interval 60 delta rising-threshold 3 event 4 falling-threshold 0 event 4
counter signal-loss poll-interval 60 delta rising-threshold 3 event 4 falling-threshold 0 event 4
counter invalid-crc poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4
```

```
counter tx-discards poll-interval 60 delta rising-threshold 100 event 4 falling-threshold 10 event 4
counter lr-rx poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4
counter lr-tx poll-interval 60 delta rising-threshold 5 event 4 falling-threshold 0 event 4
counter timeout-discards poll-interval 60 delta rising-threshold 100 event 4 falling-threshold 10 event 4
```

```
exit
port-monitor activate pmon_hosts
end
```

Result:

Policy Name : pmon_hosts								
Admin status : Active								
Oper status : Active								
Port type : All Access Ports								
Counter	Threshold	Interval	Rising Threshold	event	Falling Threshold	event	PMON	Portguard
Link Loss	Delta	60	3	4	0	4	Not enabled	
Sync Loss	Delta	60	3	4	0	4	Not enabled	
Signal Loss	Delta	60	3	4	0	4	Not enabled	
Invalid CRC's	Delta	60	5	4	0	4	Not enabled	
TX Discards	Delta	60	100	4	10	4	Not enabled	
LR RX	Delta	60	5	4	0	4	Not enabled	
LR TX	Delta	60	5	4	0	4	Not enabled	
Timeout Discards	Delta	60	100	4	10	4	Not enabled	
Credit Loss Reco	Delta	1	1	4	0	4	Not enabled	
TX Credit Not Available	Delta	1	10	4	0	4	Not enabled	

17.2.4. Troubleshooting Port Monitoring Alerts

Cisco has provided Citi with a document, [MDS – SFP and Port Monitoring](#), that covers the PMON settings, possible conditions and how to mitigate issues such as “Slow Drain”. The document is located on the CSBE Cisco webpage.

18. DCNM Web Client - Performance Manager

With DCNM Web Client, you can monitor Cisco MDS 9000 Family switch events, performance, inventory, and perform minor administrative tasks.

DCNM Web Client provides the following features:

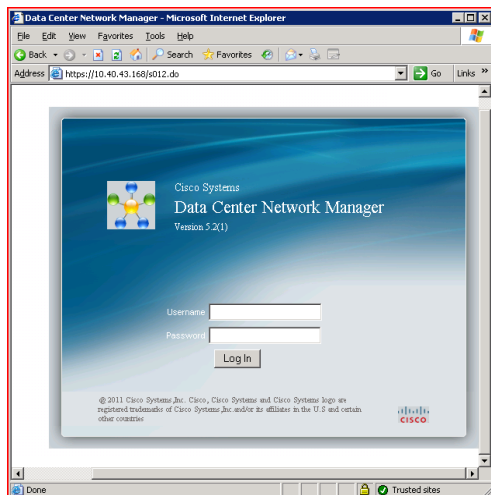
- **Summary Dashboard** - The summary dashboard provides a quick view of Inventory, Health, Daily Performance, Top Hosts, Top Storage, Federation and Topology in separate windows. It provides real-time monitoring of fabrics with visibility into traffic fluctuations and helps establish baseline traffic patterns. You can double-click the dashboard to expand a specific window for a more detailed view of individual network components.
- **Host Dashboard** - The host dashboard provides you all the information related to all the SAN hosts and virtual hosts that are discovered. The host dashboard provides very detailed information related to the network, such as I/O traffic, disk latency, CPU, memory statistics, topology, and events about each individual host and virtual machines that are configured on top of the virtual host. The host dashboard consists of four panels:
 - **Host panel** - Provides information about SAN hosts and the virtual hosts.
 - **Chart Panel** - Provides the I/O statistics, CPU and memory information, and disk latency of individual hosts or virtual machines.
 - **Topology Panel** - Provides end-to-end topology layout and path information between host enclosures and storage enclosures. The virtual machine topology view shows all of the dependencies from the virtual machine out to the physical host, through the fabric, and to the storage array with easy access to a detailed view of the path attributes.
 - **Event Panel** - Provides information about events of all of the switch ports that are configured with a specific host enclosure.
- **Summary and drill down reports** - The Performance Manager summary report provides a high-level view of your network performance. These reports list the average and peak throughput and provides hot-links to additional performance graphs and tables with additional statistics. Both tabular and graphical reports are available for all interconnections monitored by Performance Manager. Performance Manager also analyzes daily, weekly, monthly, and yearly trends. You can also view the results for specific time intervals using the interactive zooming functionality. These reports are only available if you create a collection using Performance Manager and start the collector. To view historical performance reports, you need to install Adobe Flash Player 10 or later.
- **Zero maintenance database for statistics storage** - No maintenance is required to maintain Performance Manager's round-robin database, because its size does not grow over time. At prescribed intervals the oldest samples are averaged (rolled-up) and saved. A full two days of raw samples are saved for maximum resolution. The resolution gradually is reduced as groups of the oldest samples are rolled up together.

18.1. Launching DCNM Web Client

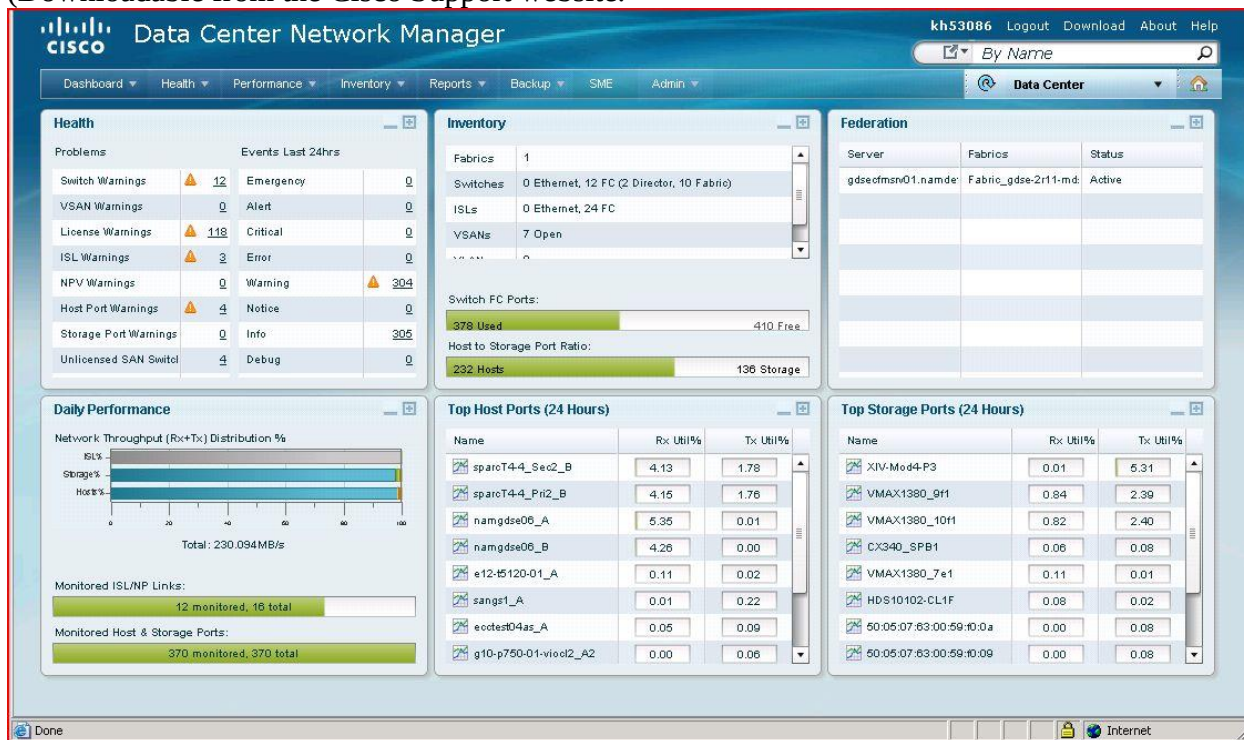
DCNM Web Client can be launched from an Internet Explorer Browser.

Enter: https://IP_Address_of_DCNM_Server

Login with your soeid and password (Active Directory).



You'll receive the DCNM Dashboard. From here, you can view performance and generate reports. More details on Performance can be found in the Cisco DCNM Fundamentals Guide, section 9. (Downloadable from the Cisco Support website.)



19. Firmware Upgrades/Downgrades

Operations should plan to deploy new releases of NX-OS for the MDS as soon as these are certified by GDSE. **Install/Upgrade the Data Center Network Manager software on the Management Server before upgrading NX-OS.** NX-OS is downloaded from the Cisco Support website using your CCO login account. The Firmware Upgrade wizard, available within DCNM, can then be used to *upgrade* or *downgrade* firmware. The wizard first transfers the image to the switch bootflash filesystem, and then initiates the upgrade. If a **CLI NX--OS upgrade** is preferred, see [Section 6.6](#) for instructions. (See [Release Notes](#) prior to upgrading).

With the increase in the number of MDS 9148 edge switches in the new SAN architecture, Cisco recommends using DCNM or CLI to pre-stage the NX-OS on the switches and running a verification a week or so prior to the actual upgrade date. This will shorten the install time, since DCNM won't need to download the NX-OS to the switches.

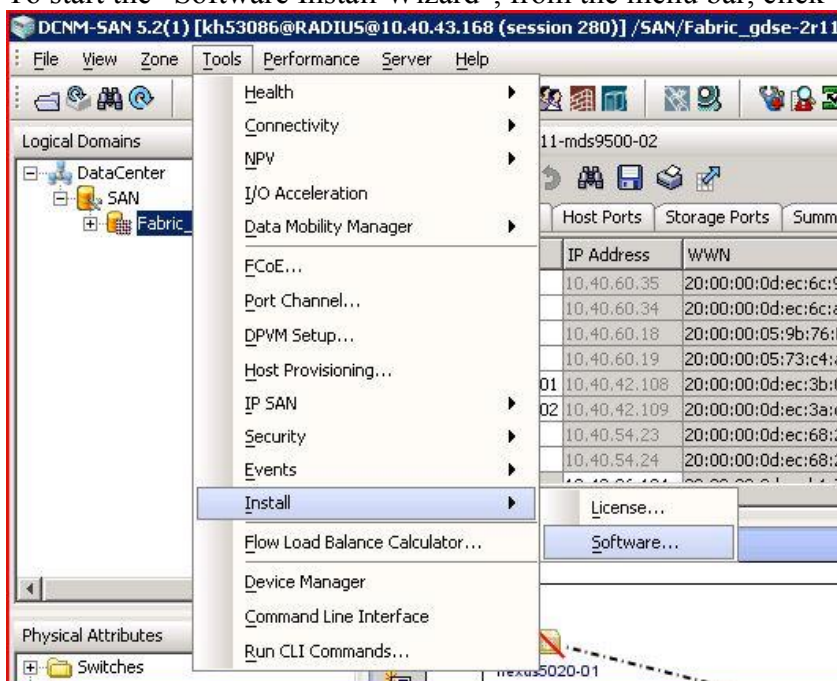
If the NX-OS files are pre-staged, Cisco recommends upgrading 20 switches at one time.

If the NX-OS files are NOT pre-staged, Cisco recommends upgrading only 10 switches at one time.

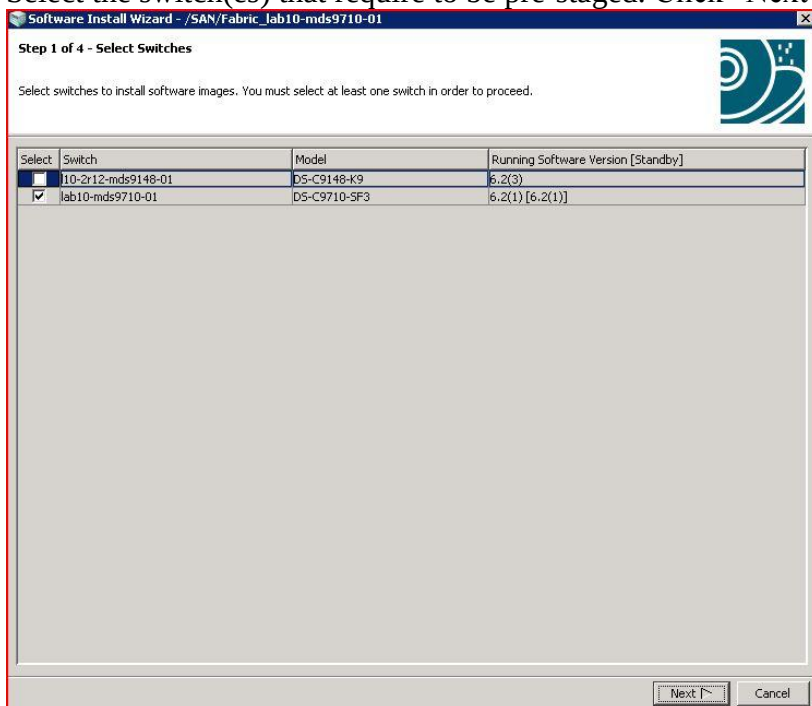
Although the firmware update process is non-disruptive, it should still be carried out in a green zone. All switches in a fabric should be upgraded together. There should be a gap of at least a week between Fabric A and Fabric B upgrade. If issues are observed when the first fabric is upgraded, it should be downgraded to the previous version and CSBE and vendor should be notified.

19.1. Pre-Stage NX-OS files via DCNM

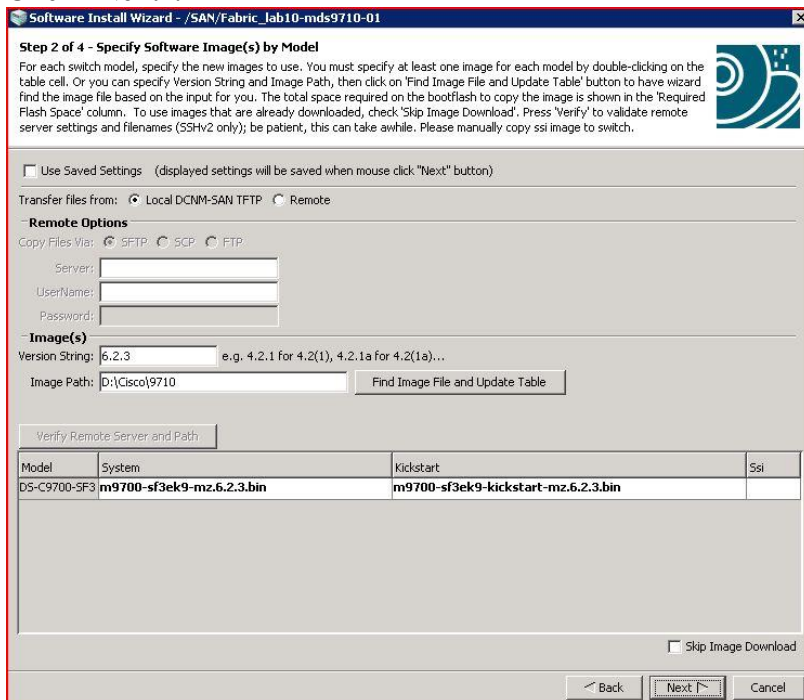
1. To start the “Software Install Wizard”, from the menu bar, click “Tools/Install/Software”.



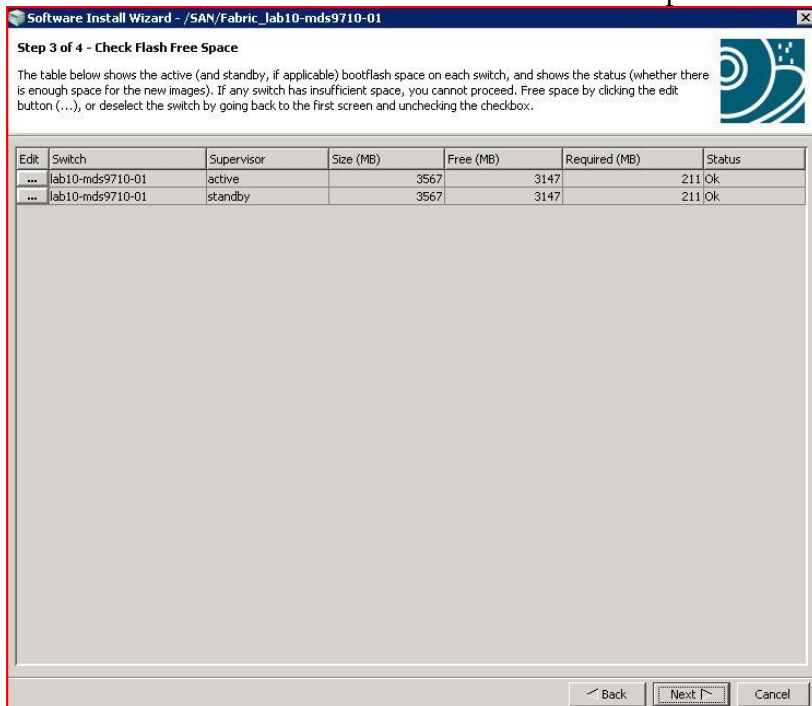
2. Select the switch(es) that require to be pre-staged. Click “Next”.



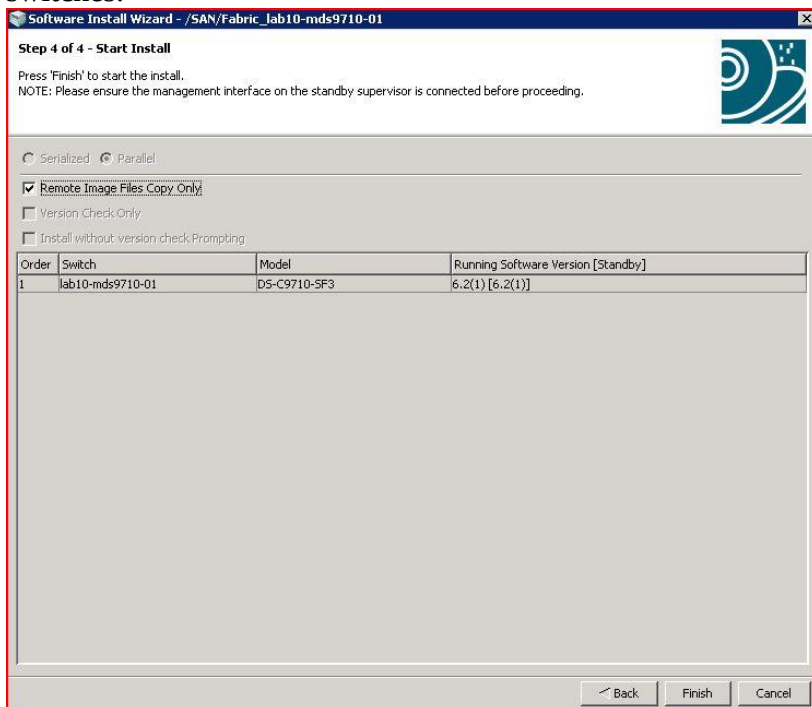
3. Click on the “Local DCNM-SAN TFTP” radio button.
Enter the Image Version String (ex: 6.2.x).
Enter the Image Path: location of the System and Kickstart binary file.
Click “Find Image File and Update Table” button.
The wizard will locate the firmware files and populate the names into the dialog box.
Click “Next”.



4. Software Install Wizard verifies there is sufficient space in bootflash.



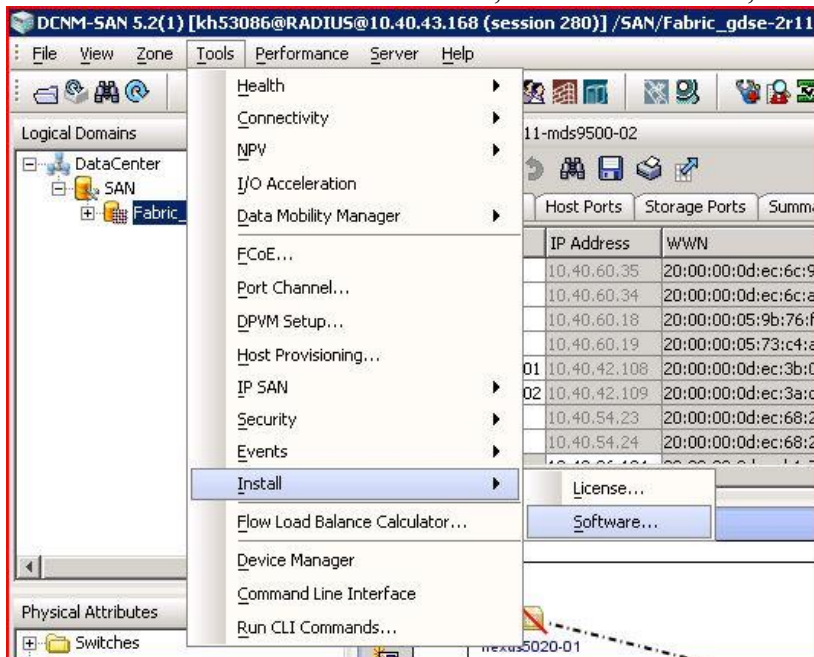
5. Select “Remote Image Files Copy Only”. Click Finish to copy the install files in parallel to the switches.



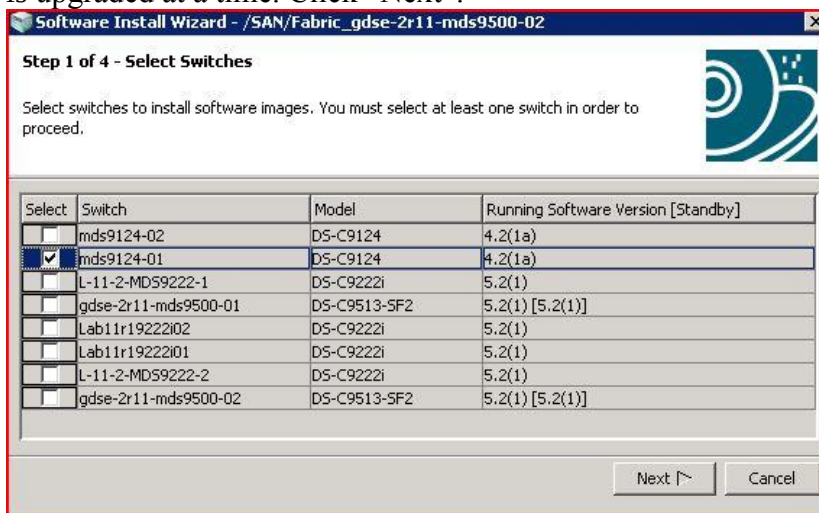
19.2. Software (Firmware) Install Wizard

This procedure is based on the NX-OS files being pre-staged on the switches to be upgraded.

1. To start the “Software Install Wizard”, from the menu bar, click “Tools/Install/Software”.



2. Select the switch(es) that require an upgrade. If multiple switches are selected, only one switch is upgraded at a time. Click “Next”.



3. Click on the “Local DCNM-SAN TFTP” radio button.
Enter the Image Version String (ex: 6.2.3).
Enter the Image Path: location of the System and Kickstart binary file.
Click “Find Image File and Update Table” button.
Click “Skip Image Download” in the bottom right of the dialog box.
The wizard will locate the firmware files and populate the names into the dialog box.

Click “Next”.

Software Install Wizard - /SAN/Fabric_lab10-mds9710-01

Step 2 of 4 - Specify Software Image(s) by Model

For each switch model, specify the new images to use. You must specify at least one image for each model by double-clicking on the table cell. Or you can specify Version String and Image Path, then click on 'Find Image File and Update Table' button to have wizard find the image file based on the input for you. The total space required on the bootflash to copy the image is shown in the 'Required Flash Space' column. To use images that are already downloaded, check 'Skip Image Download'. Press 'Verify' to validate remote server settings and filenames (SSHv2 only); be patient, this can take awhile. Please manually copy ssi image to switch.

☐ Use Saved Settings (displayed settings will be saved when mouse click "Next" button)

Transfer files from: ☒ Local DCNM-SAN TFTP ☐ Remote

Remote Options

Copy Files Via: ☒ SFTP ☐ SCP ☐ FTP

Server:

UserName:

Password:

Image(s)

Version String: e.g. 4.2.1 for 4.2(1), 4.2.1a for 4.2(1a)...

Image Path:

Model	System	Kickstart	Ssi
DS-C9700-SF3	m9700-sf3ek9-mz.6.2.3.bin	m9700-sf3ek9-kickstart-mz.6.2.3.bin	

☒ Skip Image Download

4. Double click the space under “System” to list the firmware files in bootflash. Do the same for the “Kickstart” files. Click Next.

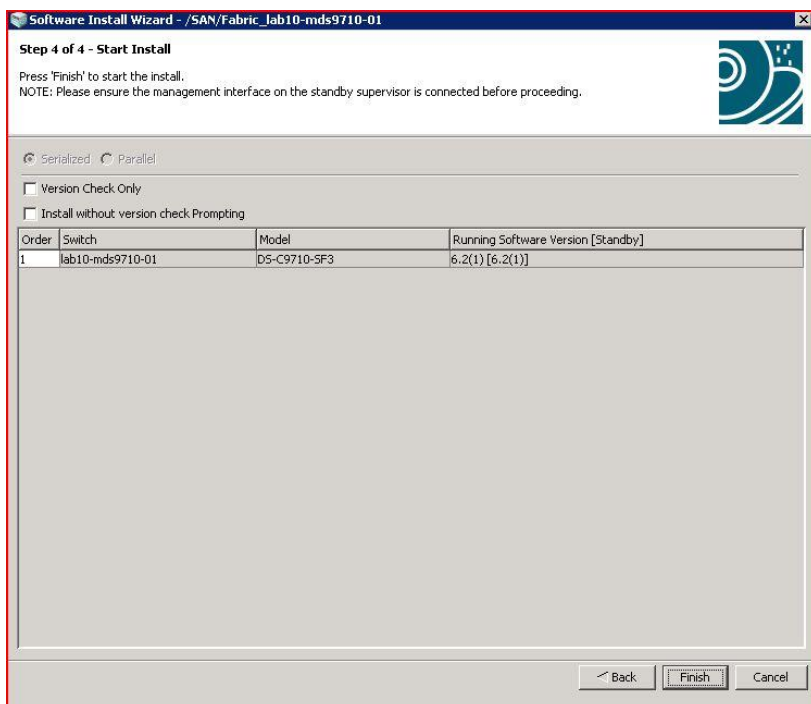
Software Install Wizard - /SAN/Fabric_lab10-mds9710-01

Step 3 of 4 - Select Downloaded Images

For each switch, select images from the bootflash to use for the install. You must select at least one image for each switch. Double-click on the table cell to choose an image.

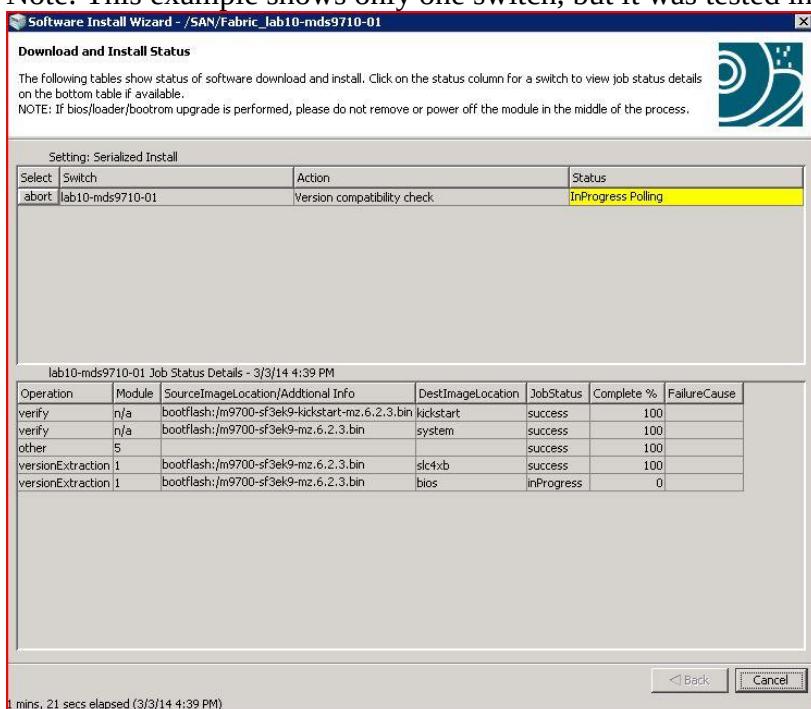
Switch	System	Kickstart	Ssi
lab10-mds9710-01			

5. If version checking was done during the pre-stage process, then you can check the box “Install without version check prompting”. Without checking the version, you can select a “Parallel” install. Otherwise, the upgrades are serial and will take longer, waiting for one complete before moving to the next switch to upgrade. Click Finish

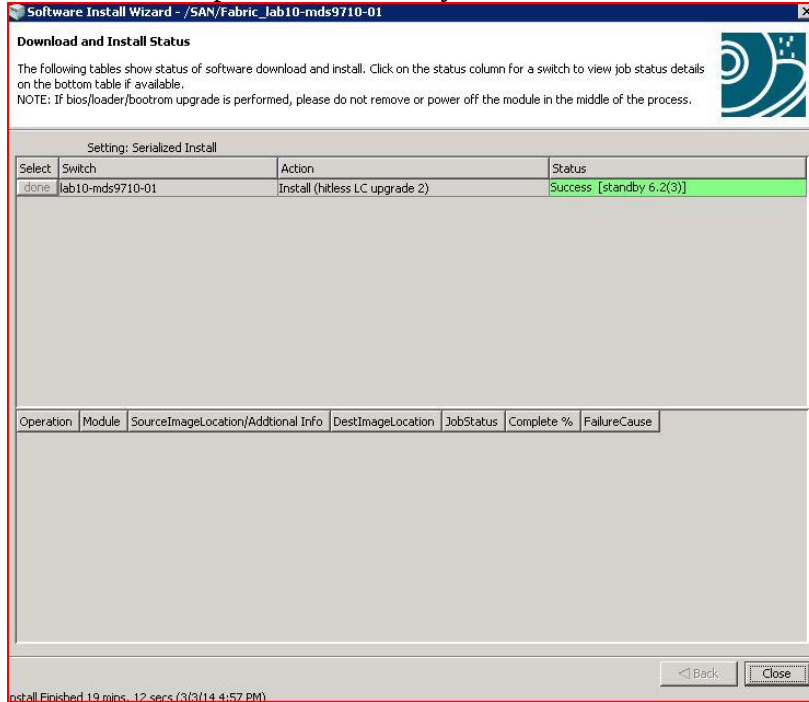


6. The installation begins.

Note: This example shows only one switch, but it was tested in the Cisco lab with 20 switches.



7. Installation completed successfully.



20. New Licensing Model for DCNM 6.3.x

Licensing allows you to access specified premium features on the switch after you install the appropriate license for that feature. A significant change for Cisco DCNM-SAN, as compared to Cisco Fabric Manager, is that licenses are no longer hosted on a specific switch. Instead, the licenses are hosted on the Cisco DCNM-SAN server. All existing Cisco Fabric Manager licenses are grandfathered into this model (which means that they continue) so customers do not need to order or deploy any additional licenses to manage their existing Cisco MDS 9000 Family switches.

- DCNM for SAN supports both switch embedded and server based licensing.
- Switch embedded licensing is when the license is attached to the serial number of the chassis (this is what is in place today).
- Server based licensing is a license that is mapped to the **MAC address of the management server**. This is the new licensing model going forward.
- If you have upgraded to Cisco DCNM, your newly purchased switch licenses will move to a license pool file that will reside on the Cisco DCNM for SAN server.
- Your existing Cisco Fabric Manager licenses will still be discovered on the switches with Cisco DCNM for SAN. Essentially, Cisco will be supporting two license models for environments with Cisco Fabric Manager.
- For customers who have upgraded from Cisco FMS to Cisco DCNM for SAN and purchased additional switches, the license pool model will apply.
- The Server based model maintains a single pool of licenses for all switches. Licenses are mapped to switch chassis and MAC address of the management server.
- Any changes to the MAC address of the management server will require a rehome of all of the licenses in the pool requiring customers to keep track of all **sales orders and PAK certificates**. Changing MAC address will disable the Advanced Edition features on both LAN and SAN versions. This does not mean you won't be able to manage your switches, it just means that any of the features that you use with the Advanced Edition are disabled until the licenses are rehomed.
- With MAC licensing, customers will no longer be able to discover the same fabric with two independent management servers since the license is tied down to the MAC address.
- For switch migrations, the license will carry over to the same series chassis with Server Based License model. Customer will retain license for the lifetime of the chassis type until Cisco EOLs the chassis.

Benefit:

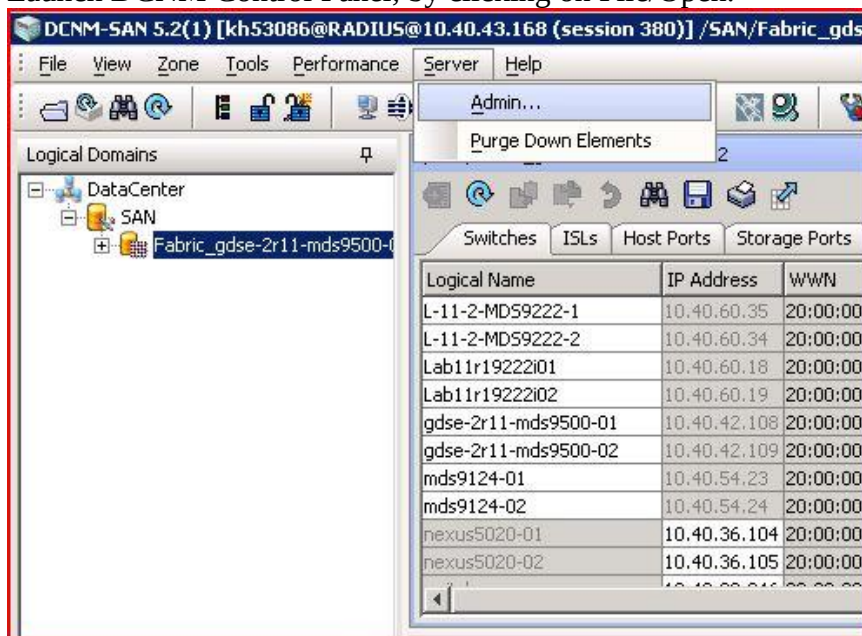
Ability to retain licenses is a great financial benefit, resulting in significant cost savings. The Customer won't have to buy a new license when replacing an older switch with the same series switch (i.e. migration from MDS 9506 to MDS 9513).

Platform	Electronic Part Number	Physical Part Numbers	Chassis Part Numbers
DCNM for SAN Advanced Edition for MDS 9100	L-DCNM-S-M91-K9=	DCNM-SAN-M91-K9=	DCNM-SAN-M91-K9
DCNM for SAN Advanced Edition for MDS 9200	L-DCNM-S-M92-K9=	DCNM-SAN-M92-K9=	DCNM-SAN-M92-K9
DCNM for SAN Advanced Edition for MDS 9500	L-DCNM-S-M95-K9=	DCNM-SAN-M95-K9=	DCNM-SAN-M95-K9
DCNM for SAN Advanced Edition for MDS 9700	L-DCNM-S-M97-K9=	DCNM-SAN-M97-K9=	DCNM-SAN-M97-K9

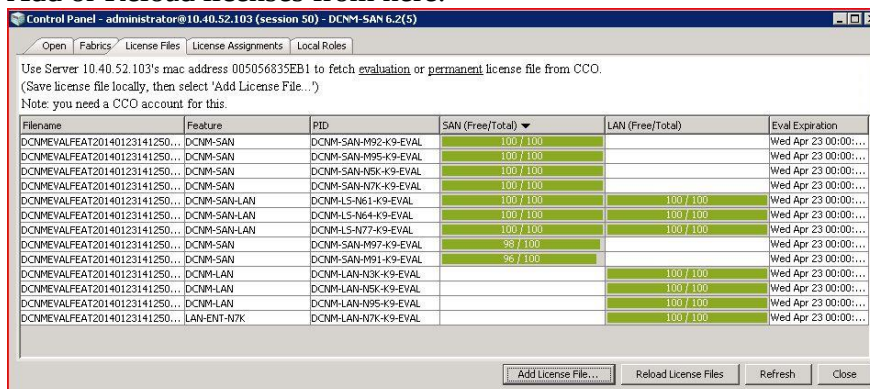
20.1. Installing Licenses for Newly Purchased Switches

Note: There is a very good “YouTube” video on obtaining a new license from Cisco and how to apply it in Data Center Network Manager (<http://www.youtube.com/watch?v=QqoZ7jTP5nk>).

1. Obtain license file (.lic) from Cisco website.
You'll need the **PAK information** and the **MAC address** of the DCNM Server.
2. Copy License file to DCNM Server directory:
C:\Program Files\Cisco Systems\dcm\licenses
3. Launch DCNM Control Panel, by clicking on File/Open.



4. Click on “**License Files**” tab.
Add or Reload licenses from here.



21. Known Issues and Bug Fixes

See the latest Release Notes on our Cisco web page for known issues and fixes to bugs.

22. Security Review Findings

After going through the SAA process, the following sections outline the Opened and Closed security findings for DCNM Client and DCNM Performance Manager web interface. There are only two NCI (Non Compliant Issues), M1 and M6. They are covered by RE #502667. These issues are listed in the SAA NCI document at the following URL: [SAA NCI Document](#), and a GAP resolution along with timeframes is listed in the NCI GAP Resolution plan at the following URL: [NCI GAP Resolution Plan](#) on the tab marked 3-plan. As the issues are resolved in future releases, they will be removed from this document.

22.1. Data Center Network Manager Findings (Open)

There are no open security findings.

22.2. Data Center Network Manager Findings (Closed)

These security finding(s) for DCNM are closed. **Any required updates to the configuration are noted.**

22.2.1. APP135 (N2) - PostgreSQL

Postgres database authentication uses unencrypted connection.

Vendor Response: Configure the PostgreSQL database with the loopback address (127.0.0.1), preventing outside connections to the database.

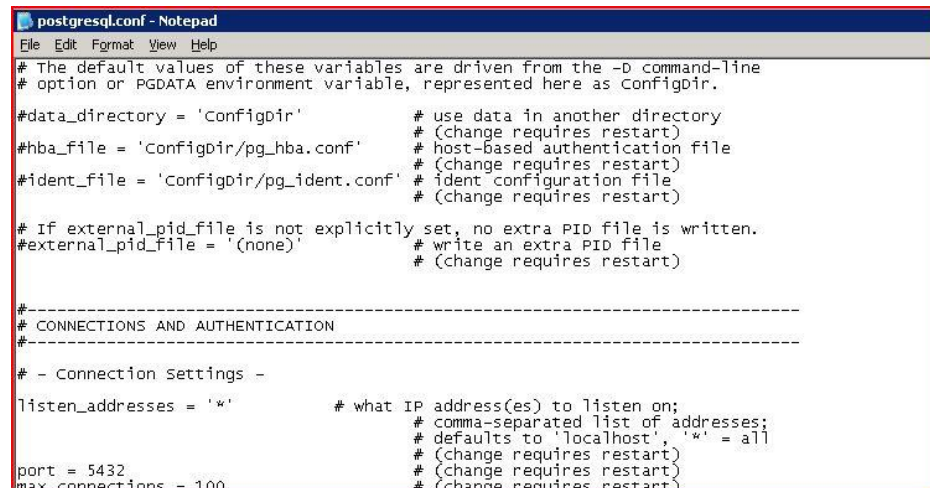
With WordPad, edit C:\Program Files\Cisco Systems\dcm\db\data "postgresql.conf".

Under # CONNECTIONS AND AUTHENTICATION

Change the listen_addresses parameter from an "*" to "127.0.0.1".

Reboot the DCNM Server.

Before:



```

# postgresql.conf - Notepad
File Edit Format View Help
# The default values of these variables are driven from the -D command-line
# option or PGDATA environment variable, represented here as ConfigDir.

#data_directory = 'ConfigDir'           # use data in another directory
#                                     # (change requires restart)
#hba_file = 'ConfigDir/pg_hba.conf'     # host-based authentication file
#                                     # (change requires restart)
#ident_file = 'ConfigDir/pg_ident.conf' # ident configuration file
#                                     # (change requires restart)

# If external_pid_file is not explicitly set, no extra PID file is written.
#external_pid_file = '(none)'           # write an extra PID file
#                                     # (change requires restart)

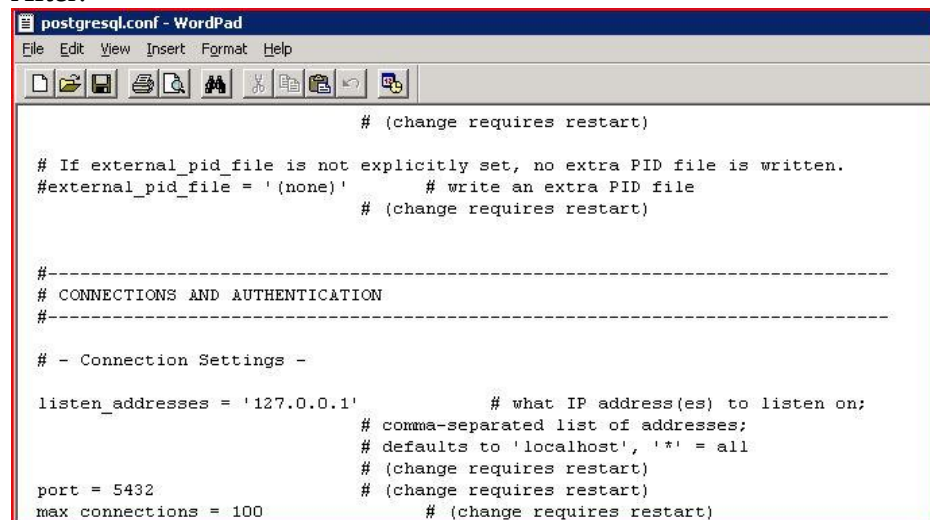
#-----
# CONNECTIONS AND AUTHENTICATION
#-----

# - Connection Settings -

listen_addresses = '*'                  # what IP address(es) to listen on;
#                                     # comma-separated list of addresses;
#                                     # defaults to 'localhost', '*' = all
#                                     # (change requires restart)
port = 5432                            # (change requires restart)
max_connections = 100                  # (change requires restart)

```

After:



```
# (change requires restart)
# If external_pid_file is not explicitly set, no extra PID file is written.
#external_pid_file = '(none)'          # write an extra PID file
#                                     # (change requires restart)

#-----
# CONNECTIONS AND AUTHENTICATION
#-----

# - Connection Settings -

listen_addresses = '127.0.0.1'          # what IP address(es) to listen on;
#                                     # comma-separated list of addresses;
#                                     # defaults to 'localhost', '*' = all
#                                     # (change requires restart)
port = 5432                            # (change requires restart)
max_connections = 100                  # (change requires restart)
```

Security Response: Configuring PostgreSQL to only listen on the loopback address (127.0.0.1) prevents any connections outside the server. Issue remediated and **CLOSED**.

22.3. DCNM Performance Manager Findings (Open)

These security findings for the Performance Manager Web interface are open and being tracked by a Cisco Tracking number. **Only M1 and M3 are on the Risk Exception.** The other Open findings were lowered to LOW.

22.3.1. LOW - APP042 and CVA0034 (H4) – File and Directory Protection

Server Path Disclosure

The web server may reveal the physical paths of directories and other confidential information on the server (<https://10.40.43.168/goHome.do>).

This file is world accessible. It contains confidential information that can lead to several server attacks if obtained by an attacker. It is recommended that this file be removed or limited to local scope (i.e. access should be limited to requests originating from IP address 127.0.0.1).

Vendor Response: Fixed in DCNM 6.2.1. Tracking number: CscuD29739

Update: 03/18/2014. This item is fixed in DCNM 6.3.1 (current certified DCNM version). CSBE will request a CIVA scan to verify whether it is still a security risk in DCNM 6.3.1.

Security Response: Finding was lowered to low because this is “post-auth” and the only users able to login already have admin access to the server and everything at the path location anyway. Lowered to **LOW**

22.3.2. CVA0077 (M1) – Browser Auto-complete

Browser Auto-complete enabled before authentication

Form fields before authentication in the application have auto-complete enabled. Any user using the same computer would be able to see information entered by a previous user.

By not setting AutoComplete to OFF the user can purposely or accidentally save sensitive information to their account into Browser Memory Space. This gives the ability for a malicious attacker to dump the clear text from memory and gain access to sensitive information.

Vendor Response: Cisco has submitted an enhancement for this security finding and it should be fixed in DCNM 6.2.1. It is being tracked under Tracking Number: CSCuD65294

Update: 03/18/2014. This item is fixed in DCNM 6.3.1 (current certified DCNM version). CSBE will request a CIVA scan to verify whether it is still a security risk in DCNM 6.3.1.

Security Response: Security finding will be included in the **RE (Risk Exception)**.

Update: 01/26/2015: CIVA scan completed and RE closed.

22.3.3. CVA0204 (M3) – Sensitive Information

Sensitive Information Obtained

Sensitive information was found in one of the following:

- Descriptive error message
- Application unexpected behavior
- Unwanted file types (e.q .template, .CAB, .DLL) were obtainable via unauthenticated download

Do not display any sensitive information in the error message, and protect any unwanted file types from being downloaded.

Vendor Response: Cisco has submitted an enhancement for this security finding and it should be fixed in DCNM 6.2.1. It is being tracked under Tracking Number: CSCue14206.

Update: 03/18/2014. DCNM 6.3.1 is based on jboss AS 7.2 (a 3rd party software), which addressed a significant number of security issues. Cisco cannot modify jboss and has closed the bug tracking number CSCue14206. CSBE will request a CIVA scan to verify whether it is still a security risk in DCNM 6.3.1.

Security Response: Security finding will be included in the **RE (Risk Exception)**.

Update: 01/26/2015: CIVA scan completed and RE closed.

22.3.4. LOW - CVA0052 (M4) – Forceful Browsing

Forceful Browsing / XML Information Gathering

An attacker may use this information to understand the logic behind the web application, or extract vital information from it.

Improper permission set to /WEB-INF directory.

Change the permissions of the /WEB-INF directory, so it cannot be viewed by all web users.

Vendor Response: Access to this directory by users is required for the application to work properly. Only users able to login already have admin access to the server and everything at the path location anyway.

Security Response: Finding lowered because this functionality must be exposed for the software to function correctly. Also software is located on a server with limited access. Lowered to **LOW**

22.3.5. LOW - CVA0029 (M6) – Cache

Cache – POST Request Returns 200 OK Server Response

The application does not prevent caching of confidential information. Upon submitting a form, it is possible to hit the back button in the browser, then the refresh button to view the information that was submitted.

Pages, which accept confidential information from users, should not allow the browser to cache information. In order to avoid this type of issue, please follow these recommendations:

If a form posts sensitive data through a POST request, the server should return a 302 "Object Moved" response, to re-direct users to a different page. This avoids caching sensitive information.

Vendor Response: Other sites, including Citi Bank perform in this same manner.

Security Response: This finding risk was lowered based on a variety of things and mitigating factors.

- 1.) CAVA no longer rates this risk as highly
- 2.) The network this software will run on is isolated making it harder for someone to use this method to gain access. Lowered to **LOW**

22.3.6. CVA2503 (L1) – SSL Signed Certificate

SSL Certificate Signed Using Weak Hashing Algorithm

The remote service uses an SSL certificate that has been signed using a cryptographically weak hashing algorithm - MD2, MD4, or MD5. These algorithms are known to be vulnerable to collision attacks. In theory, a determined attacker may be able to leverage this weakness to generate another certificate with the same digital signature, which could allow him to masquerade as the affected service.

Vendor Response: Citi issue.

Security Response: Engage Citi ENTRUST team (Certificate Authority) to have a Citi SSL Certificate created and installed.

Entrust Engineering DL

[*CATE Global Security Data Protection Engineering](#)

22.4. DCNM Performance Manager Findings (Closed)

These security findings were remediated and closed based on changes to the configuration.

Any required updates to the configuration are noted.

22.4.1. APP035 and CVA0106 (H6) – Authorization / Access Control / Entitlement

Authorization based on cookie/parameter values, not the session ID

Access control or authorization based upon parameter values may lead to impersonation or privilege escalation by manipulating the cookie/parameter values. The application does not use sessions for keeping track, instead, the credentials are resent every time via SOAP.

Avoid the use of client-side cookie/parameter values for tracking user session identity and access role information where it is easily manipulated. Instead, track the information using server-side techniques.

Vendor Response: The SOAP token is not text, or a name, etc, but a long random string. The Token is not stored locally in the browser, it is being sent thru an encrypted channel. It has nothing to do with the browser, it's part of the FlexWeb framework.

Security Response: The token appears to be some sort of binary data and is not a cleartext password. This appears likely to be binary data passed by the framework.
Finding has been **CLOSED**.

22.4.2. APP118 and CVA0035 (M5) – Session Identifier Passage

Encryption – Weak Encryption

The Web server accepts low-grade encryption and the minimum acceptable key size is 128 bits. If a user's browser negotiates such a weak protocol, the whole communication can potentially be compromised by a cryptanalytic attack. Keys less than 128-bits are not approved by the ISLC. If the site must accept less than 128-bit encryption, please implement a step up certificate.

Disable low-grade encryption and force the use of 128-bit encryption to ensure that the session is protected.

Vendor Response: Using WordPad edit **server.xml** in Directory:
C:\Program Files\Cisco Systems\dcn\jboss-4.2.2.GA\server\fm\deploy\jboss-web.deployer

Remove the following line:

sslProtocol="TLS"

Add the following line:

```
sslProtocol="SSLv3"
ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA"
```

Before:

```
<!-- SSL/TLS Connector configuration using the admin dev1 guide keystore -->
<Connector port="443"
    protocol="HTTP/1.1" SSLEnabled="true"
    maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
    emptySessionPath="true"
    server="Apache"
    scheme="https" secure="true" clientAuth="false" sslProtocol = "TLS"
    securityDomain="java:/jaas/encrypt-keystore-password"
    SSLImplementation="org.jboss.net.ssl.JBossImplementation" allowTrace="false"/>
```

After:

```
<!-- SSL/TLS Connector configuration using the admin dev1 guide keystore -->
<Connector port="443"
    protocol="HTTP/1.1" SSLEnabled="true"
    maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
    emptySessionPath="true"
    server="Apache"
    scheme="https" secure="true" clientAuth="false" sslProtocol = "SSLv3"
    ciphers="TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_W
    securityDomain="java:/jaas/encrypt-keystore-password"
    SSLImplementation="org.jboss.net.ssl.JBossImplementation" allowTrace="false"/>
```

Update: 03/18/2014. DCNM 6.3.1 is based on jboss AS 7.2 (a 3rd party software), which addressed a significant number of security issues. These settings are not modifiable in this version of jboss. CSBE will request a CIVA scan to verify whether it is still a security risk in DCNM 6.3.1.

Security Response: Issue was retested after the above fix. Only strong ciphers can be negotiated now. Finding has been **CLOSED**.

22.4.3. APP122 and CVA0274 (M7) – Secure Cookies

Modification still required?

Flash parameter AllowScriptAccess set to "always"

It is possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user.

The flash player accepts object parameters such as AllowScriptAccess. The AllowScriptAccess parameter is used when a parent SWF loads a child SWF and determines whether the loaded SWF will have the same script access to the web page as the loading SWF. If the parameter is set to 'always' any SWF loaded by the parent from any domain could inject a script into the hosting web page.

Vendor Response: The crossdomain.xml file can be modified to correct this security finding. The "<allow-access-from domain=""*"" parameter in the crossdomain.xml file can be changed to a Citi domain. Changing this parameter does not affect DCNM operations.

Instructions:

On each DCNM server, go to

C:\Program Files\Cisco Systems\dcm\jboss-4.2.2.GA\server\fm\deploy\dcm.ear

Use WinZip to open dcm.war

Note: You may have to copy the dcm.war file to your desktop and open it via WinZip). After editing, copy dcm.war back to DCNM server directory above.

Name	Size	Type	Modified	Attribut
corner4.gif	374 B	GIF Image	8/31/2006 12:39 PM	
cperccll.html	2,429 B	HTML Document	8/6/2007 5:00 PM	
cprefs.html	2,429 B	HTML Document	8/6/2007 5:00 PM	
cpu.png	698 B	PNG Image	7/16/2011 4:23 PM	
cpu.png	399 B	PNG Image	7/16/2011 4:23 PM	
cpu.png	698 B	PNG Image	7/16/2011 4:23 PM	
cpu.png	399 B	PNG Image	7/16/2011 4:23 PM	
create.gif	600 B	GIF Image	7/16/2011 4:23 PM	
create.gif	600 B	GIF Image	7/16/2011 4:23 PM	
create.gif	600 B	GIF Image	7/16/2011 4:23 PM	
create.gif	600 B	GIF Image	7/16/2011 4:23 PM	
CreateCollection.jsp.class	25 KB	CLASS File	7/16/2011 4:24 PM	
Credentials.class	3,707 B	CLASS File	7/16/2011 4:24 PM	
crossdomain.xml	452 B	XML Document	7/16/2011 4:22 PM	
crossdomain.xml	452 B	XML Document	7/16/2011 4:23 PM	
csched.html	2,429 B	HTML Document	8/6/2007 5:00 PM	
csrf.js	2,508 B	JScript Script File	7/16/2011 4:16 PM	
csrf.js	2,508 B	JScript Script File	7/16/2011 4:24 PM	
csrfguard.properties	530 B	PROPERTIES File	7/16/2011 4:17 PM	
CsrfWarning.class	1,015 B	CLASS File	7/16/2011 4:24 PM	

Right click on **each** crossdomain.xml file and select Open with WordPad (edit both crossdomain files).

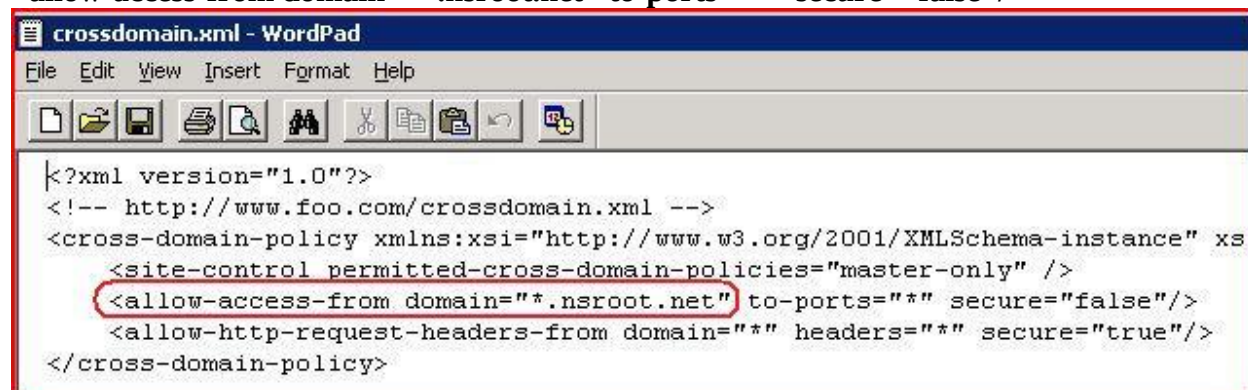
Remove:

<allow-access-from domain=""*"" to-ports=""*"" secure=""false""/>

Add:

Add (Domains required for your region):

<allow-access-from domain=""*.nsroot.net"" to-ports=""*"" secure=""false""/>



```

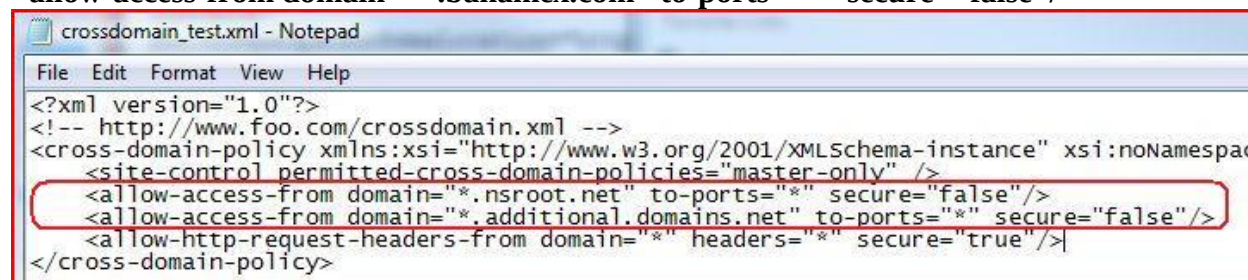
<?xml version="1.0"?>
<!-- http://www.foo.com/crossdomain.xml -->
<cross-domain-policy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.adobe.com/2004/07/cross-domain-policy/cross-domain-policy.xsd">
  <site-control permitted-cross-domain-policies="master-only" />
  <allow-access-from domain="*.nsroot.net" to-ports="*" secure="false"/>
  <allow-http-request-headers-from domain="*" headers="*" secure="true"/>
</cross-domain-policy>

```

If you have more than one domain accessing your HTTP DCNM Performance Manager, then you can add additional lines for them.

Example:

```
<allow-access-from domain="*.banamex.com" to-ports="*" secure="false"/>
```



Click File, then Save (use the default save location)

WinZip will modify the zipped file.

Update: 03/18/2014. DCNM 6.3.1 is based on jboss AS 7.2 (a 3rd party software), which addressed a significant number of security issues. These settings are not modifiable in this version of jboss. CSBE will request a CIVA scan to verify whether it is still a security risk in DCNM 6.3.1.

Security Response: Issue was retested after the above fix. Changing the “*” any to a Citi domain fixes this security finding. Finding has been **CLOSED**.

Update: 01/26/2015: CIVA scan completed. Issue fixed in DCNM 6.3.2.

22.4.4. CVA0286 (M2) – CrossFrame Scripting

Cross Frame Scripting – version 2 (XFSv2)

Pages on the application are allowed to be captured within a frame from another server. This can be exploited by attackers by sending a forged link to a user. The link will be to a malicious page with this application captured in a frame. All activity by the user can be monitored and recorded by the attacker allowing the compromise of the username, password, or any other sensitive input the user enters.

Earlier versions of Cross Frame scripting could be prevented by a frame busting script like the following. However, the new variations of the finding are able to frame the page even when the following fix is applied making the following script insufficient.

```
<script LANGUAGE="JAVASCRIPT">
```

```
if(top != self)
```

```
{
```

```
top.location=self.location;
```

```
}
```

```
</script>
```

A page vulnerable to XFSv2 also leads to other vulnerabilities such as clickjacking. Clickjacking takes the form of embedded code or script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function.

Please ensure all pages that gather user information prior to and during authentication are not vulnerable. The pages must prevent being encapsulated within a frameset of an unauthorized site.

Vendor Response: Cisco provided the following configuration modification to correct this issue.

From DCNM Performance Manager

Go to the **Admin** tab, under **General**, select **Server Properties**

Under the **WEB SECURITY** section, modify the web.enableCSRFGuard parameter:
web.enableCSRFGuard=true (Change from false to true)



```
#  
# WEB SECURITY  
#  
# Enable CSRF Guard to secure web server in untrusted environments:  
web.enableCSRFGuard true
```

Scroll to the bottom and select **Apply**.

Security Response: Issue was retested after the above fix. Setting the **web.enableCSRFGuard** to “true” fixed this security finding. Finding has been **CLOSED**.

23. Appendix A: Parts List for Cisco MDS Switches

Description	Cisco Part #	EMC Part #	HDS Part #
MDS 9710 Chassis	DS-9710	MDS-9710	DS-C9710-1K9.P
48 port 16Gb FC module	DS-X9448-768K9	MDS-48P-16GFC	DS-X9448768B8K9=.P
Supervisor 1	DS-X97-SF1-K9		(2) included in chassis part#
Fab 1 module	DS-X9710-FAB1		(3) included in chassis part#
MDS 9700 3000W AC power supply	DS-CAC97-3KW	MDS-9710-PS	(6) included in chassis part#
250VAC 20A NEMA, 6-20 Plug, USA			
250VAC 20A NEMA L6-20 Twist Lock Plug, USA			
250VAC 16A CEE 7/7 Plug, EU			
250VAC 16A IEC 309 Plug, International			
250VAC 16A, Src Plug EL224-C19, Brazil			
250VAC 16A, Src Plug IR2073-C19, Argentina			
MDS 9148 48-port switch with 48 active ports	DS-C9148-48p-K9	MDS-9148-48	DS-C9148-48P-K9.P
MDS 9148s 48-port switch with 12 port licenses	DS-C9148S-12PK9	MDS-9148S-12	DS-C9148S-12PK9
MDS 9148s – additional 12 port license (3 – required)	M9148S-PL12E=	MDS-9148S-POD	M9148S-PL12E=.P
MDS 9222i 18-port FC, 4-port GE Modular Switch	DS-C9222i-K9	MDS-9222i	
MDS 9506 Bundle *	DS-C9506-2K9	MDS-9506-V2	DS-C9506-2K9.P
MDS 9513 Bundle *	DS-C9513-2K9	MDS-9513	DS-C9513-2K9=
32 port 8Gb Adv FC module	DS-X9232-256K9	MDS-PBF-32ADV	DS-X9232-256K9.P
48 port 8Gb Adv FC module	DS-X9248-256K9	MDS-PBF-48ADV	DS-X9248-256K9.P
16-port Storage Services Node	DS-X9316-SSNK9	MDS-SSN-16	DS-X9316-SSNK9
18/4 Multiservice module	DS-X9304-18K9	MDS-PBFI-1804	DS-X9304-18K9.P
Fabric 3 module	DS-13SLT-FAB3	MDS-9513-FAB3	DS-13SLT-FAB3.P
8 Gbps SW SFP (LC)	DS-SFP-FC8G-SW	MDS-8G-SW	DS-SFP-FC8G-SW.P
8 Gbps LW SFP (LC)	DS-SFP-FC8G-LW	MDS-8G-LW	N/A
16 Gbps SW SFP (LC)	DS-SFP-FC16G-SW	DS-SFP-16GSW	DS-SFP-FC16G-SW.P
16 Gbps LW SFP (LC)	DS-SFP-FC16G-LW	DS-SFP-16GLW	DS-SFP-FC16G-LW.P
250VAC 20A NEMA 6-20	CAB-1900W-US1	MDS-PW19-US	CAB-1900W-US1=.P
250VAC 20A NEMA L6-20 Twist Lock	CAB-1900W-US2	MDS-PW19-TWST	CAB-1900W-US2=.P
FMS License	M9500FMS1K9	MDS-FMS-9500	M9500FMS1K9.P
FCIP license 18/4 module	M9500EXT1AK9	MDS-FCIP95-4	M9500EXT1AK9.P
DCNM for SAN Advanced Edition for MDS 9100	DCNM-SAN-M91-K9=	MDS-DCNM-91	L-DCNM-S-M91-K9=.P
DCNM for SAN Advanced Edition for MDS 9200	DCNM-SAN-M92-K9=	MDS-DCNM-92	L-DCNM-S-M92-K9=.P
DCNM for SAN Advanced Edition for MDS 9500	DCNM-SAN-M95-K9=	MDS-DCNM-95	L-DCNM-S-M95-K9=.P

DCNM for SAN Advanced Edition for MDS 9700	DCNM-SAN-M97-K9=	MDS-DCNM-97	L-DCNM-S-M97-K9=.P
---	------------------	-------------	--------------------

** Power Cords come in quantities of 2

NOTE:

- When ordering MDS 9148 or 9148s switches, order one or two extra for SPARE. These should be racked and configured with IP, default gateway and initial admin ID and password. In case of a failure, we'll have a replacement switch readily available to replace and restore to.
- MDS 9148s switches are sold with only 12 activated ports. To be able to use the remaining 36 ports you'll need (3) 12-port licenses. Be sure to include this in the order.
- NOTE: Since port security is no longer a requirement, we removed the need for the Enterprise Package license. This will be a considerable savings.

24. Appendix B: Glossary

Term	Description
BAU	Business As Usual; day to day procedures such as provisioning of storage
BISO	Business Information Security Officer. Each business unit has its own BISO. The BISO is ultimately responsible for interpreting CISS and approving security measures.
CEP	Common Extranet Platform – a secure IP network isolated from the corporate network by a firewall. Citi uses CEP to host applications that need partner connectivity.
CISS	Citi Information Security Standards
CLI	Command Line Access
COB	Continuity of Business
DM	Device Manager: GUI Software used to manage switch specific features
EMC	EMC Corporation http://emc.com
EP	Exposure Profile: As a part of security assessment process, a risk profile must be built for all products.
FC	Fibre Channel
DCNM Client	Data Center Network Manager: GUI Client used to manage MDS fabrics
DCNM Server	DCNM Server: Manages access from multiple simultaneous clients. DCNM clients connect to this server.
FSPF	Fabric Shortest Path First protocol: It calculates the best path between switches, establishes routes across the fabric and calculates alternate routes in event of a failure or topology change.
FTE	Full Time Employee
GDN	Global Data Network. This is Citi's corporate network or Intranet
CSBE	CATE Storage and Backup Engineering
Gen4	Generation 4 hardware
GUI	Graphical User Interface
ICQ	Information Security Compliance Questionnaire: As a part of the security assessment process, ICQ must be completed for every product. The ICQ helps identify gaps with CISS.
ISL	Inter switch link
IVR	Inter-VSAN Routing
HDS	Hitachi Data Systems http://hds.com
MPSM	Multi Protocol Services Module

Term	Description
Ops, Operations	Operations: Regional teams responsible for operating Citi SANs in various datacenters
PCM	Process Control Manual: this is where Operations document their processes. Each region has its own PCM.
Port Channel	A collection of ISLs where individual ISL failure does not trigger FSPF convergence
Port Security	Tie switch port to node PWWN or switch WWN to safeguard from unauthorized access
RA	Risk Acceptance: RA must be approved by management if product with security gaps is being deployed in production.
SA	System Administrator: Person who manages servers
SAN	Storage Area Network
NX-OS	Switch firmware
SOE	Citi Standard Operating Environment
SSM	Storage Service Module
Sup2	Generation 2 supervisor module
Traffic Engineering	Manually allocating VSANs to ISLs/Port Channels for optimal utilization, applying QoS to prioritize traffic through the network, and manually changing FSPF cost to send traffic down a different path to meet SLA.
Trunk, or Trunked ISL	An ISL that is configured to carry multiple VSANs
VSAN	Virtual SAN

25. Appendix C: Switch Configuration

The new SAN architecture with up to 88 NPV enabled MDS 9148 switches can be a challenge to configure in a timely manner. This section provides a template of commands to configure the MDS 9148 Edge switches. Change items in **red** to match the switch and environment

25.1. Initial Switch Setup

The vendor (EMC or HDS) will rack and configure the switch with its initial config.

Power on

Set generic/temp admin password **xxxxxxxx**

! Configure management interface

interface mgmt0

ip address **10.40.42.132 255.255.255.0**

ip default-gateway **10.40.42.2**

25.2. Base Config

There are two configurations for the MDS 9148 Switches, NPV and Non-NPV.

25.2.1. MDS 9148 with NPV enabled

This configuration is for NPV enabled MDS 9148 switches.

These configuration settings require modifications before executing on a switch.

!NOTE: For NPV MDS 9148 Switches that connect to MDS 9710 Directors, the 9710 directors

!require that fport trunking feature be turned on and NPIV be enabled.

!feature fport-channel-trunk

!npiv enable

!For MDS 9148 Switches that will be running in NPV Mode, enable NPV first. It will “erase”

!the config and perform a “reload”. The configuration will be lost, except for the IP configuration.

feature npv

banner motd # Unauthorized use of this system is prohibited. #

! Configure Roles

role name storage_admin

rule 1 permit config

rule 2 permit debug

rule 3 permit show

rule 4 permit exec

rule 5 deny config feature aaa

rule 6 deny config feature radius-server

```
rule 7 deny config feature ssh
rule 8 deny debug feature aaa
rule 9 deny config feature logging
rule 10 permit clear
rule 11 deny clear feature accounting
rule 12 deny clear feature logging
exit
```

```
role name vendor
rule 1 permit show
rule 2 permit exec feature attach
rule 3 permit clear
rule 4 permit debug
rule 5 permit exec feature undebug
rule 6 permit exec feature dir
rule 7 permit exec feature feping Omit, not a valid rule in NPV Mode
rule 8 permit exec feature fctrace Omit, not a valid rule in NPV Mode
rule 9 permit exec feature terminal
rule 10 permit exec feature delete
rule 11 permit exec feature copy
rule 12 permit exec feature install
rule 13 permit exec feature ping
exit
```

```
role name script
rule 1 permit show
rule 2 permit exec feature attach
rule 3 permit clear
rule 4 permit debug
rule 5 permit exec feature undebug
rule 6 permit exec feature dir
rule 7 permit exec feature feping Omit, not a valid rule in NPV Mode
rule 8 permit exec feature fctrace Omit, not a valid rule in NPV Mode
rule 9 permit exec feature terminal
exit
```

```
role name facility
rule 1 permit show
rule 2 permit exec feature system
rule 3 permit exec feature terminal

exit
role commit
```

```
ntp distribute
ntp server 192.193.215.65
```

```
ntp server 192.193.215.69
ntp server 192.193.215.73
ntp commit
```

! Allow SSH access (tcp) via NPS / Active Directory Authentication

```
ip access-list inbound1 permit tcp any any eq port dst_ssh
```

! NTP Servers

```
ip access-list inbound1 permit udp 192.193.215.65 0.0.0.0 any eq port dst_ntp
ip access-list inbound1 permit udp 192.193.215.69 0.0.0.0 any eq port dst_ntp
ip access-list inbound1 permit udp 192.193.215.73 0.0.0.0 any eq port dst_ntp
ip access-list inbound1 permit icmp any any
```

! Allow SanScreen / SRM / HPNA read-only SNMP v2 access

```
snmp-server community sanscreen group facility
snmp-server community srmdadmin group facility
snmp-server community cert1234 group facility
```

```
snmp-server enable traps license
```

```
snmp-server enable traps entity
```

```
snmp-server enable traps fedomain Omit, not a valid rule in NPV Mode
```

```
snmp-server enable traps zone Omit, not a valid rule in NPV Mode
```

```
no cdp enable Omit, not a valid rule in NPV Mode
```

! In NPV Mode, No Zoning information is stored on the switch

```
! Drop traffic when not zoned for security
```

```
no system default zone default zone permit
```

```
! Distribute all (active or not) zonesets to all switches for COB
```

```
system default zone distribute full
```

```
! Configure interfaces
```

```
! Enable all ports by default so that facility can test new connections
```

```
no system default switchport shutdown
```

```
! We do not want to automatically send all VSANs down every ISL
```

```
system default switchport trunk mode off
```

! We need to configure all ports as F ports so that no damage is done if

! switches are accidentally interconnected

```
interface fc1/1-48
switchport mode F
exit
```

! Set default for interfaces on edge switches

```
! Disable link-state-trap on all ports except ISL ports 1, 13, 25, 37
interface fc1/2-12, fc1/14-24, fc1/26-36, fc1/38-48
no link-state-trap
exit
```

```
! Enable NPIV to support HP C Class Blade Center
npiv enable
```

25.2.2. MDS 9710 Core and/or Storage Edge

These configuration settings require modifications before executing on a switch.

!NOTE: For NPV MDS 9148 Switches that connect to MDS 9710 Directors, the 9710 Core ! directors require that fport trunking feature be turned on and NPIV be enabled.

```
banner motd # Unauthorized use of this system is prohibited. #
```

```
!*****
```

```
!MDS 9710 Core Directors Only
feature fport-channel-trunk
```

```
!*****
```

```
npiv enable
```

```
! Configure roles
```

```
! Enable role distribution via CFS
```

```
role distribute
```

```
! Roles
```

```
role name storage_admin
```

```
rule 1 permit config
```

```
rule 2 permit debug
```

```
rule 3 permit show
```

```
rule 4 permit exec
```

```
rule 5 deny config feature aaa
```

```
rule 6 deny config feature radius-server
```

```
rule 7 deny config feature ssh
```

```
rule 8 deny debug feature aaa
```

```
rule 9 deny config feature logging
```

```
rule 10 permit clear
```

```
rule 11 deny clear feature accounting
```

```
rule 12 deny clear feature logging
```

```
exit
```

```
role name vendor
```

```
rule 1 permit show
```

```
rule 2 permit exec feature attach
```

```
rule 3 permit clear
```

```
rule 4 permit debug
rule 5 permit exec feature undebug
rule 6 permit exec feature dir
rule 7 permit exec feature fcping
rule 8 permit exec feature fctrace
rule 9 permit exec feature terminal
rule 10 permit exec feature delete
rule 11 permit exec feature copy
rule 12 permit exec feature install
rule 13 permit exec feature ping
exit
```

role name script

```
rule 1 permit show
rule 2 permit exec feature attach
rule 3 permit clear
rule 4 permit debug
rule 5 permit exec feature undebug
rule 6 permit exec feature dir
rule 7 permit exec feature fcping
rule 8 permit exec feature fctrace
rule 9 permit exec feature terminal
exit
```

role name facility

```
rule 1 permit show
rule 2 permit exec feature system
rule 3 permit exec feature terminal
```

exit

role commit

ntp distribute

```
ntp server 192.193.215.65
ntp server 192.193.215.69
ntp server 192.193.215.73
ntp commit
```

! Allow SSH access (tcp) via NPS / Active Directory Authentication

```
ip access-list inbound1 permit tcp any any eq port dst_ssh
```

! NTP Servers

```
ip access-list inbound1 permit udp 192.193.215.65 0.0.0.0 any eq port dst_ntp
ip access-list inbound1 permit udp 192.193.215.69 0.0.0.0 any eq port dst_ntp
ip access-list inbound1 permit udp 192.193.215.73 0.0.0.0 any eq port dst_ntp
ip access-list inbound1 permit icmp any any
```

! Allow SanScreen / SRM / HPNA read-only SNMP v2 access

snmp-server community sanscreen group facility

snmp-server community srmadmin group facility

snmp-server community cert1234 group facility

snmp-server enable traps license

snmp-server enable traps entity

snmp-server enable traps fcdomain

snmp-server enable traps zone

no cdp enable

! Zoning related configuration

! Drop traffic when not zoned for security

no system default zone default-zone permit

! Distribute all (active or not) zonesets to all switches for COB

system default zone distribute full

! Configure interfaces

! Enable all ports by default so that facility can test new connections

no system default switchport shutdown

! We do not want to automatically send all VSANs down every ISL

system default switchport trunk mode off

! We need to configure all ports as F ports so that no damage is done if

! switches are accidentally interconnected

interface fc1/1-48

switchport mode F

exit

! Enable NPIV to support HP C Class Blade Center

npiv enable

25.3. Custom Configuration (Variable Settings)

These configuration settings require modifications before executing on a switch.

25.3.1. MDS 9148 with NPV enabled

! Set up time zone and automatic DST if applicable

clock timezone **EST -5 0**

clock **summer-time EDT 2 Sunday Mar 02:00 1 Sunday Nov 02:00 60**

!UserID for EMC (if supported by EMC)

```
username emc password xxxxxxxxxx role vendor
!Or for HDS (if supported by HDS)
username hds password xxxxxxxxxx role vendor
!Change admin ID temporary password (set by vendor on install)
username admin password xxxxxxxxxx
```

```
snmp-server contact gtussansupport@imcnam.ssmb.com
snmp-server location GTDC, Georgetown, Tx
```

```
! SNMP TRAP collector server IP address, community (default public) and
! UDP port (default 162) will be provided by ESS
snmp-server host 168.109.182.108 version 2c public udp-port 162
snmp-server host 168.109.182.109 version 2c public udp-port 162
```

```
!SNMP SANscreen hosts
snmp-server host 169.193.228.119 version 2c public udp-port 2162
snmp-server host 169.193.228.120 version 2c public udp-port 2162
```

```
! Enable the following alerts on core switches ONLY, You do not want to be alerted every time a
! host is reboot or shutdown for maintenance. If you're not using core-edge topology, do not
! enable this; instead enable on a per interface basis (sample not provided in template)
! snmp-server enable traps link cisco
```

```
! Configure switch name
switchname usucd01ae001
```

```
! Enable DNS lookup
ip domain-lookup
ip name-server 10.40.32.11 150.110.234.192
ip domain-name nam.nsroot.net
```

```
! This will configure the VSAN.
! VSAN id 2 = "usucd01a" (Fabric A)
vsan database
  vsan 2 name "usucd01a"
  exit
```

```
vsan database
  vsan 2 suspend
  no vsan 2 suspend
  exit
```

```
! Port channel configuration
interface port-channel 1
  channel mode active
  switchport mode NP
```

```
switchport trunk allowed vsan 1
switchport trunk allowed vsan add 2
switchport rate-mode dedicated
switchport trunk mode on
no shut
exit
```

```
interface fc1/1, fc1/13
switchport description "To Core switch usucd01ac001"
switchport rate-mode dedicated
switchport mode NP
switchport trunk mode on
port-license acquire
channel-group 1
shut
no shut
exit
```

```
interface port-channel 2
channel mode active
switchport mode NP
switchport trunk allowed vsan 1
switchport trunk allowed vsan add 2
switchport rate-mode dedicated
switchport trunk mode on
shut
no shut
exit
```

```
interface fc1/25, fc1/37
switchport description "To Core switch usucd01ac002"
switchport mode NP
switchport trunk mode on
port-license acquire
channel-group 2
shut
no shut
exit
```

! For HDS supported switches, add this community string setting
! Allow SNMP read-only access from Hi-Track
snmp-server community hitrack group facility
! End HDS supported switch

25.3.2. MDS 9710 Storage Edge Example

! Set up time zone and automatic DST if applicable

clock timezone **EST -5 0**

clock **summer-time EDT 2 Sunday Mar 02:00 1 Sunday Nov 02:00 60**

!UserID for EMC (if supported by EMC)

username emc password **xxxxxxxxxx** role vendor

!Or for HDS (if supported by HDS)

username emc password **xxxxxxxxxx** role vendor

!Change admin ID temporary password (set by vendor on install)

username admin password **xxxxxxxxxx**

snmp-server contact **gtussansupport@imcnam.ssmb.com**

snmp-server location **GTDC, Georgetown, Tx**

! SNMP TRAP collector server IP address, community (default public) and

! UDP port (default 162) will be provided by ESS

snmp-server host **168.109.182.108** version 2c public udp-port **162**

snmp-server host **168.109.182.109** version 2c public udp-port **162**

!SNMP SANscreen hosts

snmp-server host **169.193.228.119** version 2c public udp-port 2162

snmp-server host **169.193.228.120** version 2c public udp-port 2162

! Enable the following alerts on **core switches ONLY**, You do not want to be alerted every time a

! host is reboot or shutdown for maintenance. If you're not using core-edge topology, do not

! enable this; instead enable on a per interface basis (sample not provided in template)

! **snmp-server enable traps link cisco**

! Configure switch name

switchname **usucd01as001**

! Enable DNS lookup

ip domain-lookup

ip name-server **10.40.32.11 150.110.234.192**

ip domain-name **nam.nsroot.net**

! This will configure the VSAN.

! VSAN id 2 = "usucd01a" (Fabric A)

vsan database

vsan **2** name "**usucd01a**"

exit

! Enable "enhanced" zoning mode for all production VSANs

zone mode enhanced vsan **2**

! Domain IDs related configuration
! Enable CFS distribution for domain IDs to eliminate possibility
! of duplicates and resulting isolation
fcdomain distribute

! Please use a Domain ID design guide
fcdomain domain 1 static vsan 2
fcdomain priority 128 static vsan 2
fcdomain commit vsan 2

! restart fcdomain services for changes to take effect
fcdomain restart disruptive vsan 2

! FCIDs should be made persistent
fcdomain fcid persistent vsan 2

! Reserve a block of domain IDs for VSANs
fcdomain allowed 1-52 vsan 2
fcdomain commit vsan 2

vsan database
vsan 2 suspend
no vsan 2 suspend
exit

! Device alias related configuration
! Disable device alias enhanced mode because changing device alias will cause
! automatic change to active zoneset in enhanced mode
no device-alias mode enhanced
device-alias distribute
device-alias commit

! Port channel configuration
interface fc1/1, fc2/1,,,etc
switchport description "To Core switch usucd01ac001"
switchport rate-mode dedicated
switchport mode E
channel-group xx
shut
no shut
exit

interface port-channel xx
switchport trunk mode on
channel mode active

```
switchport trunk allowed vsan 1
switchport trunk allowed vsan add 2
no shut
exit
```

```
interface fc1/2, fc2/2,,etc
switchport description "To Core switch usucd01ac002"
switchport rate-mode dedicated
switchport mode E
channel-group yy
shut
no shut
exit
```

```
interface port-channel yy
switchport trunk mode on
channel mode active
switchport trunk allowed vsan 1
switchport trunk allowed vsan add 2
shut
no shut
exit
```

! For HDS supported switches, add this community string setting

! Allow SNMP read-only access from Hi-Track

snmp-server community hitrack group facility

! End HDS supported switch

25.3.3. MDS 9710 Core Example

! Set up time zone and automatic DST if applicable

clock timezone **EST -5 0**

clock **summer-time EDT 2 Sunday Mar 02:00 1 Sunday Nov 02:00 60**

!UserID for EMC (if supported by EMC)

username emc password **xxxxxxxx** role vendor

!Or for HDS (if supported by HDS)

username emc password **xxxxxxxx** role vendor

!Change admin ID temporary password (set by vendor on install)

username admin password **xxxxxxxx**

snmp-server contact **gtussansupport@imcnam.ssmb.com**

snmp-server location **GTDC, Georgetown, Tx**

! SNMP TRAP collector server IP address, community (default public) and

! UDP port (default 162) will be provided by ESS

```
snmp-server host 168.109.182.108 version 2c public udp-port 162
snmp-server host 168.109.182.109 version 2c public udp-port 162
```

!SNMP SANscreen hosts

```
snmp-server host 169.193.228.119 version 2c public udp-port 2162
snmp-server host 169.193.228.120 version 2c public udp-port 2162
```

! Enable the following alerts on **core switches ONLY**, You do not want to be alerted every time a
! host is reboot or shutdown for maintenance. If you're not using core-edge topology, do not
! enable this; instead enable on a per interface basis (sample not provided in template)
! **snmp-server enable traps link cisco**

! Configure switch name
switchname **usucd01as001**

! Enable DNS lookup
ip domain-lookup
ip name-server **10.40.32.11 150.110.234.192**
ip domain-name **nam.nsroot.net**

! This will configure the VSAN.
! VSAN id 2 = "usucd01a" (Fabric A)
vsan database
vsan **2** name "**usucd01a**"
exit

! Enable "enhanced" zoning mode for all production VSANs
zone mode enhanced vsan **2**

! Domain IDs related configuration
! Enable CFS distribution for domain IDs to eliminate possibility
! of duplicates and resulting isolation
fcdomain distribute

! Please use a Domain ID design guide
fcdomain domain **1** static vsan **2**
fcdomain priority 128 static vsan **2**
fcdomain commit vsan **2**

! restart fcdomain services for changes to take effect
fcdomain restart disruptive vsan **2**

! FCIDs should be made persistent
fcdomain fcid persistent vsan **2**

! Reserve a block of domain IDs for VSANs

```
fcdomain allowed 1-52 vsan 2
fcdomain commit vsan 2
```

```
vsan database
vsan 2 suspend
no vsan 2 suspend
exit
```

```
! Device alias related configuration
! Disable device alias enhanced mode because changing device alias will cause
! automatic change to active zoneset in enhanced mode
no device-alias mode enhanced
device-alias distribute
device-alias commit
```

! Port channel configuration to Storage Edge

```
interface fc1/1, fc2/1,,,etc
switchport description "To Core switch usucd01as001"
switchport rate-mode dedicated
switchport mode E
channel-group xx
shut
no shut
exit
```

```
interface port-channel xx
switchport trunk mode on
channel mode active
switchport trunk allowed vsan 1
switchport trunk allowed vsan add 2
no shut
exit
```

```
interface fc1/2, fc2/2,,,etc
switchport description "To Core switch usucd01as002"
switchport rate-mode dedicated
switchport mode E
channel-group yy
shut
no shut
exit
```

```
interface port-channel yy
switchport trunk mode on
channel mode active
switchport trunk allowed vsan 1
```

```
switchport trunk allowed vsan add 2
shut
no shut
exit
```

! Port channel configuration to Host Edge

! The MDS 9148 switches are Node Ports to the director, the port channels (ISLs) on the
! MDS 9710 will be trunked fports (TF) and trunked node ports (TNP) on the 9148.

! This is an example of how to configure one fport channel on the MDS 9710. Modify for
! additional port channels.

! Port channel configuration example

```
interface port-channel xx
channel mode active
switchport mode F
switchport trunk allowed vsan 1
switchport trunk allowed vsan add 2
switchport rate-mode dedicated
switchport trunk mode on
no shut
exit
```

```
interface fc1/47, fc1/48
switchport description "To Edge switch usucd01ae001"
switchport rate-mode dedicated
switchport mode F
switchport trunk mode on
channel-group xx
shut
no shut
exit
```

! Port channel configuration example

```
interface port-channel yy
channel mode active
switchport mode F
switchport trunk allowed vsan 1
switchport trunk allowed vsan add 2
switchport rate-mode dedicated
switchport trunk mode on
no shut
exit
```

```
interface fc1/47, fc1/48
switchport description "To Edge switch usucd01ae002"
```

```
switchport rate-mode dedicated
switchport mode F
switchport trunk mode on
channel-group yy
shut
no shut
exit
```

! For HDS supported switches, add this community string setting

! Allow SNMP read-only access from Hi-Track

```
snmp-server community hitrack group facility
```

! End HDS supported switch

25.4. Final Configuration Settings

Before turning the switches over to Production, these are the final configuration updates. They are typically done manually, versus running via a script. These settings include Logging, IP ACL's and Radius configurations.

!Fab A and B DCNM Servers (if using a separate DCNM for each fabric)

```
ip access-list inbound1 permit ip 10.40.42.89 0.0.0.0 any
```

```
ip access-list inbound1 permit ip 10.40.42.91 0.0.0.0 any
```

!SAN Screen servers

```
ip access-list inbound1 permit udp 169.193.228.119 0.0.0.0 any eq port dst_snmp
```

```
ip access-list inbound1 permit udp 169.193.228.120 0.0.0.0 any eq port dst_snmp
```

!DCNM Servers

```
snmp-server host 10.40.42.89 version 2c public udp-port 2162
```

```
snmp-server host 10.40.42.91 version 2c public udp-port 2162
```

! Authenticate to NPS via RADIUS

! This should only be configured after all instruction in section 7.1 of Solutions Guide

! have been executed

! RADIUS server host is Management Server where NPS is running

! Use the Key that was configured in NPS

```
radius-server host 10.40.42.200 key cisco123
```

```
radius-server host 10.40.42.201 key cisco123
```

```
aaa group server radius radius-group1
```

```
server 10.40.42.200
```

```
server 10.40.42.201
```

```
exit
```

```
aaa authentication login default group radius-group1
```

! Console access should not be authenticated via ACS

! Console can be used for recovery from bad ACS

```
aaa authentication login console local
```

! The following command will provide local (switch) authentication in the event that the Primary and Secondary NPS server are not available.

```
aaa authentication login default group radius-group1 local
```

! End Authenticate to NPS via RADIUS section

! Warning: the following will apply ACL to interface

! Incorrect ACL will lock you out instantly - recover from console port

```
ip access-group inbound1 in
```

```
exit
```

! Execute last before going to Production

! Logging related configuration.

! Enable logging configuration distribution via CFS

```
logging distribute
```

! SYSLOG server IP address and facility

```
logging server 10.40.42.200 6 facility local1
```

```
logging server 10.40.42.201 6 facility local2
```

```
logging level auth 5
```

```
logging level authpriv 5
```

```
logging level aaa 6
```

```
logging commit
```

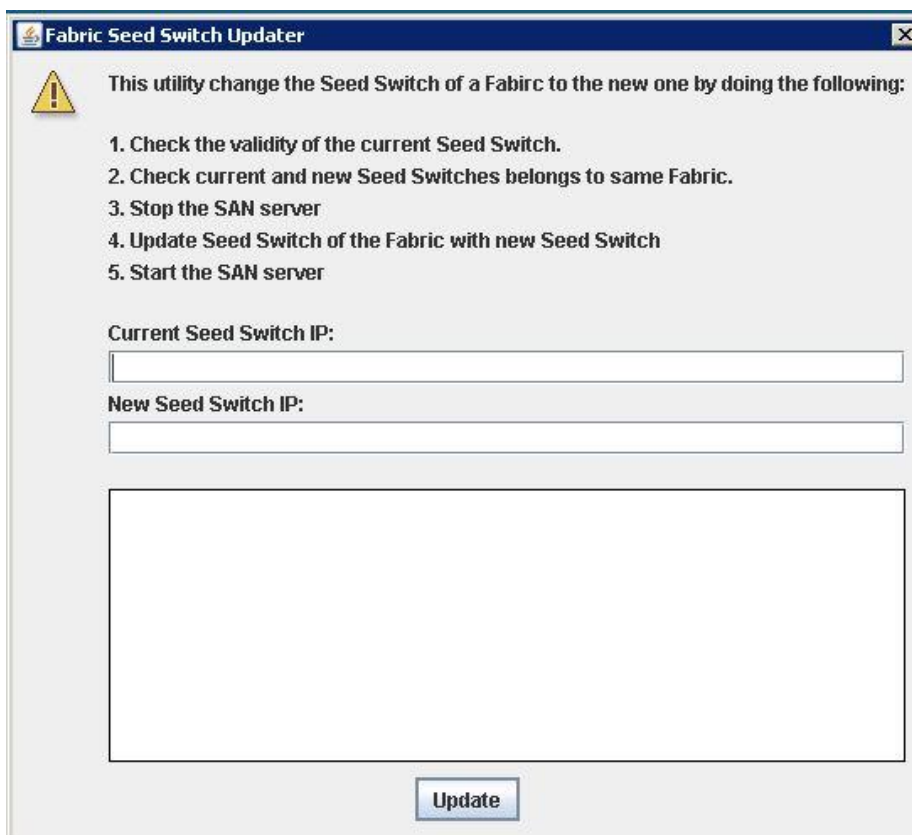
26. Appendix D: Seed Switch Utility

For SAN tech refreshes, where new switches are integrated into an existing SAN and old switches are being removed, this utility is helpful in switching the seed switch from an old switch to a new switch.

1. Create a “SeedSwitchUpdater.bat” file on the DCNM server, in the DCNM install directory (Example: D:\Program Files\Cisco Systems\dcm\fm\bin). Copy the following commands into the batch file, modifying the commands with the correct install directory.

```
rem Description: Update new Seed Switch IP with current Seed Switch.
rem Usage: 'seedSwitchUpdater'
set JAVACMD=D:\Program Files\Cisco Systems\dcm\java\jre1.7\bin\java
set JVMARGS="-Dmds.nmsRoot=D:\Program Files\Cisco Systems\dcm\fm"
set INSTALLDIR=D:\Program Files\Cisco Systems\dcm\fm
set LIB=%INSTALLDIR%\lib
set
CP2=%CP%;%INSTALLDIR%\lib\seedswitchutil.jar;%INSTALLDIR%\lib\fmserver.jar;%INSTALLDIR%\lib\log4j.jar;%INSTALLDIR%\lib\hsqldb.jar;%INSTALLDIR%\lib\jdbcpool.jar;%INSTALLDIR%\lib\installer.jar;%INSTALLDIR%\lib\ojdbc6.jar;%INSTALLDIR%\lib\postgresql-8.1.jar
cd %INSTALLDIR%
"%JAVACMD%" -cp "%CP2%" -Dmds.nmsRoot="%INSTALLDIR%" com.cisco.dcbu.sm.server.db.SeedSwitchUpdater
```

2. When you're ready to change to the new seed switch, make sure no users are logged into DCNM and then run the “SeedSwitchUpdater.bat” file (run as administrator).



Fabric Seed Switch Updater

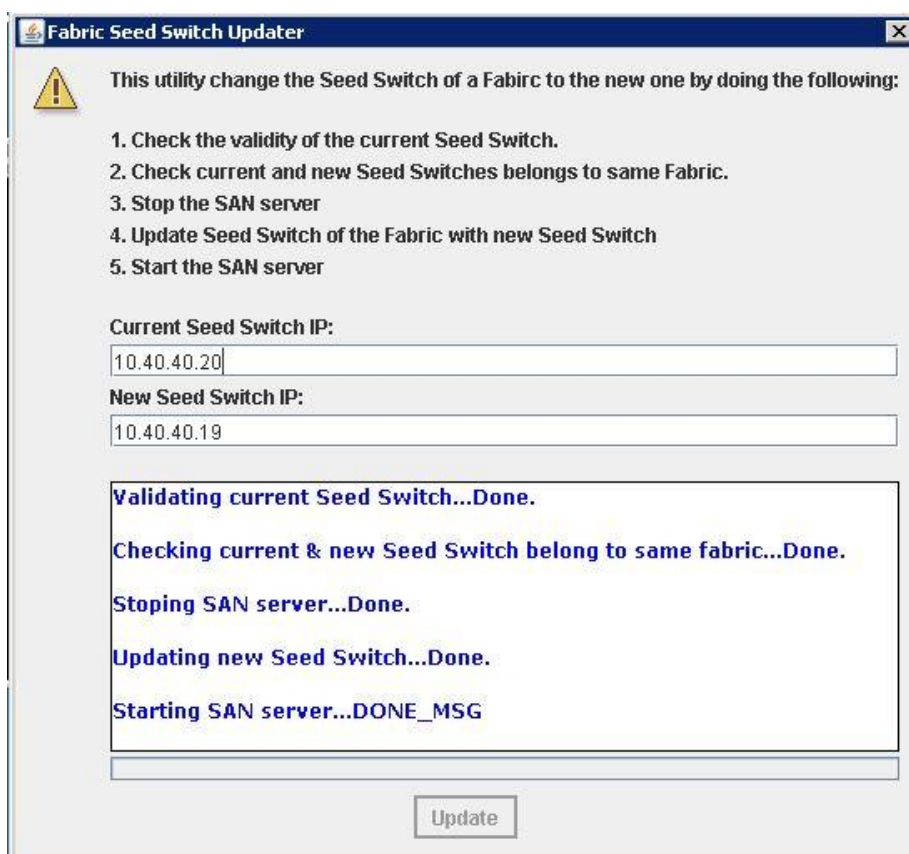
 This utility change the Seed Switch of a Fabirc to the new one by doing the following:

1. Check the validity of the current Seed Switch.
2. Check current and new Seed Switches belongs to same Fabric.
3. Stop the SAN server
4. Update Seed Switch of the Fabric with new Seed Switch
5. Start the SAN server

Current Seed Switch IP:

New Seed Switch IP:

3. Enter the IP address of the Current and New Seed Switch and click “Update”.



4. When complete, close the dialog box.
5. Log back into DCNM, from the “Control Panel” you should see the new Seed Switch IP.

27. Appendix E: Test Scope / Testing / Results

All testing information is documented in the “Release Notes” located on the CSBE Cisco webpage:

<http://catercollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/ciscomds.aspx>

28. Appendix F: Revision History

3.0 – Date: 12-Sept-08

- Modified Section 2.1
 - Released: SAN-OS 3.3(1c)
 - Released: Fabric Manager 3.3(1c)
 - Added MDS 9124, 9134 and 9222i as certified models
- Modified Section 5: Mgmt Server Build
 - Modified instructions for upgrading an existing Fabric Manager server
 - Added instructions for installing a new (Full) Fabric Manager server

- Modified “Secure Fabric Manager Server”. Locking down the Fabric Manager Client to the loopback address (127.0.0.1). Access to the client is allowed from FMS only.
- Modified “Secure Performance Manager Server”. Locking down the Performance Manager Server to the loopback address (127.0.0.1). Access to the web server is allowed from FMS only.
- Modified Fabric Manager preferences for SSH access. Blank out the “telnet” cmd.
- Modified Authentication to Active Directory. Added commands to turn on and turn off Active Directory.
- Modified Downgrade Fabric Manager. Added more detail to the downgrade process.
- Modified Section 6.6: Switch config, SANOS upgrade
 - Added clarity to the commands
- Modified Section 13: Port Security
 - Added statement making Port Security optional.
- Modified Section 16: Firmware upgrade/downgrade
 - Added detail to the process, showing wizard screenshots.
- Added Appendix: Revision History (this section)

3.2 – Date: 5-Dec-08

- Modified Section 5.10: Configuration of Active Directory
 - Added Secondary IAS Server
 - Added local authentication as secondary to IAS/AD on the switches for the Admin ID
 - Removed MSCHAP command. Using PAP, until MSCHAPv2 is supported on Cisco
- Modified Section 7.1: IAS
 - Added a Secondary IAS Server
 - Added a shortcut to creating the Secondary IAS Server
- Modified Section 17: Known Issues
 - Added “Cisco switches don’t support MSCHAPv2”

3.3 / 3.4 – Date: 6-April-10

- Modified Section 2 – added information pertinent to Generation 3 Line Cards and 8 Gbps SFPs.
- Modified Section 2.11 – modified fabric design examples
- Modified Section 5: Management Server Build
 - Edited installation instructions to reflect new Cisco directories
- Modified Section 6.9: Licensing – **Enterprise_Pkg is no longer required**. Cost savings.
- Insert Section 15: Port Group Monitoring
- Modified Section 17: Known Issues
- Removed Section 5.2.3: Fabric Manager Client Install (Installed via package)
- Removed Section 5.2.4: Device Manager Client Install (Installed via package)
- Modified Section 5.3 and 5.4: Securing Fabric Mgr Client and Performance Mgr to the loopback address (127.0.0.1) is optional. Since Fabric Mgr and Performance Mgr

authenticate with Radius/Active Directory, this no longer a requirement, you can use the Fabric Mgr Server IP address.

- Removed Section 20: Appendix C: Resolving Application Conflicts.

3.5 – Date: 22-July-10

- Modified Section 20 – Removing all the ip-access list commands for ssh. Adding ip-access list for any to any for ssh. Since all ssh access is authenticated by IAS/Active Directory, it is no longer necessary to lock it down. Received Security Office signoff.

3.6 – Date: 24-August-10

- Modified Section 5.8.2 – Newer version of Hi-Track (v5.1.0) released. Spac: Htmr5110.

3.8 – Date: 23-December-11

- This is a major revision. All sections were modified.

4.0 – Date: 28-February-12

- Updated the “Known Issues” section with the patch fix for the SNMP Timeout issue.

4.1 – Date: 28-December-12

- Modified Section 2.3 – Added additional comments to make it clear that the MDS 9506/9509 on have 96Gb of backplane bandwidth with the 8Gb Advanced Modules.
- Added Section 21 - Security Review Findings

4.2 – Date: 2-Aug -2013

- Modified Section 2.12x – Two and Three Tier SAN Examples. Added Edge-Core-Edge design examples
- Added Section 5.2.3 - DCNM Client Install on Workstation (standalone install)
- Added Section 5.2.5 _Device Manager 5.2(8b) Install (standalone install)
- Added Section 8.1 – SEMS “Include List”
- Added support for NX-OS 5.2(8b)

4.3 – Date: 6-Nov -2013

- Modified Section 2.12.2 – Two Tier SAN
 - Updated our design best practice to include the already certified MDS 9148 switches. Big cost save using 9148’s versus 9513’s
 - Added SAN examples using MDS 9148’s
- Added Section 2.12.6 MDS 9148 Switch Port Layout – ISL/Host

4.4 – Date: 18-Dec -2013

- Added support for NX-OS 5.2(8c)
- Modified Section 3.2 Power and Cooling
- Modified Section 5.2.5 Device Manager 5.2(8c) install
- Modified Section 24 Appendix C – Change command for SNMP community string from group “network-operator” to facility”. Facility has read only rights.

4.5 – Date: 6-Jun -2014

- Modified: Nearly every section of this document was updated. Key updates were:
 - NX-OS 6.2(7) for MDS 9710
 - NX-OS 5.2(8d) for MDS 9100, 9200, 9500 Series switches
 - DCNM 6.3.1 install/upgrade to enable management of MDS 9710
 - New SAN Architecture
 - Global Naming Standard
 - MDS 9710, port layout, ISL layout (port-channel information)
 - MDS 9148, port layout, ISL layout (port-channel information)
 - Radius NPS required to run on W2k8 Server Enterprise Edition to accommodate more than 50 Clients
 - Radius NPS config to accommodate NX-OS 6.2.x and 5.2.x switches
 - SNMP Traps updated
 - Switch Backup and Restore Procedure
 - Switch Configuration (Initial, Base, Custom, Final)

4.6 – Date: 28-Jul-2014

In addition to the prior updates in version 4.5 of this document (above)

- Modified Section 2.7.3 (Edge-Core-Edge) - The New SAN Architecture to use NPV enabled MDS9148 switches. This allows us to scale up to 88 edge switches in an Edge – Core – Edge design. Also added a Quad Core design to support 176 Host Edge switches.
- Modified Section 2.8 – Line card and switch port layout
- Modified Section 3.3 - Dedicated IP subnet for the MDS switches
- Modified Section 5 – DCNM 6.3.2 required to support of future MDS 9148s switches.

4.7 – Date: 5-Dec-2014

- Added support for NX-OS 5.2(8e) on the old SAN (required for GNU Bash Vulnerability)
- Added support for NX-OS 6.2(9a) on the new SAN (required for GNU Bash Vulnerability)
- Added support for MDS 9148s (MDS 9250i pending certification)
- Added Section 3.6 – Infrastructure Fibre Channel Cabling
- Added Section 7.1.1.1 – Switch Roles (vsan policy deny – not allowed)

4.8 – Date: 6-Feb-15

- Modified Section 2.8.5 – MDS 9148 Port Channel Layout – Changed the Host Edge Port-Channel numbers to Port-Channel 1 (to Core 1) and Port-Channel 2 (to Core 2). All Host Edge switches will have the same Port-Channel definitions, instead of 1-88 and 101-188.
- Modified Section 25.2.1 & 2: Added SNMP community string for SRM and HPNA
- Modified Section 25.3.1 – MDS 9148 Custom settings – Changed the Host Edge port-channel definition to reflect the use of port-channel 1 and port-channel 2.

4.9 – Date: 20-Mar-15

- Added support for NX-OS 5.2(8f) and 6.2(11b) which fixes several VTMs.
- Modified Section 17: Port Monitoring settings / Added command to send traps to SRM
- Added Section 17.2.4: Troubleshooting Port Monitoring
- Inserted Section 26: Seed Switch Utility

- Modified Section 5.6.2: Support for HDS HiTrack Monitor v7.1.