



Cisco DCNM Web Client Online Help, 10.4(2) Release

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2018 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Dashboard 1

Summary Dashboard	1
Viewing Top ISLs/Trunks Summary	2
Viewing Top SAN End Ports (SAN only) Summary	3
Viewing Top CPU Summary	3
Viewing Health Summary	4
Viewing Inventory (Ports) Summary	4
Viewing Inventory (Modules) Summary	4
Viewing Inventory (ISLs) Summary	5
Viewing Inventory (Logical) Summary	5
Viewing Inventory (Switches) Summary	5
Viewing Inventory (Port Capacity) Summary	6
Network Dashboard	6
Switch Dashboard	7
Storage Dashboard	9
Viewing Storage Enclosures Information	9
Viewing Storage Systems Information	9
Components	10
Pools	10
LUNs	11
Filer Volumes	12
Hosts	13
Storage Processors	13
Storage Ports	14
Viewing Storage Enclosure Events	14
Viewing Storage Enclosure Topology	14
Viewing Storage Enclosure Traffic	15
Compute	15

Viewing Host Enclosures	15
Viewing Host Events	16
Viewing Host Topology	16
View Host Traffic	17

CHAPTER 2

Topology 19

Topology	19
Status	19
Scope	19
Searching	20
Quick Search	20
Tags	21
Host name (VDP)	21
Host name (vCenter)	21
Host IP	21
Host MAC	21
Segment ID	21
Multicast Group	21
VXLAN ID (VNI)	22
VLAN	22
VSAN ID/Name	22
FabricPath	22
VXLAN OAM	23
Show Panel	24
Layouts	25
Zooming, Panning and Dragging	25
Switch Slide-Out Panel	25
Switch Roles	25
Beacon	26
Tagging	26
More Details	26
Link Slide-Out Panel	26
24 Hour Traffic	26

CHAPTER 3

Inventory 27

Viewing Inventory Information	27
Viewing Inventory Information for Switches	27
Interfaces	29
Adding Interfaces	29
Editing Interfaces	30
Deleting Interfaces	30
Shutting Down Interfaces	31
Displaying Interface Show Commands	31
Rediscovering Interfaces	31
Viewing Interface History	32
HBA Link Diagnostics	32
Performing HBA Link Diagnostic Tests	33
VXLAN	34
VLAN	35
Adding a VLAN	35
Editing a VLAN	36
Deleting a VLAN	36
Shutting Down a VLAN	36
Displaying VLAN Show Commands	37
FEX	37
Add FEX	39
Edit FEX	40
VDCs	41
Add VDCs	44
Configuring Ethernet VDCs	44
Configuring Storage VDCs	46
Edit VDC	48
Switch On-Board Analytics	48
Viewing Switch On-Board Analytics	49
Configuring Settings for the Switch On-Board Analytics Charts	49
Viewing Switch On-Board Analytics Charts	50
Viewing Inventory Information for Modules	52
Viewing Inventory Information for Licenses	53
Discovery	53
Adding, Editing, Re-discovering, Purging and Removing LAN, LAN Tasks and Switch	53

Adding LAN Switches	54
Editing LAN Devices	54
Removing LAN Devices from Cisco DCNM	55
Moving LAN Devices Under a Task	55
Re-discover LAN Task	55
Purging LAN	56
Adding, Editing, Re-discovering, Purging and Removing Managed Fabrics	56
Adding a Fabric	56
Deleting a Fabric	57
Editing a Fabric	57
Moving Fabrics to Another Server Federation	58
Rediscovering a Fabric	58
Purging a Fabric	58
Adding, editing, removing, rediscovering and refreshing SMI-S Storage	59
Adding SMI-S Provider	59
Deleting SMI-S Provider	59
Editing SMI-S Provider	60
Re-Discover SMI-S Provider	60
Purge SMI-S Provider	60
Adding, Editing, Re-discovering and Removing VMware Servers	60
Adding a Virtual Center Server	61
Deleting a VMware Server	61
Editing a VMware Server	61
Rediscovering a VMware Server	62

CHAPTER 4
Monitor 63

Monitoring Switch	63
Viewing Switch CPU Information	63
Viewing Switch Memory Information	64
Viewing Switch Traffic and Errors Information	64
Viewing Switch Temperature	64
Enabling Temperature Monitoring	65
Enabling Temperature Monitoring for LAN Switches	65
Enabling Temperature Monitoring for SAN Switches	65
Viewing Other Statistics	66

Viewing Switch Custom Port Groups Information	66
Viewing Accounting Information	66
Viewing Events Information	67
Monitoring SAN	67
Monitoring ISL Traffic and Errors	68
Viewing Performance Information for NPV Links	68
Viewing Inventory Information for VSANs	69
Monitoring Performance Information for Ethernet Ports	69
Viewing Inventory Information for Host Ports on FC End Devices	70
Viewing Performance Information on All Ports	70
Viewing Performance Information for FC Flows	71
Viewing Performance Information on Enclosures	71
Viewing Performance Information on Port Groups	72
SAN Host Redundancy	72
Tests to Run	73
Results	73
Slow Drain Analysis	74
Viewing Inventory Information for Regular Zones	75
Viewing Inventory Information for IVR Zones	75
Monitoring LAN	76
Monitoring Performance Information for Ethernet	76
Monitoring ISL Traffic and Errors	76
Monitoring a vPC	77
Monitoring vPC Performance	79
Monitoring Report	80
Viewing Reports	80
Generating a Report	80
Creating SAN User Defined Reports	81
Deleting a Report Template	82
Modifying a Custom Report Template	83
Viewing Scheduled Jobs Based on a Report Template	83
Monitoring Configuration	83
Monitoring Archives	83
Compare Configuration Files	84
View or Edit Configuration	85

[Exploring Endpoint Locator Details](#) 86

CHAPTER 5

[Media Controller](#) 95

[Media Controller Topology](#) 96

[PMN Hosts](#) 97

[Add PMN Hosts](#) 99

[Edit PMN Hosts](#) 99

[Delete PMN Hosts](#) 100

[Import PMN Hosts](#) 100

[Export PMN Hosts](#) 100

[Flow Alias](#) 101

[Add Flow Alias](#) 101

[Edit Flow Alias](#) 102

[Delete Flow Alias](#) 102

[Export Flow Alias](#) 102

[Import Flow Alias](#) 103

[Policies](#) 103

[Host Policies](#) 103

[Add Host Policy](#) 104

[Edit Host Policy](#) 105

[Delete Host Policy](#) 105

[Import Host Policy](#) 106

[Export Host Policy](#) 106

[Flow Policies](#) 107

[Add Flow Policy](#) 108

[Edit Flow Policy](#) 108

[Delete Flow Policy](#) 109

[Import Flow Policy](#) 109

[Export Flow Policy](#) 109

[Flow Status](#) 110

[Events](#) 113

CHAPTER 6

[Configure](#) 115

[Deploy](#) 115

[Configuring vPC Peer](#) 115

vPC Peer History	116
Add vPC Peer Wizard	117
Delete vPC Peer	119
Edit vPC Peer Configuration	119
Configuring vPC	119
vPC History	121
Add vPC	121
Delete vPC	123
Edit vPC Configuration	123
POAP Launchpad	124
Power-On Auto Provisioning (POAP)	124
DHCP Scopes	124
Adding a DHCP Scope	125
Editing an existing DHCP Scope	125
Deleting a DHCP Scope	126
Image and Configuration Servers	126
Add Image or Configuration Server URL	127
Editing an Image or Configuration Server URL	127
Deleting an Image or Configuration Server URL	127
POAP Templates	128
Add POAP template	128
Editing a Template	129
Cloning a Template	129
Importing a Template	129
Exporting a Template	130
Deleting a Template	130
POAP Template Annotation	130
POAP Definitions	132
Creating a POAP definition	135
Uploading a POAP Definition	136
Editing a POAP Definition	137
Deleting POAP Definitions	137
Publishing POAP definitions	137
Write, Erase and Reload the POAP Switch Definition	138
Change Image	138

Updating the Serial Number of a Switch for an existing POAP Definition	138
Cable Plan	139
Create a Cable Plan	139
Viewing an Existing Cable Plan Deployment	140
Deleting a Cable Plan	140
Deploying a Cable Plan	140
Revoking a Cable Plan	140
Viewing a Deployed Cable Plan from Device	141
Templates	141
Deploying Templates	141
Template Structure	142
Template Format	143
Template Variables	146
Variable Meta Property	148
Variable Annotation	151
Templates Content	152
Advanced Features	154
Adding a Template	156
Configuring Template Job	157
Modifying a Template	158
Importing a Template	158
Installing POAP Templates	159
Exporting a Template	159
Deleting a Template	159
Configuring Jobs	160
Backup	160
Switch Configuration	160
Import Configuration File	162
Compare Configuration Files	162
Copy Configuration	163
Restore Configuration	164
Golden Backup	164
View or Edit Configuration	165
Delete Configuration	165
Archive Jobs	166

Archive Jobs	166
Job Execution Details	168
Network Config Audit	169
Generating Network Config Audit Reports	169
Creating a Network Config Audit Report	170
Monitoring Network Config Audit Report	170
Deleting a Network Config Audit Report	171
Image Management	171
Upgrade [ISSU]	171
Upgrade History [ISSU]	171
New Installation	172
Finish Installation	174
View	175
Delete	176
Switch Level History	176
Patch [SMU]	177
Patch Installation History	177
Install Patch	178
Uninstall Patch	179
Delete Patch Installation Tasks	179
Switch Installed Patches	180
Package [RPM]	180
Package Installation [RPM]	180
Install Package (RPM)	181
Uninstall Package [RPM]	182
Delete Package Installation Tasks	182
Switch Installed Packages	183
Maintenance Mode [GIR]	183
Maintenance Mode [GIR]	183
Switch Maintenance History	184
Repositories	185
Add Image or Configuration Server URL	185
Editing an Image or Configuration Server URL	186
Deleting an Image or Configuration Server URL	186
File Browser	186

Image Upload	187
Credentials Management	187
SAN Credentials	187
LAN Credentials	188
LAN Fabric Settings	190
LAN Fabrics	190
Add LAN Fabric	191
Delete LAN Fabric	194
Edit LAN Fabric	194
Add Fabric Plan	195
Delete Fabric Plan	196
General LAN Fabric Settings	197
LAN Fabric General Settings	197
LAN Fabric Border-Leaf Settings	197
LAN Fabric POAP Settings	197
LAN Fabric Encapsulation Settings	197
Mobility Domains	197
Add Mobility Domains	198
Modify Mobility Domains	198
Delete Mobility Domains	199
Segment IDs	199
Add Orchestrator	200
Modify Orchestrator	200
Delete Orchestrator	200
LAN Fabric Provisioning	200
LAN Fabric Provisioning	201
Creating a New Fabric	202
Creating a Network	204
Deploying the Network	207
Editing a Network	214
Undeploying a Network	216
Deleting a Network	219
Creating a VRF	220
Deploying VRF Instances	221
Editing a VRF	225

Undeploying a VRF	226
Deleting a VRF	229
Adding Fabric Extensions	229
Viewing the Status of the LAN Fabric Provisioning	235
Migrating Cisco NFM Overlay Networks to Cisco DCNM	235
Prerequisites	236
Guidelines and Limitations	236
Migration Workflow for Overlay Network	236
Migration Workflow Status Definitions	238
Using the Migration Wizard	241
Viewing Migration Status	243
Troubleshooting Cisco NFM to Cisco DCNM Migration	244
Network Migration Failures	244
Migration Workflow Failures	244
Detailed Logs	244
LAN Fabric Auto-Configuration	245
LAN Fabric Auto-Configuration	245
Organizations	247
Adding an Organization	248
Editing an Organization	248
Deleting an Organization	248
Partitions	248
Adding a Partition	249
Editing a Partition	249
Deleting a Partition	249
Networks	250
Adding a Network	250
Editing a Network	251
Deleting a Network	251
Profiles	251
Adding a profile	253
Editing a Profile	254
Delete a Profile	254
Editing a Profile Instance	254
Border Leaf Device Pairing	255

Creating an Edge Router	256
Connect New Border leaf to the Edge Router	256
Deleting Edge Router/Border leaf devices	257
Extended Partitions	257
End Hosts	258
Adding End Hosts	259
Editing End Hosts	259
Deleting End Hosts	259
Endpoint Locator	260
Configuring Endpoint Locator	261
Flushing the Endpoint Database	270
Adding High Availability Node to Endpoint Locator Configuration	272
Configuring Endpoint Locator in DCNM High Availability Mode	272
Disabling Endpoint Locator	273
Troubleshooting Endpoint Locator	273
SAN	275
SAN Zoning	275
Zonesets	276
Zones	277
Zone Members	279
Available to Add	280
Configuring FCIP	281
Device Alias	282
Configuration	283
CFS	284
Port Monitoring	284

CHAPTER 7
Administration 289

DCNM Server	289
Starting, Restarting, and Stopping Services	289
Viewing Log Information	289
Server Properties	290
Configuring SFTP/TFTP Credentials	290
Modular Device Support	292
Managing Switch Groups	292

Adding Switch Groups	292
Deleting a Group or a Member of a Group	293
Moving a Switch Group to Another Group	293
Managing Custom Port Groups	293
Adding Custom Port Groups	293
Configuring Switch and Interface to the Port Group	294
Removing Port Group Member	294
Removing Port Group	295
Managing Licenses	295
Viewing Licenses Using the Cisco DCNM Wizard	295
Automatic License Assignment	297
Adding Cisco DCNM Licenses	297
Assigning Licenses	297
Unassigning Licenses to a Switch	298
Viewing Server Federation	298
Native HA	298
Multi Site Manager	300
Management Users	300
Remote AAA	300
Local	301
Radius	301
TACACS+	301
Switch	302
LDAP	302
Managing Local Users	302
Adding Local Users	303
Deleting Local Users	303
Editing a User	303
User Access	304
Managing Clients	304
Performance Setup	304
Performance Setup LAN Collections	304
Performance Manager SAN Collections	305
Performance Setup Thresholds	305
Configuring the RRD Database	306

Importing the RRD Statistics Index	307
Configuring User Defined Statistics	307
Event Setup	307
Viewing Events Registration	307
Notification Forwarding	308
Adding Notification Forwarding	308
Removing Notification Forwarding	310
Configuring EMC CallHome	310
Event Suppression	310
Add Event Suppression Rules	311
Delete Event Suppression Rule	311
Modify Event Suppression Rule	312

CHAPTER 8

Preview Features 313

Preview Features	313
Compute Visibility	313
Enabling the Compute Visibility Feature	314
Using the Compute Visibility Feature	316
Disabling the Compute Visibility Feature	320
Streaming Telemetry for LAN Deployments	320
Pre-requisites for Enabling the Streaming Telemetry Feature	321
Enabling the Streaming Telemetry Feature	321
Using the Streaming Telemetry Feature	323
Data Visualization For Streaming Telemetry Metrics	327
Memory Data View	327
Power Data View	328
Fan Data View	328
Telemetry Health View	329

CHAPTER 9

Border Provisioning Use Case in VXLAN BGP EVPN Fabrics - Multi-Site 331

Overview	331
Prerequisites	331
Limitations	332
Sample Scenario	332
EVPN Multi-Site Configuration	334

Prerequisite Configuration for EVPN Multi-Site Feature	334
EVPN Multi-Site Extensions from BGW_3 to RS_1	336
Underlay Extension from BGW_3 to RS_1	337
Overlay Extension from BGW_3 to RS_1	345
Other EVPN Multi-Site Configurations	349
Deploying Networks and VRF Instances	350
Deploying Networks on the BGWs	350
Configurations in site1	355
Additional References	356
Appendix	357
Route Server Configurations	357

CHAPTER 10

Border Provisioning Use Case in VXLAN BGP EVPN Fabrics - VRF Lite	359
Prerequisites	359
Sample Scenario	360
VRF Lite Inter-Fabric Configuration	362
Prerequisite Configuration for VRF Lite Configuration	362
VRF Lite Inter-Fabric Configuration (on BL-1 towards ER-1 in 9K-FABRIC)	363
Extension from BL-1 to ER-1	364
VRF Lite Inter-Fabric Configuration (on BL-2 towards ER-1 in 9K-FABRIC)	369
Edge Router Configurations	372
Deploying VRF Instances on Border Leafs	372
Resource Manager	380
Undeploying VRF Instances on the Border Leafs	381
Resource Manager Update	383
Remove VRF Lite Inter-fabric configuration on vPC border leafs	384
Additional References	386
Appendix	386
Edge Router Configurations	386



Dashboard

This section contains context-sensitive Online Help content for the **Web Client > Dashboard** tab.

- [Summary Dashboard, page 1](#)
- [Network Dashboard, page 6](#)
- [Storage Dashboard, page 9](#)
- [Compute, page 15](#)

Summary Dashboard

The intent of the **Summary** dashboard is to enable network and storage administrators to focus on particular areas of concern around the health and performance of data center switching. This information is provided as 24-hour snapshots. The functional view of LAN and SAN switching consists of six dynamic portlets that display information in the context of the selected scope by default. The scope can be adjusted in the upper right corner of the window to display focused information that is particular to the managed domain, and offers details of a specific topology or set of topologies that are a part of the data center scope.

The various scopes that are available on the Cisco Data Center Network Manager (DCNM) Web Client are:

- **Data Center**
- **Default_SAN**
- **Default_LAN**
- Each SAN Fabric
- Custom scopes created by users

From the left menu bar, choose **Dashboard > Summary**. The **Summary** window displays six default set panels:

- **Alarms**—Displays events with **Critical**, **Error**, and **Warning** severity alarms.
- **Data Center**—Displays the number of access, spine and leaf devices, and a generic health score for each switch group in the current scope. Devices are aggregated by type within a switch group.

- **Network Map**—Shows populated switch groups that are visible in a user's Role Based Access Control (RBAC) scope on a world map. If you use the scope selector, it limits the set of switch groups displayed. If you use the pop-up option, the map opens in a new tab and can be configured.

The network map dialog box has properties that are different from the **Summary** dashboard view:

- You can click and drag nodes to move them around the map. The map will save their new positions.
- You can double click a node to trigger a slider that contains summary inventory information pertaining to a specific switch group.
- You can upload an image of your choice as the background to the network map.

**Note**

Users are prompted to upload an image file with recommended dimension, given their current window size. **Reset** returns the network map to its default state, resetting the position of the nodes and clearing the custom image.

- **Link Traffic**—Displays a diagram of inter-switch link and link saturation for transmitting and receiving in the data center.
- **Audit Log**—Displays the accounting log table of DCNM.
- **Server Status**—Displays the DCNM and federation servers' status and the health check status for the components.

Click the **Dashlets** drop-down list, you can choose to view the following portlets on the **Summary** dashboard other than the six default panels:

- [Viewing Top ISLs/Trunks Summary](#)
- [Viewing Top SAN End Ports \(SAN only\) Summary](#)
- [Viewing Top CPU Summary](#)
- [Viewing Health Summary](#)
- [Viewing Inventory \(Ports\) Summary](#)
- [Viewing Inventory \(Modules\) Summary](#)
- [Viewing Inventory \(ISLs\) Summary](#)
- [Viewing Inventory \(Logical\) Summary](#)
- [Viewing Inventory \(Switches\) Summary](#)
- [Viewing Inventory \(Port Capacity\) Summary](#)

The panels can be added, removed and dragged around to re-order.

Viewing Top ISLs/Trunks Summary

You can view the top Inter-switch Links(ISLs) or trunks' summary information by following bellow steps:

Procedure

-
- Step 1** From the menu bar, choose **Dashboard > Summary**.
- Step 2** From the **Dashlets** drop-down list, choose **Top ISLs/Trunks**.
The **Top ISLs/Trunks** area is displayed on the left side of the window.

This area displays the performance data for the top 10 performing ISLs, trunk ports or both. Each entry shows the current average receive and transmit percentage, with a graph depicting the percentage of time each trunk spent exceeding the currently configured thresholds, see the [Performance Setup Thresholds, on page 305](#).
- Step 3** To view all this information in a new window, click the **Detach** icon in the upper-right corner of the **Top ISLs/Trunk** area.
- Step 4** Click the bar graph on the left of each entry, a 24-hour graph for the selected item is displayed. A context to the performance data is displayed as well.
-

Viewing Top SAN End Ports (SAN only) Summary

You can view the top SAN end ports summary information by following bellow steps:

Procedure

-
- Step 1** From the menu bar, choose **Dashboard > Summary**.
- Step 2** From the **Dashlets** drop-down list, choose **Top SAN End Ports**.
The **Top SAN End Ports** area is displayed on the left side of the window.

This area displays the performance data for the top 10 performing SAN host and storage ports. Each entry shows the current receive and transmit percentage, with a graph depicting the percentage of time each trunk spent exceeding the currently configured thresholds, see the [Performance Setup Thresholds, on page 305](#).
- Step 3** To view all the information in a new window, click the **Detach** icon in the upper-right corner of the **Top SAN End Ports** area.
- Step 4** Click the bar graph on the left of each entry, a 24-hour graph for the selected item is displayed. A context to the performance data is displayed as well.
-

Viewing Top CPU Summary

You can view the top CPU summary information by following bellow steps:

Procedure

-
- Step 1** From the menu bar, choose **Dashboard > Summary**.
- Step 2** From the **Dashlets** drop-down list, choose **Top CPU**.

The **Top CPU** area is displayed on the left side of the window.

This area displays CPU utilization for the discovered switches over the last 24 hours, with a red bar displaying the high watermark for that 24-hour period.

- Step 3** Click the bar graph on the left of each entry, a 24-hour graph for the selected item is displayed. A context to the performance data is displayed as well.
-

Viewing Health Summary

You can view the health summary information by following bellow steps:

Procedure

- Step 1** From the menu bar, choose **Dashboard > Summary**.
- Step 2** From the **Dashlets** drop-down list, choose **Health**.
The **Health Summary** area is displayed on the left side of the window. This contains two columns displaying the summary of problems and summary of events for the past 24 hours.
- Step 3** Click the **Count** adjacent the **Warnings** pertaining to switches, ISLs, hosts, or storage (other than 0) to view the corresponding inventory for that fabric.
- Step 4** Click the **Count** adjacent the event severity levels (**Emergency, Alert, Critical, Error, Warning, Notice, Info, or Debug**) to view a summary of the corresponding events and descriptions.
-

Viewing Inventory (Ports) Summary

You can view the ports inventory summary information by following bellow steps:

Procedure

- Step 1** From the left menu bar, choose **Dashboard > Summary**.
The **Summary** dashboard is displayed.
- Step 2** From the **Dashlets** drop-down list on the upper-right corner, choose **Inventory (Ports)**.
The category of the ports and the number of ports are displayed.
-

Viewing Inventory (Modules) Summary

You can view the modules inventory summary information by following bellow steps:

Procedure

- Step 1** From the menu bar, choose **Dashboard > Summary**.
 - Step 2** Click the **Dashlets** on the upper right corner, and select **Inventory (Modules)**.
The modules panel displays the switches on which the modules are discovered, the models name and the count.
-

Viewing Inventory (ISLs) Summary

You can view the Inter-switch links(ISLs) inventory summary information by following bellow steps:

Procedure

- Step 1** From the menu bar, choose **Dashboard > Summary**.
 - Step 2** Click the **Dashlets** on the upper right corner, and select **Inventory (ISLS)**.
You see the ISLs panel displaying the category and count of ISLs.
-

Viewing Inventory (Logical) Summary

You can view the logical inventory summary information by following bellow steps:

Procedure

- Step 1** From the menu bar, choose **Dashboard > Summary**.
 - Step 2** Click the **Dashlets** on the upper right corner, and select **Inventory (Logical)**.
You see the **Logical** panel displaying the category and count of logical links.
-

Viewing Inventory (Switches) Summary

You can view the switches inventory summary information by following bellow steps:

Procedure

- Step 1** From the menu bar, choose **Dashboard > Summary**.
- Step 2** Click the **Dashlets** on the upper right corner, and select **Inventory (Switches)**.

You see the switches panel displaying the switch models and the corresponding count.

Viewing Inventory (Port Capacity) Summary

You can view the port capacity inventory summary information by following bellow steps:

Procedure

- Step 1** From the menu bar, choose **Dashboard > Summary**.
- Step 2** Click the **Dashlets** on the upper right corner, and select **Inventory (Port Capacity)**.
You see the tiers, the number and percentage of the available ports, and the remaining days.
-

Network Dashboard

Cisco DCNM Web Client enables you to view details of switches including system information, switch capacity, modules, interfaces, and licenses.

Procedure

- Step 1** To access the **Network** dashboard, from the left menu bar, choose **Dashboard > Network**.
An inventory of all the switches that are discovered by Cisco DCNM Web Client is displayed.
The following table describes the fields that appear on this page.

Field	Description
Group	Displays the group name of the switch.
Device Name	Displays the name of the switch.
IP Address	Displays the IP address of the switch.
WWN/Chassis Id	Displays the World Wide Name (WWN) if available or chassis ID.
Health	Displays the health situation of the switch.
Status	Displays the status of the switch.
# Ports	Displays the number of ports.
Model	Displays the model name of the switch.

Field	Description
Serial No	Displays the serial number of the switch.
Release	Displays the switch version.
License	Displays the DCNM license installed on the switch.
Up Time	Displays the up time of the switch.

Step 2 Click on a switch in the **Device Name** column to view the [Switch Dashboard](#), on page 7.

Switch Dashboard

The switch dashboard displays the details of the selected switch.

Procedure

Step 1 From the left menu bar, choose **Dashboard > Network**. Alternatively, choose **Inventory > View > Switches**. An inventory of all the switches that are discovered by Cisco Prime DCNM Web Client is displayed.

Step 2 Click a switch in the **Device Name** column.
The **Switch** dashboard that corresponds to that switch is displayed along with the following information:

- **System Info**—Displays detailed system information such as the group name, health, module, the time when system is up, the serial number, the version number, contact, location, DCNM license, status, system log sending status, CPU and memory utilization, and VTEP IP address are displayed. Click **Health** to access the Health score screen, which includes health score calculation and health trend. The popup contains Overview, Modules, Switch Ports, and Events tabs.
 - (Optional) Click **SSH** to access the switch through Secure Shell (SSH).
 - (Optional) Click **Device Manager** to view a graphical representation of a Cisco MDS 9000 Family switch chassis, a Cisco Nexus 5000 Series switch chassis, a Cisco Nexus 7000 Series switch chassis, or a Cisco Nexus 9000 Series switch chassis including the installed switching modules, the supervisor modules, the status of each port within each module, the power supplies, and the fan assemblies.
 - (Optional) Click **HTTP** to access the switch through Hypertext Transfer Protocol (HTTP) for that switch.
 - (Optional) Click **Accounting** to go to the [Viewing Accounting Information](#), on page 66 window pertaining to this switch.
 - (Optional) Click **Backup** to go to the Viewing a Configuration window.
 - (Optional) Click **Events** to go to the [Viewing Events Registration](#), on page 307 window.
 - (Optional) Click **Show Commands** to display the device show commands. The Device Show Commands page helps you to view commands and execute them.

- (Optional) Click **Copy Running Config to Startup Config** to copy the running configuration to the startup configuration.

- **Modules**—Displays detailed modules discovered on the switch.
 - **Interfaces**—Displays all the interfaces that are discovered for the switch. Select multiple items and click **Port Group** to create a new port group or add the interfaces into an existing group.
 - **FEX**—Allows you to manage a Cisco Nexus 2000 Series Fabric Extender and its association with the Cisco NX-OS switch. You can create or modify FEX for the LAN devices by using this feature. The FEX feature is available only on LAN devices. If a Cisco Nexus switch is discovered as part of the SAN fabric, the FEX feature will not be available. The FEX feature is also not supported on Cisco Nexus 1000V devices.
 - **License**—Displays detailed information about the licenses installed on the switches.
 - **Features**—Displays all the enabled features.
 - **VXLAN**—Displays VXLANs and their details such as status, mode, multicast address, and mapped VLAN.
 - **VLAN**—Allows you to manage VLANs. You can add, edit, delete, and shutdown VLANs.
 - **Port Capacity**—This feature is available for Cisco DCNM-licensed switches only. The physical port capacity area includes the available ports in each tier, such as 40G, 10G, 8G, 4G, 2G, and 1G along with the predicted number of days remaining to reach the maximum (100%) utilization. Click a number under the **Days Left** left column to view the capacity trend.
 - **VDC**—Allows you to create and manage VDCs. As Cisco DCNM supports Cisco Nexus 7000 Series only, click an active Cisco Nexus 7000 switch. After you create a VDC, you can change the interface allocation, VDC resource limits, and the high availability (HA) policies.
 - **Switch On-Board Analytics**—Displays the switch on-board analytics charts containing the following information:
 - Top 10 Slowest Ports
 - Top 10 Slowest Target Ports
 - Top 10 Slowest Flows
 - Top 10 Slowest ITLs
 - Top 10 Port Traffic
 - Top 10 Target Ports Traffic
 - Top 10 Flow Traffic
 - Top 10 ITL Traffic
-

Storage Dashboard

The **Storage** dashboard provides information about the SAN and LAN storage.

To access the **Storage** dashboard, from the left menu bar, choose **Dashboard > Storage**.

Viewing Storage Enclosures Information

After a datasource is configured and the discovery is completed, the discovered storage systems are displayed under the **Name** column in the **Storage Enclosures** area. In this area, you can view details of SAN Storage Enclosures, Storage Systems, or both.

Procedure

-
- Step 1** From the left menu bar, choose **Dashboard > Storage**.
 - Step 2** From the **Show** drop-down list, choose **SAN Storage Enclosures**.
 - Step 3** Select the row to view more details.
You see the Events, Topology and Traffic information in the dashboard.
 - Step 4** Click the **Filter** icon to filter the storage enclosures by **Name** or by **IP Address**.
 - Step 5** In the **Traffic** pane, the **Enclosure Traffic** is displayed by default. Click the **Traffic Utilization** icon to view the traffic utilization. The daily average percentage of traffic utilization of the enclosure ports is displayed as a pie chart.
Clicking on an individual port slice of the pie chart will display specific traffic utilization details for that port.
-

Viewing Storage Systems Information

Procedure

-
- Step 1** From the left menu bar, choose **Dashboard > Storage**.
 - Step 2** From the **Show** drop-down list, choose **Storage Systems**.
 - Note**
 - The datasource must be configured and discovered at least once to display the discovered storage system(s). For more information, see [Adding, editing, removing, rediscovering and refreshing SMI-S Storage](#), on page 59.
 - Cisco DCNM now differentiate Block Storage and Filer Storage in terms of what it discovers and displays. Filer storage has additional elements: Shares, Quotas and Q-trees.
 - Shares—Individual storage folders on the file server to which users have access.
 - Quotas—File and repository size limitations.
 - Q-trees—Tree based quotas. By using Q-trees, you can partition data and take advantage of different backup strategies, security styles, and settings.

Step 3 Click the **Click to see more details...** icon to view the storage systems summary.

Step 4 The following are the elements of the **Storage Systems** area:

Components

Components are containers for a set or sub-set of the disks in a storage system. The Component elements view displays a table of the disks in the collection, total number of disks managed and a summary of the collection's used vs. raw space.

Procedure

Step 1 Use the Storage System drop-down to select the storage system.

Step 2 The right-hand pane displays a summary of the storage components. Click each name to go to the item in the left menu

Step 3 Hover the mouse cursor on the graph to display its details.

Step 4 In the left-hand pane, select the storage component to view its details.
The number of disks managed along with its details are displayed.

Step 5 Click a Serial Number to display the disk and the mapped LUNs details.

Step 6 You can use the search box to search for a specific component.

Pools

Pools are user-defined collections of LUNs displaying the pool storage. The pools elements view displays a summary of the pools, lists the LUNs in the pool and also displays the total managed and raw space.

Procedure

Step 1 Use the Storage System drop-down to select the storage system.
The bar graph next to each pool indicates the total managed space of that pool.

Step 2 In the left-hand pane, select a pool to display:

- Status of the pool
- LUN's in the pool displaying the total raw space and the total managed space.
- Raid Type
- Disk Type
- Details of the LUNs in the pool

Step 3 You can use the search box to search for a specific pool.

LUNs

LUNs refer to a storage volume or a collection of volumes abstracted into a single volume. It is a unit of storage which can be pooled for access protection and management. Each LUN in the LUN Element View is displayed along with the mapping from Hosts to LUNs. If the associated Fabric has also been discovered, additional information concerning the end-to-end connection between a host and LUN is also displayed.

You are able to create and delete LUNs, create and delete host and LUN maps, and create zoning for HLMs.

Procedure

Step 1 Use the Storage System drop-down to select the storage system.

Step 2 You can create LUN from Cisco DCNM **Web Client** > **Storage** > **LUNs**.

a) In the middle pane, click Add LUN icon.

b) Enter a valid **Name** for the LUN, and select its **Type** and **Size**. The pool which we carve the storage from is indicated.

Note The Create LUN popup can also be accessed from a Pool's details page, when the LUN list view is selected.

c) Click **Add**.

A confirmation window will display each step. Once confirmed, the status will update with the results of each step.

After LUN creation completes successfully, the user can then Assign Hosts, or click Close and assign Hosts later from the LUN Details view.

Step 3 Select a LUN in the left navigation pane to view the details.

- The LUN details along with its status and the number of Associated Hosts.
- The Host LUN Mapping details along with the Access (Granted) information.

If the associated Fabric has also been discovered, additional information about the switch interfaces and zoning concerning the end-to-end connection between the Host and LUN is also displayed.

Note All fabrics that are discovered must be licensed or the fabric correlation will be disabled in the Web Client. When the feature is disabled, all correlation fields display "Unlicensed Fabric".

Step 4 You can delete LUNs in the SMI-S Storage Enclosure.

a) Navigate to **Storage** > **Storage System** > **LUNs**.

A list of LUNs in the SMI-S Storage Enclosure is displayed in the right-hand window.

b) Select one LUN from the list and then click **Remove**.

A confirmation window will display each step. Once confirmed, the status will update with the results of each step.

c) Click **Apply**.

Step 5 You can add mapping from Host to LUN.

a) Select the **LUNs** from the left-hand pane.

A list of LUNs in the SMI-S Storage Enclosure is displayed in the right-hand window.

b) Select a LUN from the list underneath.

The details for the selected LUN are displayed, including the current Host LUN Mappings for that LUN.

c) Click the **Add** button.

The **Add Hosts to Mask** window pops out.

- d) Select one or more Hosts, and then click **Add**. The Hosts are then added to the LUN Mapping. In addition, each HLM pair will be zoned if it is not already zoned.

Note Host LUN Mappings can also be added via the Host Dashboard. See [Viewing Host Enclosures, on page 15](#), for more information.

Step 6 You can remove mapping from Host to LUN.

- a) Select the **LUNs** from the left-hand pane.
A list of LUNs in the SMI-S Storage Enclosure is displayed in the right-hand window.
- b) Select a LUN from the list underneath.
The details for the selected LUN are displayed, including the current Host LUN Mappings for that LUN.
- c) Select one or more existing Host LUN Mappings and click the remove icon.
A confirmation window appears and displays each step.
- d) Click **Apply**.
The status will update with the results of each step.

Step 7 (Optional) You can add Zoning to the LUNs.

- a) Select the **LUNs** from the left-hand pane.
A list of LUNs in the SMI-S Storage Enclosure is displayed in the right-hand window.
- b) Select a LUN from the list underneath.
The details for the selected LUN are displayed, including the current Host LUN Mappings for that LUN. One of the columns of the **Host LUN Mapping** table identifies the existing zone(s) if any of the HLM currently has for zoning.
- c) Select one or more HLMs which have Unknown or None for zoning, and click **Add Zoning**.
- d) Click **Apply**.
The status will update with the results of each step.

Filer Volumes

Filer Volumes are applicable only for NetApp. The Filer Volume Element view displays the Status, Containing Aggregate along with the total capacity and used space.

Procedure

Step 1 Use the Storage System drop-down to select the storage system.

Step 2 In the left-hand pane, select the filer to display:

- The status of the filer along with the containing aggregate name.
- Hover the mouse cursor over the graph to view the total capacity and available storage of the filer.

Step 3 You can use the search box to search for a specific Filer.

Hosts

The Hosts only describes the NWWN(s) associated with a host or host enclosure along with the associated Host LUN Mapping and the Host Ports. If the associated Fabric has also been discovered, additional information concerning the end-to-end connection between a host and LUN is also displayed.

Procedure

Step 1 Use the Storage System drop-down to select the storage system.

Step 2 In the left-hand pane, select a host to display:

- The NWWN (Node WWN) is the WWN of the device connected to the switch.
- The Host Ports along with the Host LUN Mapping.
- In the Host Ports section, click a Host Enclosure Name to view its Events, Topology and SAN Traffic. For more information see the [Storage Dashboard, on page 9](#) section.
- In the Host Ports sections, click a Host Interface to view the [Switch Dashboard, on page 7](#).
- In the Host LUN Mapping section, click a Storage Interface to view the [Switch Dashboard, on page 7](#).
- In the Host LUN Mapping section, click a Storage Name to view its Events, Topology and SAN Traffic. For more information see the [Storage Dashboard, on page 9](#) section.

If the associated Fabric has also been discovered, additional information about the switch interfaces and zoning concerning the end-to-end connection between the Host and LUN is also displayed.

Note All fabrics that are discovered must be licensed or the fabric correlation will be disabled in the Web Client. When the feature is disabled, all correlation fields display “Unlicensed Fabric”.

Step 3 You can use the search box to search for a specific host.

Storage Processors

Storage Processors are elements on a storage system, which enable some of its features. A storage processor includes the collection of Storage Ports it manages. In the Storage Processor Element View, the list of Storage Ports associated with a Storage Processor is displayed.

Procedure

Step 1 Use the Storage System drop-down to select the storage system.

Step 2 In the left-hand pane, select a storage processor to display:

- The status, adapter details and the number of ports of the storage processor.
- The storage ports details.

Step 3 You can use the search box to search for a specific storage processor.

Storage Ports

A storage port is a single port on the Storage System. It displays the summary information of each port selected.

Procedure

- Step 1** Use the Storage System drop-down to select the storage system.
 - Step 2** In the left-hand pane, select a storage port to display its details.
 - Step 3** You can use the search box to search for a specific storage port.
-

Viewing Storage Enclosure Events

Procedure

- Step 1** From the menu bar, choose **Dashboard > Storage**. Use the drop-down to select All, SAN Storage Enclosures or Storage Systems.
You see the list of storage enclosures in the table.
 - Step 2** Click the **Events** icon next to the storage enclosure to view the Events panel.
 - Step 3** You can use the slider control to resize the panel.
-

Viewing Storage Enclosure Topology

Procedure

- Step 1** From the menu bar, choose **Dashboard > Storage**. Use the drop-down to select All, SAN Storage Enclosures or Storage Systems.
You see the list of storage enclosures in the table.
 - Step 2** Select the row to view the topology details.
 - Step 3** Use the mouse scroll wheel to zoom-in and zoom-out.
 - Step 4** Click the **Fabric/Network** icon to view the Fabric/Network path.
 - Step 5** Click the **All Paths** icon to view the complete set-up.
 - Step 6** Click the **First Shortest Path** icon to view the shortest path.
- Note** Click **Map View** icon to enable the icons listed in Step 4, 5 and 6 above.

Step 7 Click the **Tabular View** icon to view the host topology in tabular format.

Viewing Storage Enclosure Traffic

Procedure

- Step 1** From the menu bar, choose **Dashboard > Storage**. Use the drop-down to select All, SAN Storage Enclosures or Storage Systems.
You see the list of storage enclosures in the table
- Step 2** Select the row to view the topology details.
- Step 3** Use the drop-down to select the traffic according to the time duration.
- Step 4** Select the icons to view the traffic as a **Grid**, **Line Chart** or **Stacked Chart**.
- Step 5** Click the **Show Events** icon to view the events.
- Step 6** Use the options at the bottom of the screen to view a pie chart or a line chart. Click on each name on the chart to view its details.
-

Compute

The compute dashboard provides you with all the information related to the discovered SAN and LAN hosts. It provides 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 compute dashboard consists of four panels:

- **Host Enclosures** panel—Lists the hosts and their network attributes.
- **Traffic** 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 discovered virtual machines are displayed and when you select the virtual machine, the path to the SAN data source is displayed. You can toggle this view to list all data paths.
- **Event** panel—Provides information about events of all of the switch ports that are configured within a specific host enclosure.

This section contains the following topics:

Viewing Host Enclosures

Beginning with Cisco NX-OS Release 6.x, you can view and search the network servers that are connected to the Cisco NX-OS devices. Cisco DCNM extends the fabric visibility up to the server and allows you to discover and search the end devices that are attached to the network.

**Note**

Beginning with Cisco NX-OS Release 6.x, Server Credentials, Servers, and Static Server-Adapter Mapping are no longer available.
Beginning from Cisco DCNM Release 10.1, you are able to assign storage to hosts.

Procedure

-
- Step 1** From the menu bar, choose **Dashboard > Compute**.
You see the list of hosts in the host enclosures table.
- Step 2** Select the row to view more details.
You see the Events, topology and Traffic information in the dashboard.
- Step 3** To edit the host name, you can select the row and click the **Rename** icon. Enter the new name in the pop-out dialog.
Note Specifying a blank name will cause the server to default the name.
- Step 4** To assign storage to host, you can select the row and click the **Assign** icon next to the Rename icon. The **Assign Storage to Host** window pops out. The selection of Host will be by enclosure, and multiple selection of LUN(s) is allowed. Once you click **assign**, a confirmation window will display each step. Once confirmed, the status will update with the results of each step.
- Step 5** Click on **Quick Filter** drop down to filter **host** enclosures (not storage) by **LAN, SAN and Virtual**.
-

Viewing Host Events

Procedure

-
- Step 1** From the menu bar, choose **Dashboard > Compute**.
You see the list of hosts in the host enclosures table.
- Step 2** Click the **Events** icon next to the host enclosure to view the Events panel.
- Step 3** You can use the slider control to resize the panel.
-

Viewing Host Topology

Procedure

-
- Step 1** From the menu bar, choose **Dashboard > Compute**.
You see the list of hosts in the host enclosures table

- Step 2** Select the row to view the host topology details.
 - Step 3** You can use the mouse scroll wheel to zoom-in and zoom-out.
 - Step 4** Click the **Fabric/Network** icon to view the fabric and network path.
 - Step 5** Click the **All Paths** icon to view the complete set-up.
 - Step 6** Click the **First Shortest Path** icon to view the first shortest path.
Note Click **Map View** icon to enable the icons listed in step 4, 5 and 6 above.
 - Step 7** Click the **Tabular View** icon to view the host topology in tabular format.
 - Step 8** Click the **Custom Port Group** icon to view the custom port group.
-

View Host Traffic

Procedure

- Step 1** From the menu bar, choose **Dashboard > Compute**.
You see the list of hosts in the host enclosures table
 - Step 2** Select the row to view the host topology details.
 - Step 3** Use the drop-down to select the traffic according to the time duration.
 - Step 4** Select the icons to view the traffic as a **Grid**, **Line Chart** or **Stacked Chart**.
 - Step 5** In the **Traffic** pane, the **Enclosure Traffic** is displayed by default. Click the **Traffic Utilization** icon to view the traffic utilization. The daily average percentage of traffic utilization of the enclosure ports is displayed as a pie chart.
-



Topology

This section contains context-sensitive Online Help content for the **Web Client > Topology** tab.

- [Topology, page 19](#)

Topology

The topology window shows color encoded nodes and links that correspond to various network elements including switches, links, fabric extenders, port-channel configurations, virtual port-channel, and more. For each of the elements, you can hover over to fetch some more information. Additionally, by clicking on the node for a switch or line for a link, a slide-out panel flies out from the right. This panel shows more detailed information about either the switch or link. Multiple tabs can be opened simultaneously and are intended to function side-by-side for comparison and troubleshooting.

Status

The color encoding of each node and link corresponds to its state. The color states are:

- **Green**—Indicates the element is in good health and functioning as intended.
- **Yellow**—Element is in warning state and requires attention to prevent any further problems.
- **Red**—Element is in critical state and requires immediate attention.
- **Gray**—Indicates lack of information to properly identify the element or the element has just been discover.

Scope

You can search the topology based on the scope. The default scopes available from the **SCOPE** drop-down list are: **DEFAULT_LAN** and **DEFAULT_SAN**. The search options differ based on the chosen scope.

The following search options are available for **DEFAULT_LAN**:

- Quick Search

- Tags
- Host name (VDP)
- Host name (vCenter)
- Host IP
- Host MAC
- Segment ID
- Multicast Group
- VXLAN ID (VNI)
- VLAN
- VSAN ID/Name
- FabricPath
- VXLAN OAM

The following search options are available for **DEFAULT_SAN**:

- Quick Search
- Tags
- VLAN
- VSAN ID/Name

For more information about these search options, see [Searching, on page 20](#).

Searching

When the node number is large, it quickly becomes hard to find the intended switches and links. You can quickly find switches and links by performing a search. You are also able to search for VM tracker and generic setups. Searching feature enables you to see which leaf the host is connected to.

The following searches are available:

Quick Search

Enables you to search for devices by *name*, *IP address*, *mode*, *serial number*, and *switch role*. This search returns immediately and results are highlighted as the user types.

To perform a search for multiple nodes and links, you can separate multiple keywords by a comma.

For example, one search might look like: *ABCD12345, N7K, sw-dc4-12345, core, 172.23.45.67*. Wildcards are also supported.

If you partially know a serial number or name, you can build a search like so: *ABCD*, sw*12345, core, *23.45.**.

If you want to limit your scope to a particular field, you can for example do: *name=sw*12345, serialNumber=ABCD12345*.

The following fields are available to search on: **Name**, **ipAddress**, **serialNumber**, **model**, and **switchRole**. This search is applicable to both the default LAN and SAN scopes.

Tags

Tagging is a very powerful and easy way to organize and provide a "shared-thread" across your various switches. To search by tags, simply click on the tags and results will be filtered to match your selected tag(s).

Tagging supports two logical operations:

- **OR-ing**—selects all switches that match any of the selected tags.
- **AND-ing**—selects all switches that match all of the selected tags.

This search is applicable to both the default LAN and SAN scopes.

Host name (VDP)

Enables you to search for hosts by using VDP.

Host name (vCenter)

Enables you to search for hosts by using vCenter.

Host IP

Search will go and talk to your switches in the scope to find any hosts (VMs or bare metal) that match your given IP address.

The Host IP search supports both IPv4 and IPv6 addresses.

Host MAC

Search will go and talk to your switches in the scope to find any hosts (VMs or bare-metal) that match your given MAC address.

Segment ID

Search will go and talk to your switches in the scope to find any hosts (VMs or bare-metal) that match your given segment ID.

Multicast Group

Search by a given multicast group.

**Note**

Multicast group is limited to VXLAN context (VTEP switches) for searching the switches to get VNIs associated with this multicast address. Click the **Details** link next to the search box to get the detailed multicast address table. The table displays the switches which have searched Multicast address configured on them along with associated VNI, VNI status and mapped VLAN.

VXLAN ID (VNI)

Search by a given VNI. Click the **Details** link next to the search box to get the detailed VNI table. The table displays the switches which have searched VNI configured on them along with associated multicast address, VNI status and mapped VLAN.

VLAN

Search by a given VLAN ID. VLAN search provides the search for the VLAN configured on the switch or the links. If STP is enabled, then it provides information related to STP protocol and the STP information for links.

This search is applicable to both the default LAN and SAN scopes.

VSAN ID/Name

Search by a given VSAN ID. VSAN search provides the search for VSAN configured on the switch or the links. In order to view the STP details associated with the VSAN, click on **STP Details** link.

This shows the STP details, if STP is enabled. If the link is blocked, it is marked as red, green in case of forwarding link and Orange if the link is blocked for one VSAN range and forwarding for the other VSAN range.

This search is applicable to both the default LAN and SAN scopes.

FabricPath

Search on the FabricPath topology ID, typically 0 or 1. After search, FabricPath topology links are displayed with purple colored links. You can use the **FabricPath Panel** below the search box to fetch various FabricPath graphs.

Click the drop-down arrow next to **FabricPath Panel**, select below type of graph:

- **Multi destination**—Select the switch from the **Anchor** drop-down list, and select the graph ID from the **Graph ID** drop-down list to get multi destination or broadcast graph.
- **Reachability**—Select the switch in the **From** drop-down list to get the reachable devices in FabricPath topology from the selected switch.
- **Unicast**—Select the switch from the **Source** and **Destination** drop-down list to get equal cost multi paths from source to destination switch in FabricPath topology.
- **Multicast**—Select from the **Anchor**, **Ftag ID** and **IGMP Addr** drop-down list to get the FabricPath multicast tree. The selected anchor switch is the root of the tree.

VXLAN OAM

You can track details such as reachability and actual path of the flows in a VXLAN EVPN based-fabric topology by choosing the **VXLAN OAM** option from the **Search** drop-down list or by entering **VXLAN OAM** in the **Search** field. This displays the **Switch to switch** and **Host to host** tabs. DCNM highlights the route on the topology between the source and destination switch for these two options.

The **Switch to switch** option provides the VXLAN OAM ping and traceroute test results for the VTEP-to-VTEP use-case. Provide the following values to enable search by using the **Switch to switch** option:

- From the **Source Switch** drop-down list, choose the source switch.
- From the **Destination Switch** drop-down list, choose the destination switch.
- From the **VRF** drop-down list, choose or enter the VRF details.
- Check the **All Path Included** check box to include all the paths in the search results.

The **Host to host** option provides the VXLAN OAM pathtrace results for the exact path taken by a given flow from the VTEP or switch that is connected to the source host to VTEP or switch that is connected to the destination host. For the **Host to host** use-case, there are two suboptions:

- VRF or SVI for a network is instantiated on the switches in the VXLAN EVPN fabric. In such a scenario, the IP address information of the end hosts is required.
- Layer 2 configuration for a given network is instantiated on the switches in the VXLAN EVPN fabric. In such a scenario, both the MAC and IP address information of the end hosts are required.

Provide the following values to enable search using the **Host to host** option:

- In the **Source IP** field, enter the IP address of the source host.
- In the **Destination IP** field, enter the IP address of the destination host.
- In the **VRF** field, choose VRF from the drop-down list or enter the VRF name that is associated with the hosts.
- (Optional) In the **Source Port** field, choose Layer 4 source port number from the drop-down list or enter its value.
- (Optional) In the **Destination Port** field, choose destination port number or enter its value.
- (Optional) In the **Protocol** field, choose the protocol value from the drop-down list or enter its value. This is the Layer 4 protocol, usually TCP or UDP.
- Click the **Interchange/Swap Source and Destination IPs (and MACs if applicable)** icon to interchange the source and destination IP addresses. This interchange allows a quick trace of the reverse path without re-entering the host IP addresses or MAC addresses.
- Check the **Layer-2 only** check box to search the VXLAN-EVPN fabric that is deployed in Layer 2 only mode for some networks, that is, Layer 2 VNIs. Note that no SVIs or VRFs should be instantiated in the fabric for these networks when you use this search option.

Enter values for the following additional fields:

- In the **Source MAC** field, enter the MAC address of the source host.
- In the **Destination MAC** field, enter the MAC address of the destination host.

- In the **VNI** field, choose the Layer 2 VNI from the drop-down list or enter the appropriate Layer 2 VNI value corresponding to the network to which the hosts belong.

Show Panel

You can choose to view your topology based on the options below:

- **Auto Refresh**—Check the check box to automatically refresh the topology.
- **Switch Health**—Check the check box to show the switch health status.
- **FEX**—Check the check box to show the Fabric Extender.

FEX feature is available on LAN devices only. Therefore, checking this check box will display only the Cisco Nexus Switches that support FEX.



Note

If a Cisco Nexus Switch is discovered as part of SAN fabric, FEX feature is not available. FEX is also not supported on Cisco Nexus 1000V devices. Therefore, such devices will not be displayed in the topology when you check the FEX check box.

- **Links**—Check the check box to show links in the topology. The following options are available:
 - **Errors Only**—Click this radio button to display only links with errors.
 - **All**—Click this radio button to display all links in the topology.
 - **VPC Only**—Check this check box to display only vPC peer-links and vPCs.
 - **Bandwidth**—Check this check box to show the color coding based on the bandwidth consumed on links.
- **OTV**—Check the check box to show Overlay Transport Virtualization (OTV) topology with cloud icon and dotted links from the OTV edge devices. Hovering the mouse over the cloud and links shows the relevant information for OTV topology such as control group, extended VLANs, etc. The OTV search box appears below the filter box which can be used to search the shown OTV topology based on **Overlay ID** and **Extended VLAN ID**. Searched virtual links based on the **Overlay ID** and **Extended VLAN ID** are marked green.

A **Details** link appears after checking the **OTV** box. Clicking the links shows the OTV topology data. The **Overlay Network** column shows whether the particular topology is multicast or unicast based. The **Edge Device** column gives the edge switches in the particular OTV topology. Other columns give the corresponding overlay interface, extended VLANs, join interface and data group information.
- **UI controls**—Check the check box to show or hide the various controls on the topology screen.
- **Refresh**—You can also perform a topology refresh by clicking the refresh icon in the upper right of this panel.

Layouts

The topology supports various different layouts as well as a **Save Layout** option which remembers how you positioned your topology.

- **Hierarchical/Hierarchical Left-Right**—Provides an architectural view of your topology. Various Switch Roles can be defined that will draw the nodes on how you configure your CLOS topology.

**Note**

When running a large scale setup, being able to easily view all your switches on a leaf-tier can become difficult. To mitigate this, DCNM will split your leaf-tier every 16 switches.

- **Random**—Nodes will be placed randomly on the screen. DCNM will try to make a guess and intelligently place nodes that belong together in close-proximity.
- **Circular/Tiered-Circular**—Draws nodes in a circular or concentric circular pattern.
- **Custom saved layout**—You can drag nodes around to your liking. Once you have the positions as how you like, you can click the save button to remember the positions. Next time you come to the topology, DCNM will draw the nodes based on your last saved layout positions.

Before a layout is chosen, DCNM checks if a custom layout is applied. If a custom layout is applied, DCNM uses it. If a custom layout is not applied, DCNM checks if switches exist at different tiers, and chooses Hierarchial layout or Hierarchial Left-Right layout. Force-directed layout is chosen if all other layouts fail.

Zooming, Panning and Dragging

You can zoom-in and zoom-out using the controls provided at the bottom left of the screen or using the mouse wheel.

To pan, click and hold anywhere in the whitespace and drag up, down, left, or right.

To drag switches, click, hold, and move around in the whitespace region of the topology.

Switch Slide-Out Panel

You can click on the switch to display the configured switch name, IP address, switch model, and other summary information like status, serial number, health, last polled CPU utilization, and last polled memory utilization.

Switch Roles

Various switch roles can be defined on the switch. When you set a role, the topology will be refreshed to reflect the role that was assigned. Switch roles are great for defining architectural views such as the hierarchy represented by CLOS topologies. You can set the switch role based on your network topology.

**Note**

This configuration is not pushed to the device. It is only a DCNM construct to help with rendering and organization.

Beacon

This button will only be shown for switches that support the beacon command. Once the beaconing starts, the button will show a countdown. By default, the beaconing will stop after 60 seconds but you can stop it immediately by clicking **stop beacon**.

**Note**

The default time can be configured in `server.properties`. Search for `beacon.turnOff.time`. The time value here is in milliseconds. Note that this requires a server restart to take effect.

Tagging

Tagging is a very powerful yet easy way to organize your switches. Tags can be virtually any string and an example of tags includes: *building 6, floor 2, rack 7, problem switch* and *Justin debugging*.

You can use the search to perform searches based on tags.

More Details

Click on **Show more details** and the detailed information pops out [Switch Dashboard, on page 7](#).

Link Slide-Out Panel

You can click on a link to view the status and the port or switches that describe the link.

24 Hour Traffic

This feature requires **Performance Monitoring** be turned **ON**. When **Performance Monitoring** is **ON**, traffic information is collected and aggregate information is displayed along with a graph showing the traffic utilization.



Inventory

This section contains context-sensitive Online Help content for the **Web Client > Inventory** tab.

- [Viewing Inventory Information, page 27](#)
- [Discovery, page 53](#)

Viewing Inventory Information

Beginning with Cisco Prime DCNM release 6.x, you can view the inventory and the performance for both SAN and LAN switches by using the global Scope pane. You can select LAN, SAN, or both to view the inventory information. You can also export and print the inventory information.

You can either Print this information or export to Microsoft Excel.



Note

You can use the **Print** icon to print the information displayed or you can also use the **Export** icon to export the information displayed to a Microsoft Excel spreadsheet. You can also choose the column you want to display.

The Inventory menu includes the following submenus:

Viewing Inventory Information for Switches

Procedure

- Step 1** From the menu bar, choose **Inventory > View > Switches**.
You see the **Switches** window displaying a list of all the switches for a selected Scope.
- Step 2** You can also view the following information.
 - In the **Device Name** column, select a switch to display the [Switch Dashboard, on page 7](#). For more information about switch dashboard, see the [Switch Dashboard, on page 7](#) section.
 - **IP Address** column displays the IP address of the switch.

- **WWN/Chassis ID** displays the World Wide Name (WWN) if available or chassis ID.
- **Health** displays the health situation of the switch.
- **Status** column displays the status of the switch.
- **# Ports** column displays the number of ports.
- **Model** column displays the model name of the switch.
- **Serial No.** column displays the serial number of the switch.
- **Release** column displays the switch version.
- **License** column displays the DCNM license installed on the switch.

Step 3 In the **Health** column, the switch health is calculated by the capacity manager based on the following formula in the server.properties file.
The function to implement is

```
# calculate(x, x1, y, y1, z)
# @param x: Total number of modules
# @param x1: Total number of modules in warning
# @param y: Total number of switch ports
# @param y1: Total number of switch ports in warning
# @param z: Total number of events with severity of warning or above
```

Step 4 The value in the **Health** column is calculated based on the following default equation.

$$((x-x1)*1.0/x) * 0.4 + ((y-y1)*1.0/y)*0.3 + ((z*1.0/1000 \geq 1) ? 0 : ((1000-z)*1.0/1000)*0.3).$$

In the above formula, the switch health value is calculated based on the following:

- Percentage of Warning Modules (Contributes 40% of the total health).
- Percentage of Warning Ports (Contributes 30% of the total health)
- Percentage of events with severity of Warning or above (Contributes 30% of the total health. If there are more than 1000 warning events, the event health value is 0).

You may also have your own health calculation formula by implementing the common interface class: com.cisco.dcbu.sm.common.rif.HealthCalculatorRif. Add the .jar file to the DCNM server and modify the health.calculator property to point to the class name you have created.

The default Java class is defined as: health.calculator=com.cisco.dcbu.sm.common.util.HealthCalculator.

- Capacity Manager calculates health only for the license switches. If the health column does not display a value, the switch either does not have a license or it has missed the capacity manager's daily cycle.
- If the switch is unlicensed, in the DCNM License column click **Unlicensed**. The **Administration > License** window appears which allows you to assign a license to the user.
- The capacity manager runs two hours after the DCNM server starts. So, if you discover a device after two hours of the DCNM start time, the health will be calculated 24 hours after this DCNM start time

Interfaces

The Interfaces tab displays all the interfaces that are discovered for the switch. You can view interface information such as the interface name, admin status, operation status, reason, policy, speed, MTU, Mode, VLANs, IP/Prefix, VRF, PC, Neighbor, and Description.

The Interface tab is based on the port selected on the device view and only works with the device view.

The VMIS range is from 1 to 255. This range is same at interface and VSAN.

You can configure interfaces on **Inventory > View > Switches**.

The following table describes the buttons that appear on this page.

Field	Description
Clear Selections	Allows you to unselect all the interfaces that you selected.
Add	Allows you to add a logical interface
Edit	Allows you to edit an interface.
Delete	Allows you to delete a logical interface.
No Shutdown	Allows you to enable an interface.
Shutdown	Allows you to disable an interface.
Show	Allows you to display the interface show commands.
Rediscover	Allows you to rediscover the selected interfaces.
Interface History	Allows you to display the interface history details.

This section contains the following:

Adding Interfaces

Procedure

- Step 1** From the menu bar, choose **Inventory > View > Switches**.
You see the Switches window displaying a list of all the switches for a selected Scope.
- Step 2** In the Device Name column, select a switch to display the Switch Dashboard.
- Step 3** Click the **Interfaces** tab.
- Step 4** Click **Add** to add a logical interface. The Add Interface window appears.
If you want to add a subinterface, you need to select an interface and then click Add.

- Step 5** In the **Type** field, choose the type of the interface. For example, VLAN, loopback, NVE.
- Step 6** In the **Number** field, specify the interface number.
- Step 7** Select the **Admin State ON** check box to specify whether the interface is shutdown or not.
-

Editing Interfaces

Procedure

- Step 1** From the menu bar, choose **Inventory > View > Switches**.
You see the Switches window displaying a list of all the switches for a selected Scope.
- Step 2** In the Device Name column, select a switch to display the Switch Dashboard.
- Step 3** Click the **Interfaces** tab.
- Step 4** Click **Edit** to edit an interface. The variables shown in the Edit Configuration window are based on the template and its policy.
- The Admin State ON check box in the Edit Configuration window indicates whether the interface is shutdown or not.
 - The Clear Config prior to deployment check box helps you to set a port to its default configuration. That is, when there is a set of configurations already available on the port and these configurations conflict with the configurations that want to place on the port, you may need to clear the configurations prior to deployment.
 - In the Preview window, the left pane shows the configurations that the template generated based on your input, whereas the right pane shows the configurations that are currently available on the switch.
-

Deleting Interfaces

Procedure

- Step 1** From the menu bar, choose **Inventory > View > Switches**.
You see the Switches window displaying a list of all the switches for a selected Scope.
- Step 2** In the Device Name column, select a switch to display the Switch Dashboard.
- Step 3** Click the **Interfaces** tab.
- Step 4** Click **Delete** to add a logical interface.
-

Shutting Down Interfaces

Procedure

- Step 1** From the menu bar, choose **Inventory > View > Switches**.
You see the Switches window displaying a list of all the switches for a selected Scope.
- Step 2** In the Device Name column, select a switch to display the Switch Dashboard.
- Step 3** Click the **Interfaces** tab.
- Step 4** Click **Shutdown** to disable an interface. For example, you may want to isolate a host from the network or a host that is not active in the network.
To enable an interface, Click **No Shutdown** button.
-

Displaying Interface Show Commands

Procedure

- Step 1** From the menu bar, choose **Inventory > View > Switches**.
You see the Switches window displaying a list of all the switches for a selected Scope.
- Step 2** In the Device Name column, select a switch to display the Switch Dashboard.
- Step 3** Click the **Interfaces** tab.
- Step 4** Click **Show** to display the interface show commands. The Interface Show Commands page helps you to view commands and execute them.
-

Rediscovering Interfaces

Procedure

- Step 1** From the menu bar, choose **Inventory > View > Switches**.
You see the Switches window displaying a list of all the switches for a selected Scope.
- Step 2** In the Device Name column, select a switch to display the Switch Dashboard.
- Step 3** Click the **Interfaces** tab.
- Step 4** Click **Rediscover** to rediscover the selected interfaces. For example, after you edit or enable an interface, you can rediscover the interface.
-

Viewing Interface History

Procedure

-
- Step 1** From the menu bar, choose **Inventory > View > Switches**.
You see the Switches window displaying a list of all the switches for a selected Scope.
- Step 2** In the Device Name column, select a switch to display the Switch Dashboard.
- Step 3** Click the **Interfaces** tab.
- Step 4** Click **Interface History** to display the interface history details such as Policy Name, Time of Execution etc.
-

HBA Link Diagnostics

The HBA Link Diagnostics feature helps in validating the health of links between Host Bus Adapters (HBAs) and Cisco MDS switches in a network. The servers connect to Storage Area Networks (SANs) through hardware devices called HBAs. This connectivity comprises of many optical and electrical components that may develop faults during their lifetime. The HBA Link Diagnostics feature allows identification of faulty cables, transceivers, ASICs, drivers, firmware issues or software issues, thereby eliminating dropped frames and ensuring reliable I/O operations of the server.

For more information about the Configuring HBA Link Diagnostics for Cisco MDS switches in a network, see the [Cisco MDS 9000 Series NX-OS System Management Configuration Guide](#).

From the menu bar of Cisco DCNM Web Client, choose **Inventory > Switches**, and then click the **Interfaces** tab. The HBA diagnostic button appears in the interfaces tab for SAN discovered switches. Click the HBA diagnostic button to launch Host Diagnostic. The Link Diagnostic screen appears.

Supported Platforms

Cisco DCNM 10.4(1) enables you to run HBA Link Diagnostics on the following platforms:

- Cisco MDS 48-Port 16-Gbps Fibre Channel Switching Module: DS-X9448-768K9
- Cisco MDS 48-Port 32-Gbps Fibre Channel Switching Module: DS-X9648-1536K9
- Cisco MDS 24/10 SAN Extension Module (FC ports only): DS-X9334-K9
- Cisco MDS 9396S Multilayer Fabric Switch

Getting Loopback Capabilities

The **Get Loopback Capabilities** button is disabled when you click the Start button. The Loopback Capabilities button is to be used before clicking the Start button to see the capabilities of port or HBA.

Aborting Link Diagnostic Tests on a Port

If you want to stop the link diagnostic test, click the **Stop** button in the Link Diagnostic screen.

Disabling a Port From the Diagnostic Mode

You can click the **Disable Diagnostic** button for taking the port out of diagnostic mode when you have finished the testing.

Monitoring the Running Diagnostic Test

You can click the **Monitor existing Diag** button to begin monitoring a test that is already running. If no test is running, then you will be informed of this and Cisco DCNM will attempt to retrieve the results from the last test that ran and display them. If the port has already been taken out of diagnostic mode then retrieving of the results will fail and a message will be printed.

Displaying Diagnostic Test Results

If the **Show Results during polling** check box is selected, it will output the CLI progress details to the output window for each poll for the test progress. Otherwise results are only printed at test completion.

Performing HBA Link Diagnostic Tests

To run the HBA Host Diagnostic test, perform the following steps:

Procedure

-
- Step 1** From the menu bar, choose **Inventory > Switches**, and then click the **Interfaces** tab. The HBA diagnostic button appears in the interfaces tab for SAN discovered switches. By default, the button is disabled until an interface is selected. However, only one interface can be selected for performing the diagnostic operation. If multiple interfaces are selected, the button will be disabled.
- Step 2** Click the HBA diagnostic button to launch Host Diagnostic. The Link Diagnostic screen appears.
- Step 3** Specify the following fields.
- **Frames: Count**—Generates frames required to conduct the traffic tests. The range is from 1-2147483646. The default is 1000000.
 - **Frames: Duration**—Specifies the duration of the link diagnostics tests per level. The range is from 1-86400.
 - **Frame size: Fixed**—Sets the fixed size for the traffic generated. The minimum frame size is set to 64. The maximum frame size is set to 2048. The step value is set to 100.
 - **Frame size: Random**—Configures the maximum frame size for the traffic generated. The value of frame-size max must be a multiple of four. The range is from 64-2048. The default is 2048.
 - **Payload**—Configures the payload for the traffic generated.
 - **Data Rate**—Configures the rate of the traffic generation of the generator port. The default is 100%. You can select any one of the following line rates at one time:
 - 100%—100% of the line rate
 - 12.5%—12.5% of the line rate
 - 25%—25% of the line rate
 - 50%—50% of the line rate
 - 6.25%—6.25% of the line rate

- Loopback Level—Runs the selected level of the diagnostics test on the diagnostic port. You can select any one of the following levels at a time:
 - Remote XCVR-Optical
 - Remote MAC
 - Remote Electrical
 - Remote All

Step 4 Click the **Start** button.

- When you click the Start button, the port will go offline because of the Diagnostic operation. The test may run for a long time depending upon the settings and therefore you can exit the dialog to perform other operations or to start a test on another port. When you exit the dialog box, the test will continue to run but you cannot continue to monitor the progress. When you return to this dialog for a port that, where you already started a test, you can click on the monitor existing button to begin monitoring the test progress again.

VXLAN

You can view VXLANs and their details under the **VXLAN** tab.

To view VXLANs, choose **Inventory > View > Switches**, and then click a switch name in the **Device Name** column.

The following table describes the fields that are displayed:

Table 1: The VXLAN Tab

Field	Description
VNI	Displays the Layer 2 (network) or Layer 3 (VRF) VXLAN VNI that is configured on a switch.
Multicast address	Displays the multicast address associated with the Layer 2 VNI, if applicable.
VNI Status	Displays the status of the VNI.
Mode	Displays the VNI modes: Control Plane or Data Plane.
Type	Displays whether the VXLAN VNI is associated with a network (Layer 2) or a VRF (Layer 3).
VRF	Displays the VRF name associated with the VXLAN VNI if it is a Layer 3 VNI.

Field	Description
Mapped VLAN	Displays the VLAN or Bridge domain mapped to VNI.

VLAN

You create a VLAN by assigning a number to it; you can delete VLANs and move them from the active operational state to the suspended operational state.

To configure VLANs, choose **Inventory > View > Switches**, and then click a switch in the Device Name column.

The following table describes the buttons that appear on this page.

Table 2: VLAN Tab

Field	Description
Clear Selections	Allows you to unselect all the VLANs that you selected.
Add	Allows you to create Classical Ethernet or Fabric Path VLANs.
Edit	Allows you to edit a VLAN.
Delete	Allows you to delete a VLAN.
No Shutdown	Allows you to enable a VLAN.
Shutdown	Allows you to disable a VLAN.
Show	Allows you to display the VLAN show commands.

This section contains the following:

Adding a VLAN

Procedure

- Step 1** From the menu bar, choose **Inventory > View > Switches**.
You see the Switches window displaying a list of all the switches for a selected Scope.

- Step 2** In the Device Name column, select a switch to display the Switch Dashboard.
- Step 3** Click the **VLAN** tab.
- Step 4** Click **Add** to create Classical Ethernet or Fabric Path VLANs. In the Add VLAN window, specify the following fields:
- a) In the **Vlan Id** field, enter the VLAN ID.
 - b) In the **Mode** field, specify whether you are adding Classical Ethernet or Fabric Path VLAN.
 - c) Select the **Admin State ON** check box to specify whether the VLAN is shutdown or not.
-

Editing a VLAN

Procedure

- Step 1** From the menu bar, choose **Inventory > View > Switches**.
You see the Switches window displaying a list of all the switches for a selected Scope.
- Step 2** In the Device Name column, select a switch to display the Switch Dashboard.
- Step 3** Select one or more VLANs, and then click the **Edit** button.
-

Deleting a VLAN

Procedure

- Step 1** From the menu bar, choose **Inventory > View > Switches**.
You see the Switches window displaying a list of all the switches for a selected Scope.
- Step 2** In the Device Name column, select a switch to display the Switch Dashboard.
- Step 3** Click **VLAN** tab.
- Step 4** Select the VLAN that you want to delete, and then click **Delete**.
-

Shutting Down a VLAN

Procedure

- Step 1** From the menu bar, choose **Inventory > View > Switches**.
You see the Switches window displaying a list of all the switches for a selected Scope.

- Step 2** In the Device Name column, select a switch to display the Switch Dashboard.
- Step 3** Click the **VLAN** tab.
- Step 4** Click **Shutdown** to disable a VLAN. For example, if you want to stop traffic on a you can shut the VLAN. To enable a VLAN, click **No Shutdown** button. For example, if you want to start traffic flow on a VLAN you can enable it.
-

Displaying VLAN Show Commands

Procedure

- Step 1** From the menu bar, choose **Inventory > View > Switches**.
You see the Switches window displaying a list of all the switches for a selected Scope.
- Step 2** In the Device Name column, select a switch to display the Switch Dashboard.
- Step 3** Click the **VLAN** tab.
- Step 4** Click **Show** to display the VLAN show commands. Based on the VLAN selection, you can show the VLAN commands. Interface Show Commands page helps users to view commands and execute them.
-

FEX

The Fabric Extender feature allows you to manage a Cisco Nexus 2000 Series Fabric Extender and its association with the Cisco NX-OS switch that it is attached to. A Fabric Extender is connected to the switch through physical Ethernet interfaces or a Port Channel. By default, the switch does not allow the attached Fabric Extender to connect until it has been assigned a chassis ID and is associated with the connected interface. You can configure a Fabric Extender host interface port as a routed or Layer 3 port. However, no routing protocols can be tied to this routed interface.



Note FEX feature is available on LAN devices only. Therefore, you will see FEX on Cisco DCNM **Web Client > Inventory Switches**. If a Cisco Nexus Switch is discovered as part of SAN fabric, FEX feature is not available. FEX is also not supported on Cisco Nexus 1000V devices.



Note 4x10G breakout for FEX connectivity is not supported on Cisco Nexus 9500 Switches.



Note The Fabric Extender may connect to the switch through a number of separate physical Ethernet interfaces or at most one port channel interface.

This section describes how to manage Fabric Extender (FEX) on Cisco Nexus Switches through Cisco DCNM. You can create and manage FEX from Cisco DCNM **Web Client > Inventory > Switches**.

**Note**

FEX tab is visible only if you choose a LAN device.

The following table describes the fields that appear on this page.

Table 3: FEX Operations

Field	Description
Add	Click to add a new FEX to a Cisco Nexus Switch.
Edit	<p>Select any active FEX radio button and click Edit to edit the FEX configuration.</p> <p>You can create an edit template and use it for editing FEX. Select template type as <input type="checkbox"/>POLICY<input type="checkbox"/> and sub type as <input type="checkbox"/>FEX<input type="checkbox"/>.</p>
Delete	Select the FEX radio button, and click Delete icon to delete the FEX associated with the switch.
Show	<p>Allows you to view various configuration details for the selected FEX ID. You can select the following from the drop-down list.</p> <ul style="list-style-type: none"> • show_diagnostic • show_fex • show_fex_detail • show_fex_fabric • show_fex_inventory • show_fex_module <p>The variables for respective show commands are displayed in the Variables area. Review the Variables and click Execute. The output appears in the Output area.</p> <p>You can create a show template for FEX. Select template type as <input type="checkbox"/>SHOW<input type="checkbox"/> and sub type as <input type="checkbox"/>FEX<input type="checkbox"/>.</p>
FEX History	Allows you to view the history of the FEX configuration tasks for a particular FEX. You can review the Event Type, Policy Name, Status, Time of Execution, User Name for the selected FEX.

Table 4: FEX Table Field and Description

Field	Description
Fex Id	Uniquely identifies a Fabric Extender that is connected to a Cisco NX-OS device.

Field	Description
Fex Description	Description configured for the Fabric Extender.
Fex Version	Specifies the version of the FEX associated with the switch..
Pinning	An integer value that denotes the maximum pinning uplinks of the Fabric Extender that will be active at a time.
State	Specifies the status of the FEX as associated with the Cisco Nexus Switch.
Model	Specifies the model of the FEX.
Serial No.	Specifies the configured serial number. Note If this configured serial number and the serial number of the Fabric Extender are not the same the Fabric Extender will not be active.
Port Channel	Specifies the port channel number to which the FEX is physically connected to the Switch.
Ethernet	Refers to the physical interfaces to which the FEX is connected.
vPC ID	Specifies the vPC ID configured for FEX.

This chapter includes the following sections:

Add FEX

To add single-home FEX, perform the steps below.

Before You Begin

Cisco DCNM allows you to add a Fabric Extender (FEX) to the Cisco Nexus Switches through the Cisco DCNM Web Client. If the FEX is physically connected to the switch, FEX will become online after it is added. If the FEX is not physically connected to the switch, the configuration will be deployed to the switch, which in turn will enable FEX when connected.



Note

You can create only single homed FEX through Cisco DCNM **Web Client > Inventory > Switches > FEX > Add FEX**. To create a dual-homed FEX, use the vPC wizard through Cisco DCNM **Web Client > Configure > Deploy > vPC**. For more information, see [Add vPC, on page 121](#).

Ensure that you have successfully discovered LAN devices and configured LAN credentials before you configure FEX.

Procedure

- Step 1** From the menu bar, select **Inventory > Switches > FEX**.
- Step 2** Click **Add FEX** icon.
- Step 3** In the General tab, in the **PORTCHANNEL** field, enter the interface port channel number which is connected to the FEX.
- Step 4** In the **INT_RANGE** field, enter the interface range within which the FEX will be connected to the switch.
Note You must not enter the interface range if the interfaces are already a part of port channel.
- Step 5** In the **FEX_ID** field, enter the ID for FEX that is connected to a Cisco NX-OS device.
The identifier must be an integer value between 100 to 199.
- Step 6** Click **Add**.
The configured Single-home FEX appears in the list of FEXs associated to the device.
-

Edit FEX

To edit and deploy FEX, perform the steps below.

Procedure

- Step 1** From the menu bar, select **Inventory > Switches > FEX**.
- Step 2** Select the FEX radio button that you must edit. Click **Edit FEX** icon.
- Step 3** In the Edit Configuration window, from the Policy drop-down list, select **Edit_FEX** to edit the FEX configuration.
- Step 4** Edit the **pinning** and **FEX_DESC** fields, as required.
Note If you initially configured port 33 on the parent switch as your only fabric interface, all 48 host interfaces are pinned to this port. If you provision another port, for example 35, then you must perform this procedure to redistribute the host interfaces. All host interfaces are brought down and host interfaces 1 to 24 are pinned to fabric interface 33 and host interfaces 25 to 48 are pinned to fabric interface 35.
- Step 5** Click **Preview**.
You can view the generated configuration for the selected FEX ID. The following is a configuration example for FEX ID 101.
- ```
fex 101
pinning max-links 1
description test
```
- Step 6** After you review the configuration summary on the Preview window, on the Edit Configuration screen, click **Deploy** to deploy the FEX for the switch.
-

## VDCs

This section describes how to manage virtual device contexts (VDCs) on Cisco Nexus 7000 Switches through Cisco DCNM.

Users with the network administrator (network-admin) role can create virtual device contexts (VDCs). VDC resource templates limit the amount of physical device resources available to the VDC. The Cisco NX-OS software provides a default resource template, or you can create resource templates.

You can create and manage VDCs from Cisco DCNM **Web Client > Inventory > Switches > VDCs**. As Cisco DCNM supports DCNM on Cisco Nexus 7000 Series only, click on an active Cisco Nexus 7000 Switch. After you create a VDC, you can change the interface allocation, VDC resource limits, and the high availability (HA) policies.

The following table describes the fields that appear on this page.

**Table 5: Vdc Operations**

| Field      | Description                                                                                                                                                                                                                                                                                                                                                          |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add        | Click to add a new VDC.                                                                                                                                                                                                                                                                                                                                              |
| Edit       | Select any active VDC radio button and click Edit to edit the VDC configuration.                                                                                                                                                                                                                                                                                     |
| Delete     | Allows you to edit the VDC configuration. Select any active VDC radio button and click Edit to edit the VDC configuration.                                                                                                                                                                                                                                           |
| Resume     | Allows you to delete the VDC. Select any active VDC radio button and click Delete to remove the VDC associated with the device.                                                                                                                                                                                                                                      |
| Suspend    | <p>Allows you to suspend an active non default VDC.</p> <p>You must save the VDC running configuration to the startup configuration before suspending the VDC. Otherwise, you will lose the changes to the running configuration.</p> <p><b>Note</b> You cannot suspend the default VDC.</p> <p><b>Caution</b> Suspending a VDC disrupts all traffic on the VDC.</p> |
| Rediscover | Allows you to resume a non default VDC from the suspended state. The VDC resumes with the configuration saved in the startup configuration.                                                                                                                                                                                                                          |

| Field | Description                                                                                                                                                                                                                                                                                                                          |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Show  | <p>Allows you to view the Interfaces and Resources allocated to the selected VDC.</p> <p>In the Interface tab, you can view the mode, admin-status and operational status for each interface associated with the VDC.</p> <p>In the Resource tab, you can view the allocation of resources and current usage of these resources.</p> |

**Table 6: Vdc Table Field and Description**

| Field                      | Description                                                                                                                             |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Name                       | Displays the unique name for the VDC                                                                                                    |
| Type                       | <p>Species the type of VDC. The two types of VDCs are:</p> <ul style="list-style-type: none"><li>• Ethernet</li><li>• Storage</li></ul> |
| Status                     | Specifies the status of the VDC.                                                                                                        |
| Resource Limit-Module Type | Displays the allocated resource limit and module type.                                                                                  |



| Field                                                                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HA-Policy <ul style="list-style-type: none"> <li>• Single Supervisor</li> <li>• Dual Supervisor</li> </ul>   | <p>Specifies the action that the Cisco NX-OS software takes when an unrecoverable VDC fault occurs.</p> <p>You can specify the HA policies for single supervisor module and dual supervisor module configurations when you create the VDC. The HA policy options are as follows:</p> <p><b>Single supervisor module configuration:</b></p> <ul style="list-style-type: none"> <li>• Bringdown—Puts the VDC in the failed state. To recover from the failed state, you must reload the physical device.</li> <li>• Reload— Reloads the supervisor module.</li> <li>• Restart—Takes down the VDC processes and interfaces and restarts it using the startup configuration.</li> </ul> <p><b>Dual supervisor module configuration:</b></p> <ul style="list-style-type: none"> <li>• Bringdown—Puts the VDC in the failed state. To recover from the failed state, you must reload the physical device.</li> <li>• Restart—Takes down the VDC processes and interfaces and restarts it using the startup configuration.</li> <li>• Switchover— Initiates a supervisor module switchover.</li> </ul> <p>The default HA policies for a non default VDC that you create is restart for a single supervisor module configuration and switchover for a dual supervisor module configuration. The default HA policy for the default VDC is reload for a single supervisor module configuration and switchover for a dual supervisor module configuration.</p> |
| Mac Address                                                                                                  | Specifies the default VDC management MAC address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Management Interface <ul style="list-style-type: none"> <li>• IP Address Prefix</li> <li>• Status</li> </ul> | Species the IP Address of the VDC Management interface. The status shows if the interface if up or down.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SSH                                                                                                          | Specifies the SSH status                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

This chapter includes the following sections:

## Add VDCs

To add VDC, perform the steps below.

### Before You Begin

Ensure that you have discovered the physical device using a username that has the network-admin role.

Obtain an IPv4 or IPv6 address for the management interface (mgmt 0) if you want to use out-of-band management for the VDC.

You must create a storage VDC to run FCoE. The storage VDC cannot be the default VDC and you can have one storage VDC on the device.

### Procedure

---

**Step 1** From the menu bar, select **Inventory > Switches > VDC**.

**Step 2** Click **Add VDC** icon.

**Step 3** From the drop-down list, select the VDC type.  
You can configure the VDC in two modes.

- Ethernet VDC
- Storage VDC

The default VDC type is Ethernet.

**Step 4** Click **OK**.

---

## Configuring Ethernet VDCs

To configure VDC in Ethernet mode, perform the steps below.

### Procedure

---

**Step 1** In the General Parameter tab, specify the **VDC Name**, **Single supervisor HA-policy**, **Dual supervisor HA-policy**, and **Resource Limit - Module Type**.

**Step 2** In the Allocate Interface tab, select the network interfaces (dedicated interfaces membership) to be allocated to the VDC.  
Click **Next**.

**Step 3** In the Allocate Resource tab, specify the resource limits for the VDC.  
Select the radio button and choose **Select a Template from existing Templates** or **Create a New Resource Template**. VDC resource templates describe the minimum and maximum resources that the VDC can use. If you do not specify a VDC resource template when you create a VDC, the Cisco NX-OS software uses the default template, vdc-default.

- If you choose **Select a Template from existing Templates**, from the **Template Name** drop-down list, you can select **None**, **global-default**, or **vdc-default**.

The template resource limits are detailed in the table below.

**Table 7: Template Resource Limits**

| Resource                                    | Minimum | Maximum                            |
|---------------------------------------------|---------|------------------------------------|
| Global Default VDC Template Resource Limits |         |                                    |
| Anycast Bundleid                            |         |                                    |
| IPv6 multicast route memory                 | 8       | 8<br>Route memory is in megabytes. |
| IPv4 multicast route memory                 | 48      | 48                                 |
| IPv6 unicast route memory                   | 32      | 32                                 |
| IPv4 unicast route memory                   |         |                                    |
| VDC Default Template Resource Limits        |         |                                    |
| Monitor session extended                    |         |                                    |
| Monitor session mx exception                |         |                                    |
| Monitor SRC INBAND                          |         |                                    |
| Port Channels                               |         |                                    |
| Monitor DST ERSPAN                          |         |                                    |
| SPAN Sessions                               |         |                                    |
| VLAN                                        |         |                                    |
| Anycast Bundleid                            |         |                                    |
| IPv6 multicast route memory                 |         |                                    |
| IPv4 multicast route memory                 |         |                                    |
| IPv6 unicast route memory                   |         |                                    |
| IPv4 unicast route memory                   |         |                                    |
| VRF                                         |         |                                    |

- If you choose Create New Resource Template, enter a unique **Template Name**. In the Resource Limits area, enter the minimum and maximum limits, as required for the resources.

You can edit individual resource limits for a single VDC through the Cisco DCNM **Web Client > Inventory > Switches > VDC**.

Click **Next**.

**Step 4** In the Authenticate tab, you can allow the Admin to configure the password and also authenticate users using AAA Server Groups.

In the Admin User Area:

- Check the **Enable Password Strength Check** checkbox, if required.
- In the **Password** field, enter the admin user password.
- In the **Confirm Password** field, reenter the admin user password.
- In the **Expiry Date** field, click the down arrow and choose an expiry date for the admin user from the Expiry Date dialog box. You can also select **Never** radio button to never expire the password.

In the AAA Server Groups area:

- In the **Group Name** field, enter an AAA server group name.
- In the **Servers** field, enter one or more host server IPv4 or IPv6 addresses or names, separated by commas.
- In the **Type** field, choose the type of server group from the drop-down list.

Click **Next**.

**Step 5** In the Management Ip tab, enter IPv4 or IPv6 Address information.

Click **Next**.

**Step 6** In the Summary tab, review the VDC configuration.

Click **Previous** to edit any parameters.

Click **Deploy** to configure VDC on the device.

**Step 7** In the Deploy tab, the status of the VDC deployment is displayed.

A confirmation message appears. Click **Know More** to view the commands executed to deploy the VDC.

Click **Finish** to close the VDC configuration wizard and revert to view the list of VDCs configured on the device.

---

### Configuring Storage VDCs

To configure VDCs in storage mode, perform the steps below.

#### Before You Begin

You must create a separate storage VDC when you run FCoE on the device. Only one of the VDCs can be a storage VDC, and the default VDC cannot be configured as a storage VDC.

You can configure shared interfaces that carry both Ethernet and Fibre Channel traffic. In this specific case, the same interface belongs to more than one VDC. The shared interface is allocated to both an Ethernet and a storage VDC.

## Procedure

- 
- Step 1** In the General Parameter tab, specify the **VDC Name**, **Single supervisor HA-policy**, **Dual supervisor HA-policy**, and **Resource Limit - Module Type**.
- Step 2** In the Allocate FCoE Vlan tab, select the available **Ethernet Vdc** from the drop-down list. The existing Ethernet VLANs range is displayed. Select **None** to not choose any available Ethernet VDCs. You can allocate specified FCoE VLANs to the storage VDC as well as specified interfaces. Click **Next**.
- Step 3** In the Allocate Interface tab, add the dedicated and shared interfaces to the FCoE VDC.  
**Note** The dedicated interface carries only FCoE traffic and the shared interface carries both the Ethernet and the FCoE traffic. You can configure shared interfaces that carry both Ethernet and Fibre Channel traffic. In this specific case, the same interface belongs to more than one VDC. FCoE VLAN and shared interface can be allocated from same Ethernet VDC. Click **Next**.
- Step 4** In the Authenticate tab, you can allow the Admin to configure the password and also authenticate users using AAA Server Groups. In the Admin User Area:
- Check the **Enable Password Strength Check** checkbox, if required.
  - In the **Password** field, enter the admin user password.
  - In the **Confirm Password** field, reenter the admin user password.
  - In the **Expiry Date** field, click the down arrow and choose an expiry date for the admin user from the Expiry Date dialog box. You can also select **Never** radio button to never expire the password.
- In the AAA Server Groups area:
- In the **Group Name** field, enter an AAA server group name.
  - In the **Servers** field, enter one or more host server IPv4 or IPv6 addresses or names, separated by commas.
  - In the **Type** field, choose the type of server group from the drop-down list.
- Click **Next**.
- Step 5** In the Management Ip tab, enter IPv4 or IPv6 Address information. Click **Next**.
- Step 6** In the Summary tab, review the VDC configuration. Click **Previous** to edit any parameters. Click **Deploy** to configure VDC on the device.
- Step 7** In the Deploy tab, the status of the VDC deployment is displayed. A confirmation message appears. Click **Know More** to view the commands executed to deploy the VDC. Click **Finish** to close the VDC configuration wizard and revert to view the list of VDCs configured on the device.
-

## Edit VDC

To edit VDC, perform the steps below.

### Procedure

- 
- Step 1** From the menu bar, select **Inventory > Switches > VDC**.
  - Step 2** Select the VDC radio button that you must edit. Click **Edit** VDC icon.
  - Step 3** Modify the parameters as required.
  - Step 4** After you review the configuration summary on the Summary tab, click **Deploy** the VDC with the new configuration.
- 

## Switch On-Board Analytics

The **Switch On-Board Analytics** dashboard displays the following charts:

- Top 10 Slowest Ports
- Top 10 Slowest Target Ports
- Top 10 Slowest Flows
- Top 10 Slowest ITLs
- Top 10 Port Traffic
- Top 10 Target Ports Traffic
- Top 10 Flow Traffic
- Top 10 ITL Traffic

The following metrics are supported by the Switch On-Board Analytics charts:

- Read and Write Completion Time — Time taken for an IO to complete successfully, that is, the time gap between IO status from a Target and IO command from an Initiator. The following metrics are supported:
  - Read Completion Time Min
  - Read Completion Time Max
  - Write Completion Time Min
  - Write Completion Time Max

The IO engine tracks the maximum and minimum IO completion time for read and write commands in the context of a switch's port, target port, flows, initiators, and LUNs.

- Read and Write Initiation Time — Time taken for an IO to initiate, that is, the time gap between first response packet from a Target and IO Command from Initiator. The following metrics are supported:

- Read Initiation Time Min
- Read Initiation Time Max
- Write Initiation Time Min
- Write Initiation Time Max

The IO engine tracks the maximum and minimum IO initiation time for read and write commands in the context of a switch's port, target port, flows, initiators, and LUNs.

- Read and Write IO Bandwidth — Read and write command bandwidth observed in the context of a switch's port traffic, target port traffic, flow traffic, initiators, and LUNs. The IO bandwidth is computed at every four second time interval based on the number of bytes read or written.
- Read and Write IO Rate — Read and write command IO rate observed in the context of a switch's port traffic, target port traffic, flow traffic, initiators, and LUNs. The IO rate is computed at every four second time interval based on the number of IO performed.
- Read and Write IO Size — Read and write command IO size observed in the context of a switch's port traffic, target port traffic, flow traffic, initiators, and LUNs. The following metrics are supported:
  - Read IO Size Min
  - Read IO Size Max
  - Write IO Size Min
  - Write IO Size Max

The IO engine tracks the maximum and minimum IO size for read and write commands.

## Viewing Switch On-Board Analytics

You can view the switch on-board analytics information by performing these steps:

### Procedure

- 
- Step 1** From the left menu bar, choose **Inventory > View > Switches**.  
An inventory of all the switches that are discovered by Cisco DCNM Web Client is displayed.
  - Step 2** Click a switch name in the **Device Name** column.  
The **Switch** dashboard that corresponds to that switch is displayed.
  - Step 3** Click the **Switch On-Board Analytics** tab.  
This tab displays the Switch On-Board Analytics charts.
- 

## Configuring Settings for the Switch On-Board Analytics Charts

Perform the following actions to configure the settings for the switch on-board analytics charts:

- From the **Show Time** drop-down list, choose time to be shown in the charts. You can choose one of the following options:

- **Microseconds**
- **Milliseconds**
- **Seconds**

By default, **Microseconds** is chosen.




---

**Note** The **Show Time** drop-down list is applicable only for the top 10 slowest ports, target ports, flows, and ITLs.

---

- From the **Show Flow From** drop-down list, choose whether to show flows from a **Target** or from an **Initiator**. By default, flows from a **Target** are chosen.




---

**Note** The **Show Flow From** drop-down list is applicable only for the charts displaying flows and ITLs.

---

- From the **bandwidth and size** drop-down list, choose the traffic information to be shown in the charts. You can choose one of the following options:

- **Bytes**
- **KB**
- **MB**

By default, **Bytes** is chosen.

- Check the **Filter results** check box, and click either the **by fc port** or **by VSAN** radio button and specify the appropriate values to filter the chart results. The FC port value must be in the **fc slot/port** format and the VSAN value must be a digit within the allowed VSAN range.




---

**Note** Filtering results by VSAN is not applicable for the **Top 10 Slowest Ports** or **Top 10 Port Traffic** charts.

---

- Check the **Single Column** check box to display the charts in a single column instead of double columns.
- Click the **Refresh** icon in the upper-right corner to refresh the charts.

## Viewing Switch On-Board Analytics Charts

Perform the following actions to view the charts under the **Switch On-Board Analytics** tab:

- View the charts for the top 10 slowest ports, target ports, flows, and ITLs by choosing one of the following variables from the drop-down list:



- **Read Completion Time** — The read command completion time observed in the context of a switch's port.
- **Write Completion Time** — The write command completion time observed in the context of a switch's port.
- **Read Initiation Time** — The read command initiation time observed in the context of a switch's port.
- **Write Initiation Time** — The write command initiation time observed in the context of a switch's port.

**Note**

- By default, **Read Completion Time** is selected and all the units for time are in **Microseconds**.
- Each chart contains a legend that provides information about the variable displayed. Each variable has a check box. Unselecting the check box removes the variable data from the chart or table.

- View the charts for the top 10 port traffic, target port traffic, flow traffic, and ITL traffic by choosing one of the following variables from the drop-down list:
  - **Read IO Rate** — The read command data observed in the context of a switch's port.
  - **Write IO Rate** — The write command observed in the context of a switch's port.
  - **Read IO Size** — The read command size observed in the context of a switch's port.
  - **Write IO Size** — The write command size observed in the context of a switch's port.
  - **Read IO Bandwidth** — The read command bandwidth observed in the context of a switch's port.
  - **Write IO Bandwidth** — The write command bandwidth observed in the context of a switch's port.

**Note**

- By default, **Read IO Rate** is selected. The **Read IO Rate** is IO per second. Both **Rate** and **Bandwidth** units are per second over an 8-second range. The **Size** value is for the life of the switch or since the last clear command was run from the CLI.
- The **Read IO Size** and **Read IO Bandwidth** units are in bytes per second. You can change this unit by using the **Show Bandwidth and Size** drop down list. You can choose from the three options: **Bytes**, **KB**, and **MB**.
- Each chart contains a legend that provides information about the variable displayed. Each variable has a check box. Unselecting the check box removes the variable data from the chart or table.

- Choose the format to display information from the **Show** drop-down list. You can choose one of the following formats:
  - **Chart**

- **Table**
- **Chart and Table**

**Note**

To display information in the **Chart and Table** format, enlarge your browser window or check the **Single Column** check box on the upper right hand corner.

- Use the **Chart Type** drop-down list to display information in the **Bar Chart** or **Stacked Bar Chart**.
- Use the **Actions** drop-down list to export information in a CSV or PDF, or print the required information.
- To view a chart or a table in a new window, click the **Detach** icon on the upper-right corner of a chart or a table.

## Viewing Inventory Information for Modules

### Procedure

- 
- Step 1** From the menu bar, choose **Inventory > View > Modules**.  
You see the **Modules** window displaying a list of all the switches and its details for a selected Scope.
- Step 2** You can view the following information.
- **Group** column displays the group name of the module.
  - **Switch** column displays the switch name on which the module is discovered.
  - **Name** displays the module name.
  - **ModelName** displays the model name.
  - **SerialNum** column displays the serial number.
  - **2nd SerialNum** column displays the second serial number.
  - **Type** column displays the type of the module.
  - **Slot** column displays the slot number.
  - **Hardware Revision** column displays the hardware version of the module.
  - **Software Revision** column displays the software version of the module.
  - **Asset ID** column displays the asset id of the module.
-

## Viewing Inventory Information for Licenses

### Procedure

---

- Step 1** From the menu bar, choose **Inventory > View > Licenses**.  
You see the **Licenses** window displaying the license type and the warnings, based on the selected Scope.
- Step 2** You can view the following information.
- **Group** column displays the group name of switches.
  - **Switch** column displays the switch name on which the feature is enabled.
  - **Feature** displays the installed feature.
  - **Status** displays the usage status of the license.
  - **Type** column displays the type of the license.
  - **Warnings** column displays the warning message.
- 

## Discovery

Starting from Cisco DCNM release 10.x, Cisco DCNM Web Client allows the **admin** to associate **user** to one or more device scope or group. That means you can only access and configure the associated group or scope devices based on Role Based Access Control (RBAC). Even though you might not have the access to other users' associated devices, you can still see all the discovered devices under the **Inventory > Discovery** tab.

From the left menu bar, go to **Administration > Management Users**. You can create users and associate groups, manage remote authentication and see all the connected clients. For more information about RBAC, please go to [Managing Local Users](#).

## Adding, Editing, Re-discovering, Purging and Removing LAN, LAN Tasks and Switch

Cisco DCNM Web Client reports information obtained by the Cisco DCNM-LAN devices.



### Tip

If the discovered Device is not in the scope of the current user the check box for the LAN Device in the LAN table greys out.

This section contains the following:

## Adding LAN Switches

### Procedure

- 
- Step 1** From the menu bar, choose **Inventory > Discovery > LAN Switches**.  
You see the list of LAN devices in the **Switch** column.
- Step 2** Click on the **Add** icon to add LAN.  
You see the **Add LAN Devices** dialog box.
- Step 3** Select **Hops from seed Switch** or **Switch List**. The fields vary depending on your selection.
- Step 4** Enter the **Seed Switch** IP address for the fabric.  
For LAN Switches Discovery, DCNM allow both IPv4 and IPv6 address for the Seed Switch.
- Step 5** The options vary depending on the discovery type selected. For example, if you check **Use SNMPv3/SSH**, varied fields are displayed.
- Step 6** Click the drop-down menu and choose the **Auth-Privacy** security level.
- Step 7** Enter the **Community**, or user credentials.
- Step 8** Select the LAN group from the LAN groups candidates which is in the scope of the current user.  
**Note** Select DCNM server and click **Add** to add LAN switches.
- Step 9** Click **Next** to begin the shallow discovery.
- Step 10** In the **LAN Discovery** window, you can select all switches by using the checkbox next to the switch name column or select individual switches. Click Previous to go back and edit the parameters.  
**Note** In the Status column, if the switch status is **timeout** or **Cannot be contacted**, these switches cannot be added. Only the switches that are reachable and not managed yet are available to select. The checkbox is greyed out for the switches that are not available.
- Step 11** Select a switch and click **Add** to add a switch to the switch group.  
If the seed switch(es) are not reachable, it will be shown as "unknown" on the shallow Discovery window.
- 

## Editing LAN Devices

You can modify a LAN from Cisco DCNM Web Client.

### Procedure

- 
- Step 1** From the menu bar, choose **Inventory > Discovery > LAN Switches**.
- Step 2** Select the check box next to the LAN that you want to edit and click **Edit** icon.  
You see the **Edit LAN** dialog box.
- Step 3** Enter the **User Name** and **Password**.  
**Note** Select **Credential** or **Management State** to change the Credential or Management state. If **Credential** is selected, you can change the SNMP version and Auth-Privacy if v3, username or password. If **Management State** is selected, you can change the status to managed or unmanaged.

- Step 4** Select the LAN status as Managed or Unmanaged.
  - Step 5** Click **Apply** to save the changes.
- 

## Removing LAN Devices from Cisco DCNM

You can remove a LAN switch from Cisco DCNM Web Client.

### Procedure

---

- Step 1** From the menu bar, choose **Inventory > Discovery > LAN Switches**.
  - Step 2** Select the check box next to the LAN that you want to remove and click the move icon to remove the switches and all their data.
  - Step 3** Click **Yes** to review the LAN device.
- 

## Moving LAN Devices Under a Task

You can move LAN devices under a task to a different server using Cisco DCNM Web Client. This feature is available only in the federation setup and the Move LAN is displayed in the federation setup screen.

You can move the LAN from a sever that is down to an active server. The management state remains the same.

### Procedure

---

- Step 1** From the menu bar, choose **Inventory > Discovery > LAN Switches**.
  - Step 2** Choose the LAN Devices(s) from the LAN table. Click **Move**.
  - Step 3** In the **Move LAN Tasks to another DCNM Server** dialog box, enter the LAN Device that need to be moved and specify the DCNM server.  
All the LAN devices under the selected tasks will be moved.
- 

## Re-discover LAN Task

### Procedure

---

- Step 1** From the menu bar, choose **Inventory > Discovery > LAN Switches**.
  - Step 2** Click the rediscover LAN icon.
  - Step 3** Click **Yes** in the pop-up window to re-discover the LAN.
-

## Purging LAN

You can clean and update the LAN discovery table through **Purge**.

### Procedure

---

- Step 1** From the menu bar, choose **Inventory > Discovery > LAN Switches**.
- Step 2** Click the Purge unreachable devices or dead links in selected LAN icon.
- Step 3** Click **Yes** in the pop-up window to purge the LAN device.
- Note** In case of a federation set-up, you will have to select the LAN to purge.
- 

## Adding, Editing, Re-discovering, Purging and Removing Managed Fabrics

Cisco DCNM Web Client reports information obtained by the Cisco DCNM-SAN on any fabric known to Cisco DCNM-SAN.

This section contains the following:

### Adding a Fabric

You can discover new fabric and start managing a fabric from Cisco DCNM Web Client. Before you discover a new fabric, ensure you create a SNMP user on the switch.

### Procedure

---

- Step 1** From the menu bar, choose **Inventory > Discovery > SAN Switches**.  
You see a list of fabrics (if any) managed by Cisco DCNM-SAN in the Opened column.
- Step 2** Click on the **Add** icon to add a new fabric.  
You see the **Add Fabric** dialog box.

- Step 3** Enter the **Fabric Seed Switch** IP address for this fabric.
- Step 4** (Optional) Check the SNMPV3 check box. If you check SNMPV3, the field **Community** change to **Username** and **Password**.
- Step 5** Enter the **User Name** and **Password** for this fabric.
- Step 6** Select the privacy settings from the **Auth-Privacy** drop-down list.
- Step 7** (Optional) Check the **Limit Discovery by VSAN** checkbox to specify the included VSAN list or excluded VSAN list from the VSANs provided to discover a new fabric.
- Step 8** (Optional) Check the **Enable NPV Discovery in all Fabrics** check box. If you check enable NPV discovery in all fabrics, the changes are applied to all the fabrics that are previously discovered.
- Step 9** Click **Options** button and specify the **UCS User Name** and **UCS Password**.
- Step 10** Click **Add** to begin managing this fabric.
- You can remove single or multiple fabrics from the Cisco DCNM Web Client.
- 

## Deleting a Fabric

### Procedure

---

- Step 1** From the menu bar, choose **Inventory > Discovery > SAN Switches**.
- Step 2** Select the check box next to the fabric that you want to remove and click **Delete** fabric icon to remove the fabric from the datasource and to discontinue data collection for that fabric.
- 

## Editing a Fabric

### Procedure

---

- Step 1** From the menu bar, choose **Inventory > Discovery > SAN Switches**.
- Step 2** Select the check box next to the fabric that you want to edit and click on the **Edit** icon. You see the **Edit Fabric** dialog box. You can edit only one fabric at a time.
- Step 3** Enter a new fabric **Name**.
- Step 4** (Optional) Check the SNMPV3 check box. If you check SNMPV3, the **Community** field change to **Username** and **Password**.
- Step 5** Enter the **User Name** and **Password**, privacy and specify how you want DCNM Web Client to manage the fabric by selecting one of the status options.
- Step 6** Change the fabric management state to **Managed**, **Unmanaged**, or **Managed Continuously**.
- Step 7** Click **Apply** to save the changes.
- Note** In the **Inventory > Discovery > SAN Switches**, select the fabric for which the fabric switch password is changed. Click **Edit**, unmanage the fabric, specify the new password and then manage the fabric. You will not be able to open the fabric as the new password will not sync with the database. To open the fabric, you can go to **Configure > SAN > Credentials** to sync the password.

---

## Moving Fabrics to Another Server Federation

This feature is only available on the federation setup and the Move Fabric is only displayed in the federation setup screen.

You can move the fabrics from a sever that is down to an active server. The management state will remain the same.

### Procedure

---

- Step 1** From the menu bar, choose **Inventory > Discovery > SAN Switches**.
  - Step 2** Select the switch that need to be moved from the switches table and click **Move**.
  - Step 3** In the **Move Fabrics to another Federation server** dialog box, select the DCNM server where the fabrics will be moved. The server drop-down list will list only the active servers.
- 

## Rediscovering a Fabric

### Procedure

---

- Step 1** From the menu bar, choose **Inventory > Discovery > SAN Switches**.
  - Step 2** Select the check box next to the fabric and click the **Rediscover** icon.
  - Step 3** Click **Yes** in the pop-up window.  
The **Fabric** will now be re-discovered.
- 

## Purging a Fabric

You can clean and update the fabric discovery table through the **Purge** option.

### Procedure

---

- Step 1** From the menu bar, choose **Inventory > Discovery > SAN Switches**.
  - Step 2** Select the check box next to the fabric and click the **Purge** fabric icon.
  - Step 3** Click **Yes** in the pop-up window.  
The **Fabric** will now be purged.
-



## Adding, editing, removing, rediscovering and refreshing SMI-S Storage

The SMI-S providers are managed using the Cisco DCNM Web Client.

This section contains the following:

### Adding SMI-S Provider

#### Procedure

- 
- Step 1** From the menu bar, choose **Inventory > Discovery > Storage Devices**.
- Step 2** Click the **Add SMI-S** provider icon.
- Step 3** In the **Add SMI-S Provider** window, use the drop-down to select the **Vendor**.  
All the supported vendor can be found in the drop-down list. Additional SMI-S storage vendors are discovered through a 'best effort' handler using the **Other** vendor option in the drop-down.
- Note** At least one valid DCNM license must be provisioned before adding SMI-S storage discovery data sources.
- Step 4** Specify the **SMI-S Server IP**, **User Name** and **Password**.
- Step 5** Specify the **Name Space** and **Interop Name Space**.
- Step 6** By default, the **Port** number is pre-populated.  
If you select the **Secure** checkbox, then the default secure port number is populated.  
  
When using the **Secure** mode with EMC, the default setting is mutual authentication. For more information, see EMC's documentation about adding an SSL certificate to their trust store, or set SSLClientAuthentication value to *None* in the *Security\_Settings.xml* configuration file and then restart the ECOM service.
- Step 7** Click **Add**.  
The credentials are validated and if it's valid the storage discovery starts. If the credential check fails, you will be prompted to enter valid credentials.
- 

### Deleting SMI-S Provider

#### Procedure

- 
- Step 1** From the menu bar, choose **Inventory > Discovery > Storage Devices**.
- Step 2** Use the check-box to select the SMI-S provider and click the **Delete** icon.  
The provider is removed and all data associated with the provider is purged from the system.
-

## Editing SMI-S Provider

### Procedure

- 
- Step 1** From the menu bar, choose **Inventory > Discovery > Storage Devices**.
  - Step 2** Use the check-box to select the SMI-S provider and click the **Edit** SMI-S provider icon.
  - Step 3** In the **Edit SMI-S Provider** window, use the drop-down to select the **Vendor**.
  - Step 4** Specify the **SMI-S Sever IP**, **User Name** and **Password**.
  - Step 5** Specify the **Name Space** and **Interop Name Space**.
  - Step 6** By default, the **Port** number is pre-populated.  
If you select the **Secure** checkbox, then the default secure port number is populated.
  - Step 7** Click **Apply**.  
The storage discovery is stopped and a new task is created using the new information and the storage discovery is re-started.
- 

## Re-Discover SMI-S Provider

### Procedure

- 
- Step 1** From the menu bar, choose **Inventory > Discovery > Storage Devices**.
  - Step 2** Use the check-box to select the SMI-S provider and click the **Rediscover** SMI-S provider icon.
- 

## Purge SMI-S Provider

### Procedure

- 
- Step 1** From the menu bar, choose **Inventory > Discovery > Storage Devices**.
  - Step 2** Use the check-box to select the SMI-S provider and click the **Purge** icon.  
The providers are purged.
- 

## Adding, Editing, Re-discovering and Removing VMware Servers

Cisco DCNM Web Client reports information gathered by Cisco DCNM-SAN on any VMware servers supported by Cisco DCNM-SAN.

**Note**

Ensure that the LAN and SAN are discovered before you add the vCenter on the datasource.

This section contains the following:

## Adding a Virtual Center Server

You can add a virtual center server from Cisco DCNM Web Client.

### Procedure

- Step 1** From the menu bar, choose **Inventory > Discovery > Virtual Machine Manager**.  
You see the list of VMware servers (if any) that are managed by Cisco DCNM-SAN in the table.
- Step 2** Click the **Add** icon.  
You see the **Add VCenter** dialog box.
- Step 3** Enter the **Virtual Center Server** IP address for this VMware server.
- Step 4** Enter the **User Name** and **Password** for this VMware server.
- Step 5** Click **Add** to begin managing this VMware server.

## Deleting a VMware Server

You can remove a VMware server from the Cisco DCNM Web Client.

### Procedure

- Step 1** From the menu bar, choose **Inventory > Discovery > Virtual Machine Manager**.
- Step 2** Select the check box next to the VMware server that you want to remove and click **Delete** to discontinue data collection for that VMware server.

## Editing a VMware Server

You can edit a VMware server from Cisco DCNM Web Client.

### Procedure

- Step 1** From the menu bar, choose **Inventory > Discovery > Virtual Machine Manager**.
- Step 2** Check the check box next to the VMware server that you want to edit and click **Edit** virtual center icon.  
You see the **Edit VCenter** dialog box.

**Step 3** Enter a the **User Name** and **Password**.

**Step 4** Select managed or unmanaged status.

**Step 5** Click **Apply** to save the changes.

---

## Rediscovering a VMware Server

You can rediscover a VMware server from Cisco DCNM Web Client.

### Procedure

---

**Step 1** From the menu bar, choose **Inventory > Discovery > Virtual Machine Manager**.

**Step 2** Select the check box next to the VMware that you want to rediscover.

**Step 3** Click **Rediscover** virtual center icon.

**Step 4** Click **Yes** in the dialog box.

---



## CHAPTER 4

# Monitor

---

This section contains context-sensitive Online Help content for the **Web Client > Monitor** tab.

- [Monitoring Switch, page 63](#)
- [Monitoring SAN, page 67](#)
- [Monitoring LAN, page 76](#)
- [Monitoring Report, page 80](#)
- [Monitoring Configuration, page 83](#)
- [Exploring Endpoint Locator Details, page 86](#)

## Monitoring Switch

The Switch menu includes the following submenus:

### Viewing Switch CPU Information

#### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Switch > CPU**.  
You see the CPU pane. This pane displays the CPU information for the switches in that scope.
  - Step 2** You can use the drop-down to filter the view by 24 Hours, Week, Month and Year.
  - Step 3** In the **Switch** column, click the switch name to view the [Switch Dashboard, on page 7](#).
  - Step 4** Click the chart icon in the **Switch** column to view the CPU utilization. You can also change the chart timeline to 24 hours, Week, Month and Year. You can choose the chart type and chart options to show as well.
-

## Viewing Switch Memory Information

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Switch > Memory**.  
You see the memory panel. This panel displays the memory information for the switches in that scope
- Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.
- Step 3** Click the chart icon in the **Switch** column to see a graph of the memory usage of the switch.
- Step 4** In the **Switch** column, click the switch name to view the [Switch Dashboard, on page 7](#).
- Step 5** You can use the drop-down to view the chart in different time lines. Use the chart icons to view the memory utilization chart in varied views.
- 

## Viewing Switch Traffic and Errors Information

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Switch > Traffic**.  
You see the **Switch Traffic** panel. This panel displays the traffic on that device for the past 24 hours.
- Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.
- Step 3** To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.
- Step 4** Click the switch name to view the Switch Dashboard section..
- 

## Viewing Switch Temperature

Cisco DCNM includes the module temperature sensor monitoring feature, using which you can view the sensor temperature of a switch. You can choose an interval by which to filter the sensor list. The default interval is **Last Day**. Note that only sensors that have historical temperature data will be shown in the list. You can choose between Last 10 Minutes, Last Hour, Last Day, Last Week, and Last Month.



### Note

It is not necessary to configure the LAN or SAN credentials under the **Configure > Credentials Management > LAN Credentials** screen to fetch the temperature monitoring data from the switches.

---

### Procedure

---

- Step 1** From the menu, choose **Monitor > Switch > Temperature**. The **Switch Temperature** window is displayed with the following columns.

- **Scope**—The sensor belongs to a switch, which is part of a fabric. The fabric it belongs to is shown as its scope. When the scope selector at the top of Cisco DCNM is used, the sensor list is also filtered by that scope.
- **Switch Name**—Name of the switch the sensor belongs to.
- **IP Address**—IP Address of the switch.
- **Temperature Module**—The name of the sensor module.
- **Avg/Range**—The first number is the average temperature over the interval specified at the top of the table. The second set of numbers is the range of the temperature over that interval.
- **Peak**—The maximum temperature over the interval

**Step 2** From this list, each row has a chart icon, which you can click. This brings up a chart in the lower portion of the page, which shows historical data for the sensor. The interval for this chart can be changed as well, between 24 hours, 1 week, and 1 month.

---

## Enabling Temperature Monitoring

You can enable the temperature monitoring feature for LAN switches from the LAN Collections screen, and for the SAN switches by setting a few properties under Administration > DCNM Server > Server Properties screens.

### Enabling Temperature Monitoring for LAN Switches

- 1 From the menu bar, choose **Administration > Performance Setup > LAN Collections**.
- 2 Select the **Temperature Sensor** check box.
- 3 Select the type(s) of LAN switches for which you want to collect performance data.
- 4 Click **Apply** to save the configuration

### Enabling Temperature Monitoring for SAN Switches

- 1 From the menu bar, select **Administration > DCNM Server > Server Properties**.
- 2 Navigate to the # **PERFORMANCE MANAGER > COLLECTIONS** area.
- 3 Set the environment fields **pm.collectSanTemperature** & **pm.sanSensorDiscovery** to **TRUE**.
- 4 Click **Apply Changes** to save the configuration.
- 5 Restart Cisco DCNM.

## Viewing Other Statistics

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Switch > User Defined**.  
You see the **Other** window.
- Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.  
There are variations to this procedure. In addition to these basic steps, you can also do the following:
- Select the time range, and click **Filter** to filter the display.
  - Click the chart icon in the **Switch** column to see a graph of the performance for this user defined object.  
You can change the time range for this graph by selecting it from the drop-down list in the upper right corner.
  - Use the chart icons to view the traffic chart in varied views.
- 

## Viewing Switch Custom Port Groups Information

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Switch > Custom Port Groups**.  
The Custom Port Groups page shows statistics and performance details for custom port groups.
- Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.
- Step 3** To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.
- Step 4** Click the switch name to view the [Switch Dashboard](#), on page 7.
- 

## Viewing Accounting Information

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Switch > Accounting**.  
The fabric name or the group name along with the accounting information is displayed.



- Step 2** Select **Advanced Filter** beside the filter icon to search the accounting information by **Source**, **User Name**, **Time** and **Description**. Or select **Quick Filter** to search under each column.
- Step 3** You can also select a row and click on the delete icon to delete accounting information from the list.
- Step 4** You can use the **Print** icon to print the accounting details and use the **Export** icon to export the data to a Microsoft Excel spreadsheet.
- 

## Viewing Events Information

You can view the events and syslog from Cisco DCNM Web Client.

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Switch > Events**.  
The fabrics along with the switch name and the events details are displayed.  
The **Count** column displays the number of times that the same event has occurred during the time period that is shown in the **Last Seen** and **First Seen** columns.  
If you click a switch name displayed in the **Switch** column, Cisco DCNM Web Client displays the switch dashboard.
- Step 2** Select one events in the table and click the **Add Suppressor** icon to open the shortcut of adding an event suppressor rule. For detailed information about adding event suppressor rules, please refer to [Add Event Suppression Rules](#), on page 311.
- Step 3** Select one or more events from table and click the **Acknowledge** icon to acknowledge the event information for the fabric.
- Once you have acknowledged the event for a fabric, the acknowledge icon is displayed in the **Ack** column next to the fabric.
- Step 4** You can cancel an acknowledgment for a fabric by selecting the fabric and clicking the **Unacknowledge** icon.
- Step 5** Select **Advanced Filter** beside the filter icon to search the accounting information by **Source**, **User Name**, **Time** and **Description**. Or select **Quick Filter** to search under each column.
- Step 6** Select a fabric and use the **Delete** icon to delete the fabric and it's event information from the list.
- Step 7** You can use the **Print** icon to print the event details and use the **Export to Excel** icon to export the data to a Microsoft Excel spreadsheet.
- 

## Monitoring SAN

The SAN menu includes the following submenus:

## Monitoring ISL Traffic and Errors

### Procedure

**Step 1** From the menu bar, choose **Monitor > SAN > ISLs**.  
You see the **ISL Traffic and Errors** pane. This panel displays the ISL information for the end devices in that scope. You can reduce or expand the scope of what is displayed by using the scope menu.

**Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

**Note** **NaN** (Not a Number) in the data grid means that the data is not available.

**Note** It will be empty for non-FCIP ports under the **FCIP Compression Ratio** column.

There are variations to this procedure. In addition to these basic steps, you can perform the following steps to view detailed information for ISLs:

- To change the time range for this graph, select it from the drop-down list in the upper-right corner.
- To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
- Use the chart icons to view the traffic chart in varied views. You can also use the icons to Append, Predict and Interpolate Data. To view real-time information, choose **Refresh** icon from in the upper right corner. The real-time data is updated in every 10 seconds.
- To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.
- For the Rx/Tx calculation, see the following Rx/Tx calculation formula.

**Note** The conversion for Fabrics is 10 bit = 1 byte and for LAN traffic, the conversion is 8 bit = 1 byte.

- Average Rx/Tx % = Average Rx/Tx divided by Speed \* 100
- Peak Rx/Tx % = Peak Rx/Tx divided by Speed \* 100

If the performance tables do not contain any data, see the Performance Setup Thresholds section to turn on performance.

## Viewing Performance Information for NPV Links

### Procedure

**Step 1** From the menu bar, choose **Monitor > SAN > NPV Links**.  
You see the **NPV Links** window. This window displays the NPV links for the selected scope.

**Step 2** You can use the drop-down to filter the view by **24 hours**, **Week**, **Month** and **Year**.

**Step 3** Click the chart icon in the **Name** column to see a list of the traffic for the past 24 hours. There are variations to this procedure. In addition to these basic steps, you can also perform the following steps to view detailed information for NPV links:

- You can change the time range for this information by selecting from the drop-down list in the upper-right corner.
- To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
- Use the chart icons to view the traffic chart in varied views. You can also use the icons to **Append**, **Predict** and **Interpolate Data**.
- To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.
- To view real-time information, choose **Real Time** from the drop-down list in the **Chart** menu.

**Note** If the performance tables do not contain any data, see the [Performance Setup Thresholds](#), on page 305 section to turn on performance data collection.

## Viewing Inventory Information for VSANs

### Procedure

From the menu bar, choose **Monitor > SAN > VSANs**.

You see the **VSAN** window displaying the VSAN details along with the status and **Activated Zoneset** details.

## Monitoring Performance Information for Ethernet Ports

### Procedure

**Step 1** From the menu bar, choose **Monitor > SAN > Ports**.  
You see the **Ethernet Ports** window.

**Step 2** You can use the drop-down to filter the view by **24 hours**, **Week**, **Month** and **Year**. There are variations to this procedure. In addition to these basic steps, you can also perform the following steps:

- Select the name of an Ethernet port from the **Name** column to see a graph of the traffic across that Ethernet port for the past 24 hours. You can change the time range for this graph by selecting it from the drop-down list in the upper-right corner.
- To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.

- Use the chart icons to view the traffic chart in varied views. You can also use the icons to Append, Predict and Interpolate Data.
- For the Rx/Tx calculation, see the following Rx/Tx calculation formula.

**Note** The conversion for Fabrics is 10 bit = 1 byte and for LAN traffic, the conversion is 8 bit = 1 byte.

- Average Rx/Tx % = Average Rx/Tx divided by Speed \* 100
- Peak Rx/Tx % = Peak Rx/Tx divided by Speed \* 100

**Note** If the performance tables do not contain any data, see the [Performance Setup Thresholds](#), on page 305 section to turn on performance data collection.

## Viewing Inventory Information for Host Ports on FC End Devices

### Procedure

- 
- Step 1** From the menu bar, choose **Monitor > SAN > FC Ports**.  
You see the **Inventory > End Ports** window displaying details of the FC End Devices on the host ports.
- Step 2** Use the drop-down to view All or Warning information for the FC End devices on host ports.
- Step 3** Click the **Show Filter** icon to enable filtering by **Enclosure**, **Device Name** or **VSAN**.
- 

## Viewing Performance Information on All Ports

You can view the performance of devices connected to host ports, storage ports and all ports.

### Procedure

- 
- Step 1** From the menu bar, choose **Performance > End Devices**.  
You see the **End Devices Traffic and Errors** window.
- Step 2** You can choose to display **All** ports, **Host** ports or **Storage** ports from the drop-down list on the upper right corner.
- Step 3** You can use the drop-down to filter the view by **24 hours**, **Week**, **Month** and **Year**.
- Step 4** To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.
- Step 5** Click the chart icon in the **Name** column to see:
- A graph of the traffic on that device according to the selected timeline.
  - Use the chart icons to view the traffic chart in varied views. To view real-time information, click the refresh icon from the drop-down list in the upper right corner. The real-time data is updated in every 10 seconds. You can also use the icons to **Append**, **Predict** and **Interpolate Data**.

**Note** If the performance tables do not contain any data, see the [Performance Setup Thresholds](#), on page 305 section to turn on performance data collection.

---

## Viewing Performance Information for FC Flows

You can view the performance of the **FC Flow** traffic through the Cisco DCNM Web Client.

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > SAN > FC Flows**.  
You see the **FC Flows** window.
- Step 2** You can use the drop-down to filter the view by **24 hours**, **Week**, **Month** and **Year**.
- Step 3** To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.
- Step 4** Click the chart icon in the **Name** column to see:
- A graph of the traffic on that device according to the selected timeline.
  - Use the chart icons to view the traffic chart in varied views. To view real-time information, click on the refresh icon from the drop-down list in the upper right corner.
  - You can also use the icons to **Append**, **Predict** and **Interpolate Data**.

**Note** If the performance tables do not contain any data, see the [Performance Setup Thresholds](#), on page 305 section to turn on performance data collection.

---

## Viewing Performance Information on Enclosures

You can view the performance of devices connected to the host enclosure.

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > SAN > Enclosures**.  
You see the **Enclosures Traffic and Errors** window.
- Step 2** You can select to view **Host Enclosures** or **Storage Enclosures** from the drop-down list on the upper right corner.
- Step 3** You can use the drop-down to filter the view by **24 hours**, **Week**, **Month** and **Year**.
- Step 4** To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.
- Step 5** Click the chart icon in the **Name** column to see:
- A graph of the traffic on that device according to the selected timeline.
  - Use the chart icons to view the traffic chart in varied views.
  - You can also use the icons to **Append**, **Predict** and **Interpolate Data**.

**Note** If the performance tables do not contain any data, see the [Performance Setup Thresholds](#), on page 305 section to turn on performance data collection.

---

## Viewing Performance Information on Port Groups

You can view the performance of devices connected to the port groups.

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > SAN > Port Groups**.  
You see the **Port Group Traffic and Errors** window.
- Step 2** You can use the drop-down to filter the view by **24 hours**, **Week**, **Month** and **Year**.
- Step 3** Click the name port group to see the members of that port group.  
There are variations to this procedure. In addition to these basic steps, you can also perform the following steps to view detailed information for the port groups:
- To change the time range for this graph, select it from the drop-down list in the upper right corner.
  - To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
  - Use the chart icons to view the traffic chart in varied views.
  - You can also use the icons to **Append**, **Predict** and **Interpolate Data**.
  - To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.

**Note** If the performance tables do not contain any data, see the [Performance Setup Thresholds](#), on page 305 section to turn on performance data collection.

---

## SAN Host Redundancy

The **SAN Host Path Redundancy** check enables you to view the non-redundant host storage paths. It helps you identify the host enclosure errors along with the resolution to fix the errors.



### Note

All fabrics that are discovered must be licensed or this feature will be disabled in the Cisco DCNM Web Client. When the feature is disabled, a notification is displayed stating unlicensed fabrics are discovered.

---

From the menu bar, choose **Monitor > SAN > Host Path Redundancy**.

You can see two parts in this window:

- [Tests to Run](#)
- [Results](#)

## Tests to Run

### Procedure

- 
- Step 1** From the menu bar, choose **Monitor > SAN > Host Path Redundancy**.
  - Step 2** Under the upper **Tests to Run** area, use the check boxes to select the host redundancy optional checks.
  - Step 3** Check the **Automatically Run Check Every 24 hours** checkbox to enable periodic running of the checker. The checker will run every 24 hours starting 10 minutes after the server starts.
  - Step 4** Check **Limit by VSANs** check box, and select **Inclusion** or **Exclusion**. Enter VSAN or VSAN range in the text field to include or skip the host enclosures that belong to VSAN(s) from the redundancy check.
  - Step 5** Check other optional checks to do the relevant check.
  - Step 6** Click **Clear Results** to clear all the errors displayed.
  - Step 7** Click **Run Tests Now** to run the check at anytime.
  - Step 8** The results are displayed in the below [Results](#) area.
- 

## Results

### Procedure

- 
- Step 1** From the menu bar, choose **Monitor > SAN > Host Path Redundancy** tab.
  - Step 2** The bottom **Results** area has four tabs that are **Host Path Errors**, **Ignored Hosts**, **Ignored Storage** and **Ignored Host Storage Pairs**.
  - Step 3** Click **Host Path Errors** tab to display the host path redundancy errors table. On the top of the table, the colored **Good**, **Skipped** and **Errored** host enclosure counts, along with the last update time are displayed.
    - a) The **Host Enclosure** column displays the hosts that contain the errors. These are counts of each path in the host enclosures seeing an error. The **Storage Enclosure/Storage Port** column displays the connected storage that is involved the errors. In the **Fix?** column, hover the mouse cursor on the ? icon to view a solution to fix the error.
    - b) Select a row and click **Ignore Hosts** to add the selected row(s) host enclosure to an exclusion list. The errors from that host will no longer be reported and the current errors will be purged from the database.
    - c) Select a row and click **Ignore Storage** to add the selected row(s) storage enclosure to an exclusion list.
    - d) Select a row and click **Ignore Host Storage Pair** to add the selected row(s) host-storage pair enclosure to an exclusion list.
    - e) In the drop-down list next to **Show** on the upper right corner of the table, select **Quick Filter**. Enter the keywords in the column headers of the table to filter the items. Select **All** to display all the items.
    - f) Click the circulation icon on the upper right corner of the table to refresh the table.
    - g) Click the **Print** icon on the upper right corner of the table to print the errors as tables.

h) Click the **Export** icon on the upper right corner of the table to export the table to a Microsoft excel spreadsheet.

**Step 4** Click the **Ignored Hosts** tab to display the list of host enclosures that have been skipped or ignored by the redundancy check along with the reason the host enclosure check was skipped. The following reasons may be displayed:

- Skipped: Enclosure has only one HBA.
- Host was ignored by the user.
- Host ports managed by more than one federated servers. Check can't be run.
- Skipped: No path to storage found.

Select a host enclosure and click the **Delete** button to remove the host from the ignored list and begin receiving errors about a host you had chosen to ignore. However, you can delete entries with message Host was ignored by user.

**Step 5** Click the **Ignored Storage** tab to display the list of storage enclosures that have been selected to be ignored during redundancy check. Select a storage enclosure and click the **Delete** button to remove the storage from the ignored list and begin receiving errors about a storage you had chosen to ignore.

**Step 6** Click the **Ignored Host Storage Pair** tab to display the list of host-storage pairs that have been selected to be ignored during redundancy check. Select a row and click **Delete** to delete the storage pair from the ignored list.

## Slow Drain Analysis

The **Slow Drain Analysis** enables you to view slow drain statistics at the switch level and the port level. You can monitor the slow drain issue within any time frame. You can display the data in a chart format and export the data for analysis also.

The slow drain statistics are stored in the cache memory. Therefore, the statistics will be lost when the server is restarted or a new diagnostic request is placed.



### Note

The jobs run in the background, even after you log off.

To configure and view the slow drain statistics,

### Procedure

**Step 1** From the menu bar, choose **Monitor > SAN > Slow Drain Analysis**.

**Step 2** In the **Scope** field, select the fabric from the drop-down list.

**Step 3** In the **Duration** drop-down list, select **Once** or **Daily** for scheduled daily job. **Once** will include intervals, such as 10min, 30min, 1hour, and other hours and run the job immediately; while **Daily** will allow user to pick a start up time, and run the job for selected interval. Use the radio button to select the desired Interval to collect data.

Only daily slow drain job will sent out report which can be viewed from **Monitor > Report > View**.



- Step 4** Click the **Play** icon to begin polling.  
The server begins to collect the slow drain statistics based on the scope defined by the user. The **Time Remaining** is displayed in the right-side of the page.
- Step 5** Click the **Stop** icon to stop polling.  
The server maintains the counters in the cache, until a new diagnostic request is placed. You can stop the polling before the time is up.
- Step 6** Click on the arrow next to **Current jobs** to display the slow drain details for the jobs running on the fabric. The **Fabric Name**, the **Status** of polling, **Start**, **End**, and **Duration** icon for each fabric is displayed.
- Step 7** Select the fabric and click **Result**, **Delete** and **Stop** to view, delete and stop the job.
- Step 8** Click on the **Detail** icon to view the saved information.
- Step 9** Click on Interface chart icon to display the slow drain value for the switch port in chart format.
- Step 10** Click on the **Filter** icon to display the details based on the defined value for each column.
- Step 11** Select the **Data Rows Only** checkbox to filter and display the non-zero entries in the statistics.
- Step 12** Click on the **Print** icon to Prints the slow drain details.
- Step 13** Click on the **Export** icon to export the slow drain statistics to a Microsoft Excel spreadsheet.
- 

## Viewing Inventory Information for Regular Zones

### Procedure

- Step 1** From the menu bar, choose **Monitor > SAN > Regular Zones**.  
You see the **Regular Zones** window displaying the inventory details of the fabrics in the regular zone.
- Step 2** Click the **Settings** icon to choose the displaying columns.
- 

## Viewing Inventory Information for IVR Zones

### Procedure

- Step 1** From the menu bar, choose **Inventory > Active Zones > IVR Zones**.  
You see the IVR Zones window displaying the inventory details of the fabrics in the IVR zone.
- Step 2** Click the **Settings** icon to choose the display column.
-

# Monitoring LAN

The LAN menu includes the following submenus:

## Monitoring Performance Information for Ethernet

### Procedure

**Step 1** From the menu bar, choose **Monitor > LAN > Ethernet**.

You see the **Ethernet** window.

**Step 2** You can use the drop-down to filter the view by **24 hours**, **Week**, **Month** and **Year**.

There are variations to this procedure. In addition to these basic steps, you can also perform the following steps:

- Select the name of an Ethernet port from the **Name** column to see a graph of the traffic across that Ethernet port for the past 24 hours. You can change the time range for this graph by selecting it from the drop-down list in the upper-right corner.
- To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.
- Use the chart icons to view the traffic chart in varied views. You can also use the icons to Append, Predict and Interpolate Data.
- For the Rx/Tx calculation, see the following Rx/Tx calculation.

**Note** The conversion for Fabrics is 10 bit = 1 byte and for LAN traffic, the conversion is 8 bit = 1 byte.

- Average Rx/Tx % = Average Rx/Tx divided by Speed \* 100
- Peak Rx/Tx % = Peak Rx/Tx divided by Speed \* 100

**Note** If the performance tables do not contain any data, see the [Performance Setup Thresholds](#), on page 305 section to turn on performance data collection.

## Monitoring ISL Traffic and Errors

### Procedure

**Step 1** From the menu bar, choose **Monitor > LAN > Link**.

You see the **ISL Traffic and Errors** pane. This panel displays the ISL information for the end devices in that scope. You can reduce or expand the scope of what is displayed by using the scope menu.

**Step 2** You can use the drop-down to filter the view by 24 hours, Week, Month and Year.

**Note** NaN (Not a Number) in the data grid means that the data is not available.

There are variations to this procedure. In addition to these basic steps, you can perform the following steps to view detailed information for ISLs:

- To change the time range for this graph, select it from the drop-down list in the upper-right corner.
- To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
- Use the chart icons to view the traffic chart in varied views. You can also use the icons to Append, Predict and Interpolate Data. To view real-time information, choose **Real Time** from the drop-down list in the **Chart** menu.
- To export the data into a spreadsheet, choose **Export** from the drop-down list in the **Chart** menu and then click **Save**.
- For the Rx/Tx calculation, see the following Rx/Tx calculation.

**Note** The conversion for Fabrics is 10 bit = 1 byte and for LAN traffic, the conversion is 8 bit = 1 byte.

- Average Rx/Tx % = Average Rx/Tx divided by Speed \* 100
- Peak Rx/Tx % = Peak Rx/Tx divided by Speed \* 100

**Note** If the performance tables do not contain any data, see the Performance Setup Thresholds section to turn on performance.

## Monitoring a vPC

The virtual port channel (vPC) feature enables you to view the links that are physically connected to different devices as a single port channel. A vPC is an extended form of a port channel which allows you to create redundancy and increase bisectional bandwidth by enabling multiple parallel paths between nodes and allowing load balancing traffic. Traffic is distributed among two single device vPC end points. If there is an inconsistency in the vPC configurations, the vPC does not function correctly.



**Note**

To view the vPC in **vPC Performance**, both primary and secondary device should be designated to the user. If either one kind of switch is not designated, vPC information will not displayed.

Cisco DCNM **Web Client** > **Monitor** > **vPC** will display only consistent vPCs displays both the consistent and inconsistent vPCs.

You can identify the inconsistent vPCs and resolve the inconsistencies in each vPC by using the Cisco DCNM **Web Client** > **Configure** > **Deploy** > **vPC Peer** and **Web Client** > **Configure** > **Deploy** > **vPC**.

[Table 8: vPC Performance, on page 78](#) displays the following vPC configuration details in the data grid view.

**Table 8: vPC Performance**

| Column                                          | Description                                                                  |
|-------------------------------------------------|------------------------------------------------------------------------------|
| Search box                                      | Enter any string to filter the entries in their respective column.           |
| <b>vPC ID</b>                                   | Displays vPC ID's configured device.                                         |
| <b>Domain ID</b>                                | Displays the domain ID of the vPC peer switches.                             |
| <b>Multi Chassis vPC EndPoints</b>              | Displays the multi-chassis vPC endpoints for each vPC ID under a vPC domain. |
| <b>Primary vPC Peer - Device Name</b>           | Displays the vPC Primary device name.                                        |
| <b>Primary vPC Peer - Primary vPC Interface</b> | Displays the primary vPC interface.                                          |
| <b>Primary vPC Peer - Capacity</b>              | Displays the capacity for the primary vPC peer.                              |
| <b>Primary vPC Peer - Avg. Rx/sec</b>           | Displays the average receiving speed of primary vPC peer.                    |
| <b>Primary vPC Peer - Avg. Tx/sec</b>           | Displays the average transmitting speed of primary vPC peer.                 |
| <b>Primary vPC Peer - Peak Util%</b>            | Displays the peak utilization percentage of primary vPC peer.                |
| <b>Secondary vPC Peer - Device Name</b>         | Displays the vPC secondary device name.                                      |
| <b>Secondary vPC Interface</b>                  | Displays the secondary vPC interface.                                        |
| <b>Secondary vPC Peer - Capacity</b>            | Displays the capacity for the secondary vPC peer.                            |
| <b>Secondary vPC Peer - Avg. Rx/sec</b>         | Displays the average receiving speed of secondary vPC peer.                  |
| <b>Secondary vPC Peer - Avg. Tx/sec</b>         | Displays the average transmitting speed of secondary vPC peer.               |
| <b>Secondary vPC Peer - Peak Util%</b>          | Displays the peak utilization percentage of secondary vPC peer.              |

You can use this feature as below:

## Monitoring vPC Performance

You can view the relationship among consistent virtual port channels (vPCs). You can view the statistics of all member interfaces and the aggregate of the statistics at the port channel level.

**Note**

This tab only displays consistent vPCs.

### Procedure

- Step 1** From the menu bar, choose **Monitor > LAN > vPC**.  
The **vPC Performance** statistics appears and the aggregated statistics of all vPCs are displayed in a tabular manner.
- Step 2** Click on the **vPC ID** and a window appears.  
You are able to view the vPC topology and **vPC Details**, **Peer-link Details** and **Peer-link Status** table.  
The **vPC Consistency**, **Peer-link Consistency**, and **vPC Type2 Consistency** for the vPC is displayed.
- Click the **vPC Details** tab, you can view the parameter details of vPC **Basic Setting** and **Layer 2 Settings** for both Primary and Secondary vPC devices.
  - Click the **Peer-link Details** tab, you can view the parameter details of peer-link **vPC Global Setting** and **STP Global Settings** for both Primary and Secondary vPC devices.
  - Click the **Peer-link Status** tab, the **vPC Consistency** and **Peer-Link Consistency** status is displayed, as well as the parameter details of **Role Status** and **vPC Peer keep-alive Status** for both Primary and Secondary vPC devices.
- Step 3** Click on the peer-link icon in front of the **Device Name** in the **Primary vPC peer** or **Secondary vPC peer** column to view its member interface.  
A pop-up window displays the member interfaces of the selected device.
- Step 4** Click the **Show Chart** icon of the corresponding interface to view its historical statistics.  
The traffic distribution statistics appear at the bottom of the vPC window. By default, the Cisco DCNM Web Client displays the historical statistics for 24 hours.
- There are variations to this procedure. In addition to these basic steps, you can also perform the following steps to view detailed information for flows:
- To change the time range for this graph, select it from the drop-down list in the upper right corner.
  - To view the detailed information for a specific period, drag the slider control to choose the time interval for which you need the information.
  - Use the chart icons to view the traffic chart in varied views.
  - You can also use the icons to **Append**, **Predict** and **Interpolate Data**.
  - To export the data into a spreadsheet, click the **Export** icon in the upper-right corner and then click **Save**.

**Note** If the performance tables do not contain any data, see the [Performance Setup Thresholds](#), on page 305 section to turn on performance data collection.

---

# Monitoring Report

The Report menu includes the following submenus:

## Viewing Reports

You can view the saved reports based on the following selection options:

- **By Template**
- **By User**
- From the menu bar, select **Monitor > Report > View**.

You see the **View Reports** window displaying the **View Reports** by tree on the left pane.

### Procedure

---

- Step 1** In the left pane, expand **By Template** or **By User** folder.
- Step 2** Select the report you wish to view. You can view the report in the main screen or you can select the report in the **Report** column to view the HTML version of the report in a new browser.
- Step 3** To delete a specific report, select the check box and click the **Delete** icon.
- Step 4** To delete all reports, check the check box in the header, and click the **Delete** icon.
- Note** If you have multiple fabrics, you can select the DCNM-SAN group in the Scope to view Host to Storage connectivity of multiple fabrics in a single report. The report is divided into two sections:
- A summary report for all the devices that have faulty modules. The table displays information for every device that includes the device host name, number of faulty modules and the module number with its PID.
  - A detailed information for the device of the module. The table contains details about the tests failed.
- 

## Generating a Report

You can generate reports based on a selected template or you can schedule the report to run at a specified time.

### Procedure

---

- Step 1** From the menu bar, select **Monitor > Report > Generate**.  
You see the **Generate Report** window.

- Step 2** In the configuration window, use the drop-down to define the scope for report generation. In the **Scope** drop-down, you can select a scope group with dual fabrics, the traffic data generated by hosts and storage end devices are displayed side-by-side which enables you to view and compare traffic data generated on dual fabrics. To view this report, in the **Other Predefined** folder, select **Traffic by VSAN** (Dual Fabrics). Click Options to select the **Device Type** and **Fabrics**. Click **Save** to save the configuration.
- Step 3** In the pane on the left hand, expand the folders and select the report.
- Step 4** (Optional) In the pane on the right hand, you can edit the **Report Name**.
- Step 5** (Optional) Check the **Export to Csv/Excel** check box to export the report in to a Microsoft Excel spreadsheet.
- Step 6** In the **Repeat** radio buttons, if you select:
- **Never** - The report is generated only during the current session.
  - **Once** - The report is generated on a specified date and time apart from the current session.
  - **Daily** - The report is generated everyday based on the Start and End date at a specified time.
  - **Weekly** - The report is generated once a week based on the Start and End date at a specified time.
  - **Monthly** - The report is generated once every month based on the Start and End date at a specified time.

When you generate a report for Network Configuration Audit, the daily job generates a report for the selected devices for last 1 day. Similarly, the weekly job generates a report for the last 7 days, and the monthly job generates a report for the last 30 days.

- Step 7** Click the **Create** button to generate a report based on the specifications. You see the report results in a new browser window.

Alternatively, you can view the report by choosing **Monitor > Report > View** and selecting the report name from the report template that you used in the navigation pane.

**Note** The **Start Date** must be at least five minutes earlier than the **End Date**

The report is divided into two sections:

- A summary report for all the devices that have faulty modules. The table displays information for every device that includes the device host name, number of faulty modules and the module number with its PID.
- A detailed information for the device of the module. The table contains details about the tests failed.

## Creating SAN User Defined Reports

You can create custom reports from all or any subset of information obtained by Cisco DCNM-SAN. You create a report template by selecting events, performance, and inventory statistics you want in your report and set the desired SAN, fabrics or VSAN to limit the scope of the template. You can generate and schedule a report of your fabric based on this template immediately or at a later time. DCNM Web Client saves each report based on the report template used and the time you generate the report.

Since the Cisco MDS NX-OS Release 5.0, the report template design has changed to resolve the limitations of the earlier versions. With the new design model, you can perform add, delete, and modify functionalities

on a single page. You can choose multiple fabrics and VSANs using the new navigation system, which allows you to add new items and categories in the future.

The new design model has three panels:

- **Template** panel - The **Template** panel allows you to add new templates, modify existing templates and delete existing templates.
- **Configuration** panel - The **Configuration** panel allows you to configure a new template when it is added, and modify an existing template. The options in the configuration panel are disabled until you either add a new template or select an existing template. The upper portion of the configuration panel contains many categories that you can choose and configure.
- **User Selection** panel - The **User Selection** panel displays your configuration options in real-time. While the configuration panel can display information pertaining to one category at a time, the **User Selection** panel displays all of your selections or configurations.

Follow the steps to create custom reports

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Report > User Defined**.  
You see the **Create User Defined** window.
- Step 2** In the **Template** panel, under the **Name** column, select **CLICK TO ADD NEW CUSTOM** to edit the **Name** of the new report.  
In the **Configuration** panel:
- Step 3** Click **Scope** to define scope of the report. The default scope will have Data Center, SAN, LAN, and Fabric configurations.
- Step 4** Click **Inventory** and use the checkbox to select the inventory information required in the report. You can also use the drop-down to filter by selecting the Top performance and the timeline required in the report.
- Step 5** Click **Performance** and use the checkbox to select the performance information required in the report.
- Step 6** Click **Health** and use the checkbox to select the health information required in the report.
- Step 7** Click **Save** to save this report template.  
A confirmation message is displayed confirming that the report is saved.
- 

## Deleting a Report Template

### Procedure

---

- Step 1** In the **Template** panel, select the report template that you want to delete.
- Step 2** Click the **Delete** icon to delete the report.
- Step 3** In the confirmation pop-up, click **Yes** to delete the template.
-



## Modifying a Custom Report Template

### Procedure

- 
- Step 1** From the menu bar, choose **Monitor > Report > User Defined**.  
You see the **Template**, **Configuration** and **User Selection** panels.
- Step 2** Select a report from the **Template** panel.  
You see the current information about this report in the **User Selection** panel.
- Step 3** Modify the information in the **Configuration** panel.
- Step 4** Click **Save** to save the report template.  
A confirmation message is displayed confirming that the report is saved.
- Note** You cannot change the scope for an existing report. You must generate a new report for a new scope.
- 

## Viewing Scheduled Jobs Based on a Report Template

### Procedure

- 
- Step 1** From the menu bar, choose **Monitor > Report > Jobs**.  
You see the **Report Jobs** window displaying details of the reports scheduled for generation along with its status.
- Step 2** Select the checkbox for a specific report and click the **Delete** Job icon to delete a report.
- 

## Monitoring Configuration

The Configuration menu includes the following submenus:

## Monitoring Archives

A user with network operator role can view configuration archives for a switch and their details in the **Archives** window.

The following tables describe the icons and fields that are displayed in this window.

**Table 9: Archive Operations**

| Icon             | Description                                                                                        |
|------------------|----------------------------------------------------------------------------------------------------|
| <b>Compare</b>   | Allows you to compare two configuration files either from different devices or on the same device. |
| <b>View/Edit</b> | Allows you to view or edit a configuration file.                                                   |

**Table 10: Archive Field and Description**

| Field Name           | Description                                                                                                         |
|----------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>Device Name</b>   | Displays the device name<br>Click on the arrow next to the device to view the configuration files.                  |
| <b>IP Address</b>    | Displays the IP address of the device.                                                                              |
| <b>Group</b>         | Displays the group of the device.                                                                                   |
| <b>Configuration</b> | Displays the configuration files archived for that device.                                                          |
| <b>Archive Time</b>  | Displays the time at which the device configuration files were archived.<br>The format is Day:Mon:DD:YYYY HH:MM:SS. |
| <b>Size</b>          | Displays the size of the archived file.                                                                             |
| <b>Golden</b>        | Shows whether the current version is a Golden backup or not.                                                        |

This section contains the following:

## Compare Configuration Files

This feature allows you to compare one version of a configuration file with another version of the same configuration file in the same device, or the configuration files of two different devices.  
Perform the following task to compare configuration files.

### Procedure

- 
- Step 1** In the Cisco DCNM web client home page, choose **Monitor > Configuration > Archives**.
- Step 2** In the **Archives** area, click the arrow adjacent the name of the device whose configuration files you want to view. The list of configuration files is displayed.
- Step 3** Check the check box next to configuration files and select two configuration files to compare. The first file you select is designated as source and the second configuration file is designated as the target file.
- Step 4** Click **Compare**.  
The **View Config Diff** page displays the difference between the two configuration files.  
The Source and Target configuration files' content are displayed in two columns. From the drop-down list in the right-top corner, choose **All** to view the entire configuration or choose **Changed** to view the configuration differences between the configuration files.  
The differences in the configuration files are shown in a table, with legends.  
Red—Deleted configuration details  
Green—Newly added configuration  
Blue—Modified configuration details
- 

## View or Edit Configuration

You can view an archived configuration file, or you can edit and save this file on your local system. The changes made to the archived configuration file is applied only to the file saved in your local system. The archived configuration file on the DCNM host server remains unchanged.

Perform the following task to view or edit the configuration file for the devices.

### Procedure

- 
- Step 1** In the web client home page, choose **Monitor > Configuration > Archives**.
- Step 2** In the **Archives** area, click the arrow adjacent the name of the device whose configuration files you want to view. The list of configuration files are displayed.
- Step 3** Click the radio button adjacent the corresponding file you want to view or edit.
- Step 4** Click the **View/Edit** configuration icon.  
The **View/Edit** configuration window appears showing the configuration file content in the right column.
- Step 5** Edit the configuration file as required.
- Step 6** Click **Save** to apply the changes and download the configuration file on your local system, or click **Cancel** to discard changes.
-

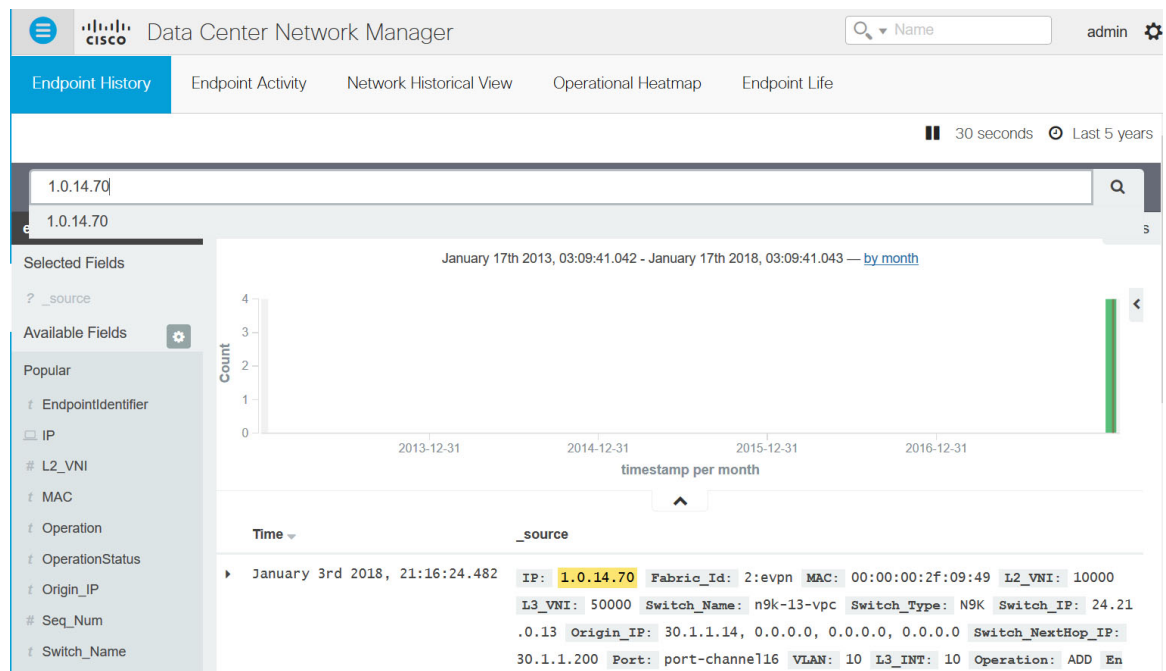
# Exploring Endpoint Locator Details

## Procedure

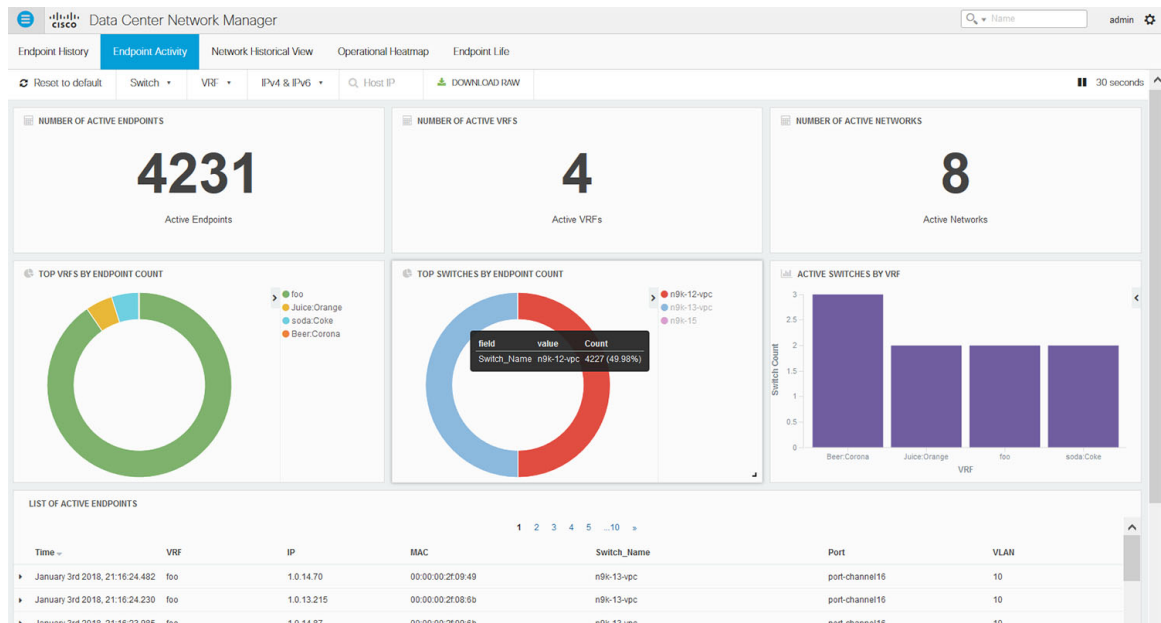
From the menu bar, choose **Monitor > Endpoint Locator > Explore**. The Endpoint Locator dashboard appears.

The Endpoint Locator Dashboard displays the following information:

- **Endpoint History**—Real time plot displaying Endpoint events for the period specified in the relative or absolute date range. A user can search for a specific metric value in the search bar. Search is supported on any of the fields as specified under the “Available Fields” column on the menu on the left. A sample screenshot of the endpoint history based on an IP address specified in the search field is depicted below.



- **Endpoint Activity**—This view displays the current state of the active endpoints in the fabric. The number of active endpoints including the number of active VRFs and active networks are listed in the top 3 tiles. The break-up of active endpoints is also available on a per VRF as well as a per switch basis. This is depicted by the first two tiles in the second row. If there is at least one active endpoint in a given VRF behind a switch, then that VRF is considered as active on that switch. Note that the VRF may be configured on a number of switches but it is only considered active and justifies burning resources on the switch, if there is at least one active endpoint in that VRF behind that switch. In that sense, the “ACTIVE SWITCHES BY VRF” tile can provide a good insight for the network administrator into removing extraneous VRF configurations from switches where it may not be needed. At the bottom of the dashboard, there is a data table that provides a list of endpoints with context information such as the VRF, IP, MAC, Switch, VLAN, Port etc. By default, the endpoint information is refreshed every 30 seconds. However, the refresh interval may be changed as desired.



Users can search for specific endpoints using various search filters such as VRF, switch, IPv4/IPv6 address etc. Multiple filters may be applied at the same time. The entire dashboard view across all tiles and the data table, are updated as soon as the search filters are applied. The search results can be downloaded in csv format by clicking on the “DOWNLOAD RAW” icon. A sample snippet of the downloaded csv file from a search result is shown below:

|    | A         | B         | C                 | D      | E      | F          | G           | H          | I           | J           | K           | L                 | M         | N    | O      | P         | Q         | R         | S       | T             | U         | V          | W                     | X         | Y         | Z                  | AA | AB | AC |
|----|-----------|-----------|-------------------|--------|--------|------------|-------------|------------|-------------|-------------|-------------|-------------------|-----------|------|--------|-----------|-----------|-----------|---------|---------------|-----------|------------|-----------------------|-----------|-----------|--------------------|----|----|----|
| 1  | Fabric_Id | IP        | MAC               | L2_VNI | L3_VNI | Switch_No  | Switch_Type | Switch_IP  | Origin_IPv4 | Origin_IPv6 | Origin_IPv4 | Switch_NextHop_IP | Port      | VLAN | L3_INT | Operation | EndpointT | Timestamp | Seq_Num | VRF           | Br_Domain | Cluster    | Valid                 | Operation | RouteDist | EndpointIdentifier |    |    |    |
| 2  | 2evpn     | 1.0.0.231 | 00:00:00:2e:ee:8b | 10000  | 50000  | n9k-13-vpc | NK          | 24.21.0.13 | 30.1.1.14   | 0.0.0.0     | 0.0.0.0     | 30.1.1.200        | port-chan | 10   | 10     | AD0       | Wed Jan 0 | 0         | foo     | 10.30.1.1.200 | 1         | 30.1.1.211 | (IPv4:1.0.0.231:10000 |           |           |                    |    |    |    |
| 3  | 2evpn     | 1.0.0.232 | 00:00:00:2e:ee:8d | 10000  | 50000  | n9k-13-vpc | NK          | 24.21.0.13 | 30.1.1.14   | 0.0.0.0     | 0.0.0.0     | 30.1.1.200        | port-chan | 10   | 10     | AD0       | Wed Jan 0 | 0         | foo     | 10.30.1.1.200 | 1         | 30.1.1.211 | (IPv4:1.0.0.232:10000 |           |           |                    |    |    |    |
| 4  | 2evpn     | 1.0.1.198 | 00:00:00:2e:fd:45 | 10000  | 50000  | n9k-13-vpc | NK          | 24.21.0.13 | 30.1.1.14   | 0.0.0.0     | 0.0.0.0     | 30.1.1.200        | port-chan | 10   | 10     | AD0       | Wed Jan 0 | 0         | foo     | 10.30.1.1.200 | 1         | 30.1.1.211 | (IPv4:1.0.1.198:10000 |           |           |                    |    |    |    |
| 5  | 2evpn     | 1.0.1.198 | 00:00:00:2e:fd:49 | 10000  | 50000  | n9k-13-vpc | NK          | 24.21.0.13 | 30.1.1.14   | 0.0.0.0     | 0.0.0.0     | 30.1.1.200        | port-chan | 10   | 10     | AD0       | Wed Jan 0 | 0         | foo     | 10.30.1.1.200 | 1         | 30.1.1.211 | (IPv4:1.0.1.198:10000 |           |           |                    |    |    |    |
| 6  | 2evpn     | 1.0.0.226 | 00:00:00:2e:ee:81 | 10000  | 50000  | n9k-13-vpc | NK          | 24.21.0.13 | 30.1.1.14   | 0.0.0.0     | 0.0.0.0     | 30.1.1.200        | port-chan | 10   | 10     | AD0       | Wed Jan 0 | 0         | foo     | 10.30.1.1.200 | 1         | 30.1.1.211 | (IPv4:1.0.0.226:10000 |           |           |                    |    |    |    |
| 7  | 2evpn     | 1.0.0.230 | 00:00:00:2e:ee:89 | 10000  | 50000  | n9k-13-vpc | NK          | 24.21.0.13 | 30.1.1.14   | 0.0.0.0     | 0.0.0.0     | 30.1.1.200        | port-chan | 10   | 10     | AD0       | Wed Jan 0 | 0         | foo     | 10.30.1.1.200 | 1         | 30.1.1.211 | (IPv4:1.0.0.230:10000 |           |           |                    |    |    |    |
| 8  | 2evpn     | 1.0.1.199 | 00:00:00:2e:fd:4b | 10000  | 50000  | n9k-13-vpc | NK          | 24.21.0.13 | 30.1.1.14   | 0.0.0.0     | 0.0.0.0     | 30.1.1.200        | port-chan | 10   | 10     | AD0       | Wed Jan 0 | 0         | foo     | 10.30.1.1.200 | 1         | 30.1.1.211 | (IPv4:1.0.1.199:10000 |           |           |                    |    |    |    |
| 9  | 2evpn     | 1.0.1.200 | 00:00:00:2e:fd:4d | 10000  | 50000  | n9k-13-vpc | NK          | 24.21.0.13 | 30.1.1.14   | 0.0.0.0     | 0.0.0.0     | 30.1.1.200        | port-chan | 10   | 10     | AD0       | Wed Jan 0 | 0         | foo     | 10.30.1.1.200 | 1         | 30.1.1.211 | (IPv4:1.0.1.200:10000 |           |           |                    |    |    |    |
| 10 | 2evpn     | 1.0.1.203 | 00:00:00:2e:fd:53 | 10000  | 50000  | n9k-13-vpc | NK          | 24.21.0.13 | 30.1.1.14   | 0.0.0.0     | 0.0.0.0     | 30.1.1.200        | port-chan | 10   | 10     | AD0       | Wed Jan 0 | 0         | foo     | 10.30.1.1.200 | 1         | 30.1.1.211 | (IPv4:1.0.1.203:10000 |           |           |                    |    |    |    |
| 11 | 2evpn     | 1.0.1.204 | 00:00:00:2e:fd:55 | 10000  | 50000  | n9k-13-vpc | NK          | 24.21.0.13 | 30.1.1.14   | 0.0.0.0     | 0.0.0.0     | 30.1.1.200        | port-chan | 10   | 10     | AD0       | Wed Jan 0 | 0         | foo     | 10.30.1.1.200 | 1         | 30.1.1.211 | (IPv4:1.0.1.204:10000 |           |           |                    |    |    |    |
| 12 | 2evpn     | 1.0.2.188 | 00:00:00:2e:fd:35 | 10000  | 50000  | n9k-13-vpc | NK          | 24.21.0.13 | 30.1.1.14   | 0.0.0.0     | 0.0.0.0     | 30.1.1.200        | port-chan | 10   | 10     | AD0       | Wed Jan 0 | 0         | foo     | 10.30.1.1.200 | 1         | 30.1.1.211 | (IPv4:1.0.2.188:10000 |           |           |                    |    |    |    |
| 13 | 2evpn     | 1.0.2.194 | 00:00:00:2e:fd:41 | 10000  | 50000  | n9k-13-vpc | NK          | 24.21.0.13 | 30.1.1.14   | 0.0.0.0     | 0.0.0.0     | 30.1.1.200        | port-chan | 10   | 10     | AD0       | Wed Jan 0 | 0         | foo     | 10.30.1.1.200 | 1         | 30.1.1.211 | (IPv4:1.0.2.194:10000 |           |           |                    |    |    |    |
| 14 | 2evpn     | 1.0.0.217 | 00:00:00:2e:ee:6f | 10000  | 50000  | n9k-13-vpc | NK          | 24.21.0.13 | 30.1.1.14   | 0.0.0.0     | 0.0.0.0     | 30.1.1.200        | port-chan | 10   | 10     | AD0       | Wed Jan 0 | 0         | foo     | 10.30.1.1.200 | 1         | 30.1.1.211 | (IPv4:1.0.0.217:10000 |           |           |                    |    |    |    |
| 15 | 2evpn     | 1.0.0.223 | 00:00:00:2e:ee:7b | 10000  | 50000  | n9k-13-vpc | NK          | 24.21.0.13 | 30.1.1.14   | 0.0.0.0     | 0.0.0.0     | 30.1.1.200        | port-chan | 10   | 10     | AD0       | Wed Jan 0 | 0         | foo     | 10.30.1.1.200 | 1         | 30.1.1.211 | (IPv4:1.0.0.223:10000 |           |           |                    |    |    |    |
| 16 | 2evpn     | 1.0.0.234 | 00:00:00:2e:ee:87 | 10000  | 50000  | n9k-13-vpc | NK          | 24.21.0.13 | 30.1.1.14   | 0.0.0.0     | 0.0.0.0     | 30.1.1.200        | port-chan | 10   | 10     | AD0       | Wed Jan 0 | 0         | foo     | 10.30.1.1.200 | 1         | 30.1.1.211 | (IPv4:1.0.0.234:10000 |           |           |                    |    |    |    |

It is possible to search based on any of the fields describing the information of each endpoint. For example, if the user wants to know the list of endpoints in a given network, that can be achieved as follows. Recall that each network is represented by a unique 24-bit identifier. This parameter is represented by the field L2\_VNI. Here are the steps:

- Go to the ‘List of endpoints’ data table and click on any row. This will expand the row as shown below:

**LIST OF ACTIVE ENDPOINTS**

1 2 3 4 5 ...10

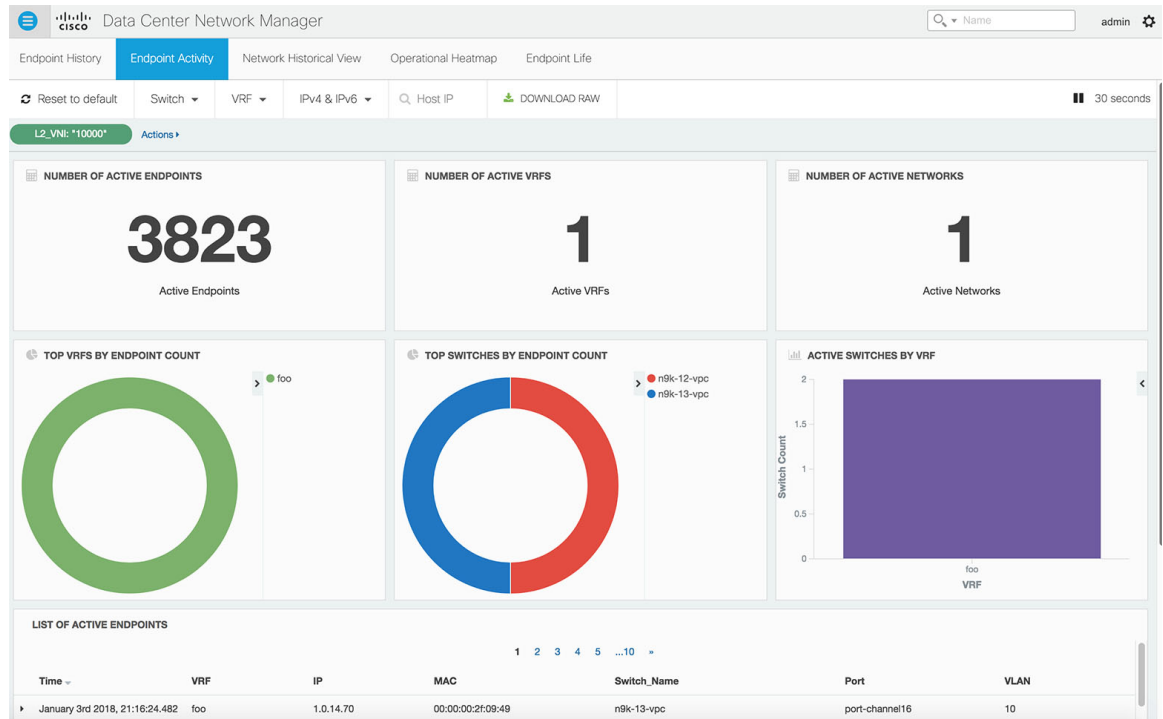
| Time                           | VRF | IP        | MAC               | Switch_Name | Port           | VLAN |
|--------------------------------|-----|-----------|-------------------|-------------|----------------|------|
| January 3rd 2018, 21:16:24.482 | foo | 1.0.14.70 | 00:00:00:2f:09:49 | n9k-13-vpc  | port-channel16 | 10   |

[Link to /api/cache/today/endpoint/evpn%3A1.0.14.70%3A30.1.1.219%3A32777](#)

[Table](#) [JSON](#)

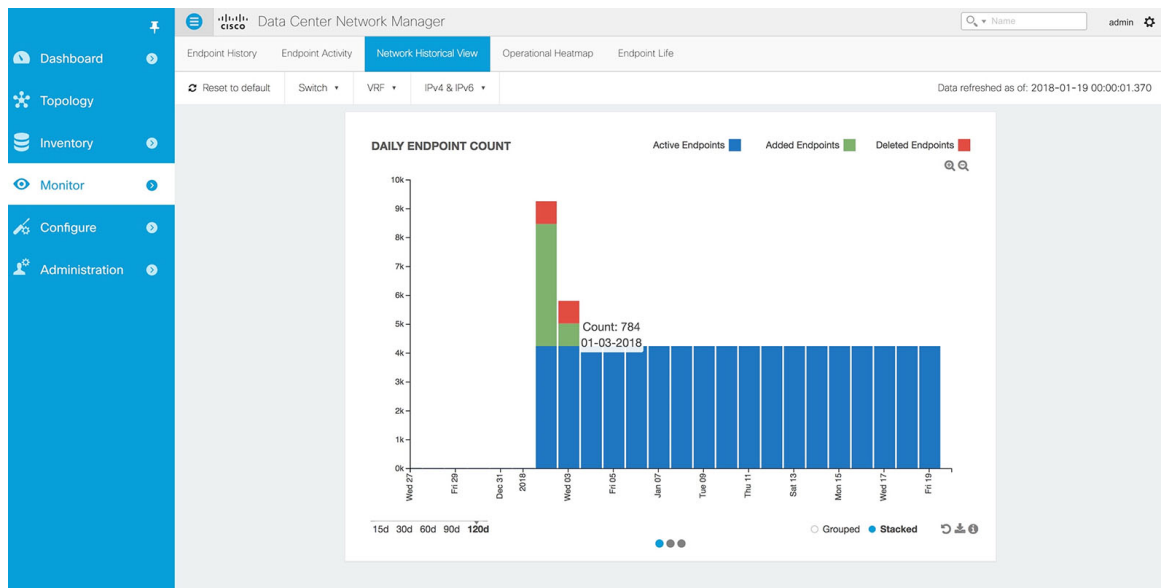
- Br\_Domain: 10
- Cluster: 30.1.1.200:0
- EndpointIdentifier: IPv4:1.0.14.70:10000
- EndpointType: Q
- Fabric\_Id: 2:evpn
- IP: 1.0.14.70
- L2\_VNI: 10000
- L3\_INT: Filter out value

- Click on the + icon next to the L2\_VNI field. This selects the highlighted value (10000 in this example) and filters the search results based on that. In other words, the information of all active endpoints in the network associated with L2\_VNI 10000 is displayed on the dashboard. If instead, all endpoints that are not in the network L2\_VNI are required, click the – icon next to the L2\_VNI value of 10000. In the same manner, one can choose any combination of fields to get the set of endpoints matching the corresponding selected filter criteria.

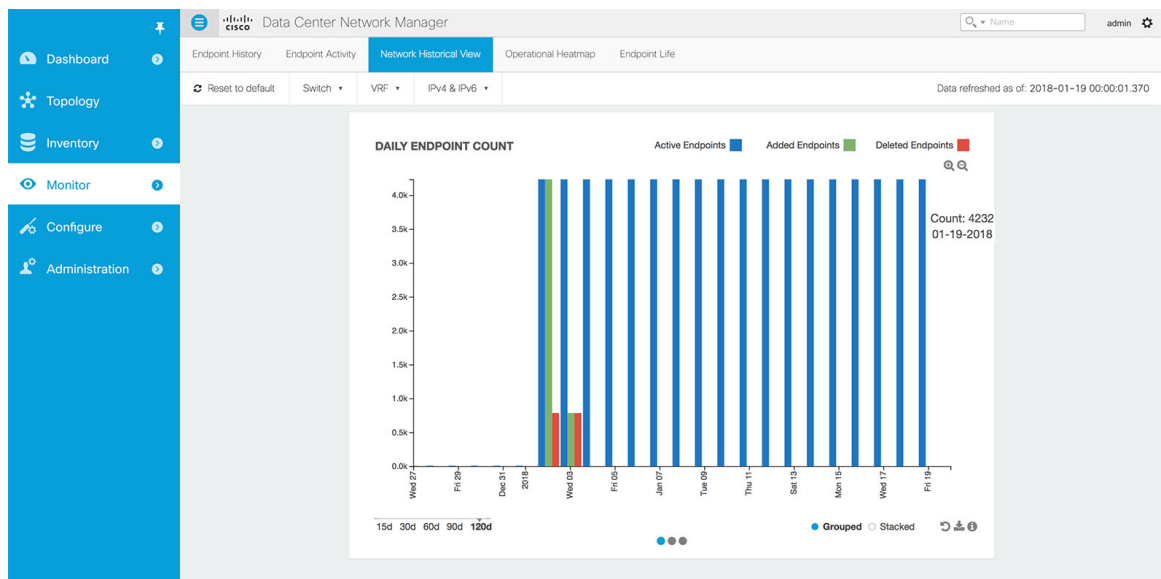


- Network Historical View**— The NHV view displays historical information of endpoints, networks, and VRFs (tenants) captured on a daily basis. These graphs are updated once a day at mid-night based on the DCNM server time. The time at which the data is refreshed/updated is listed at the top right. The idea is to provide a daily report of the Active, Added (New) and Deleted endpoints, networks, and VRFs respectively. If the same endpoint is added and removed on a day, then that contributes to an add count of 1 and a delete count of 1. Users can select one of the 3 dots at the bottom to toggle between the endpoints, networks, & VRF views. There are options to zoom in/out using zoom icons on top right. The users can also select the type of visualization with the choices being – Grouped or Stacked (shown below). Daily reports up to 180 days in the past can be displayed. Active endpoints/networks/VRFs are shown in blue color, deleted ones are shown in red color while the added ones are shown in green color. Every block in all screens is ‘clickable’ and the complete dataset associated with the selection, can be downloaded in csv format.

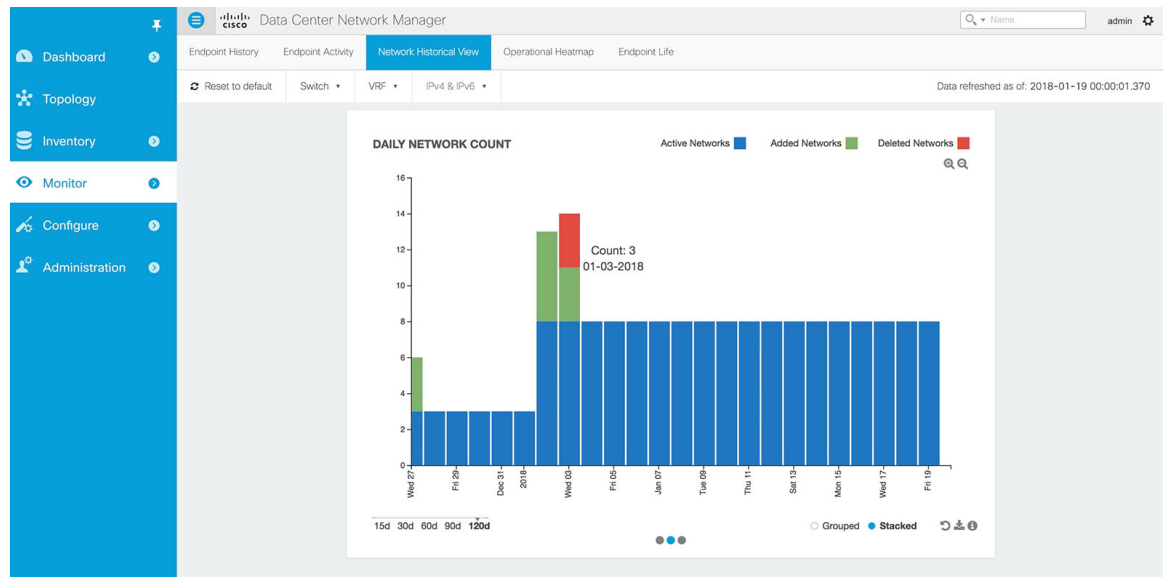
The historic endpoint count in ‘Stacked’ format is shown below:



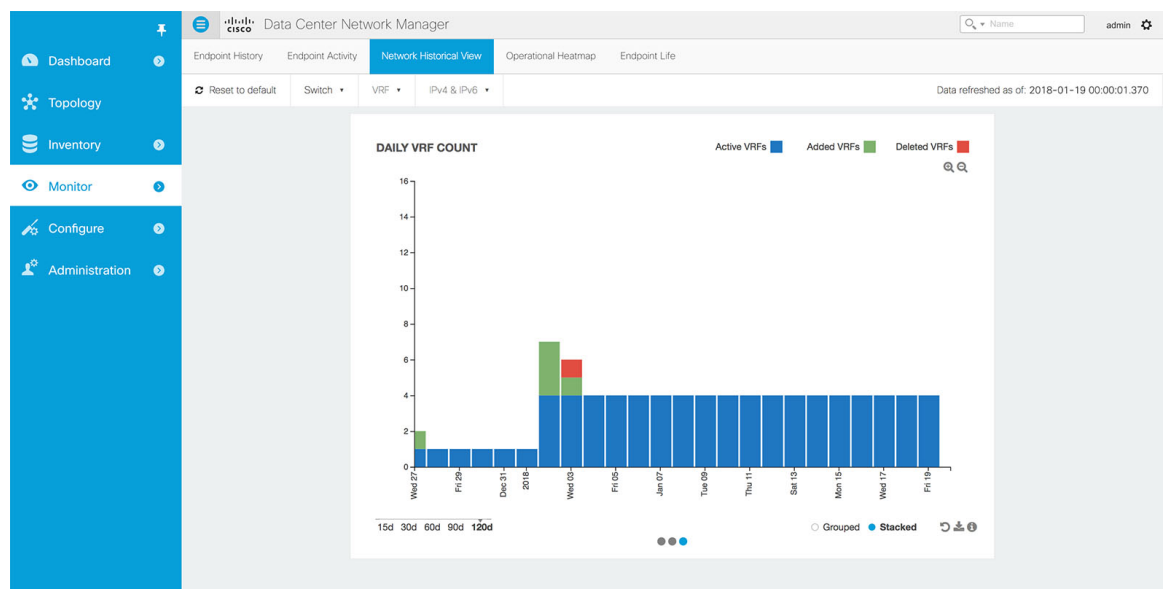
The same representation with the Grouped visualization selection is shown below:



Similarly, the figure below depicts the historic network count in stacked format:



Along the same lines, the figure below depicts the historic vrf count:



The figure below provides a sample screenshot of the endpoints added on 01-03-2018 obtained by clicking on the blue bar for that day.



Data Center Network Manager
 admin

[Endpoint History](#)
[Endpoint Activity](#)
[Network Historical View](#)
[Operational Heatmap](#)
[Endpoint Life](#)

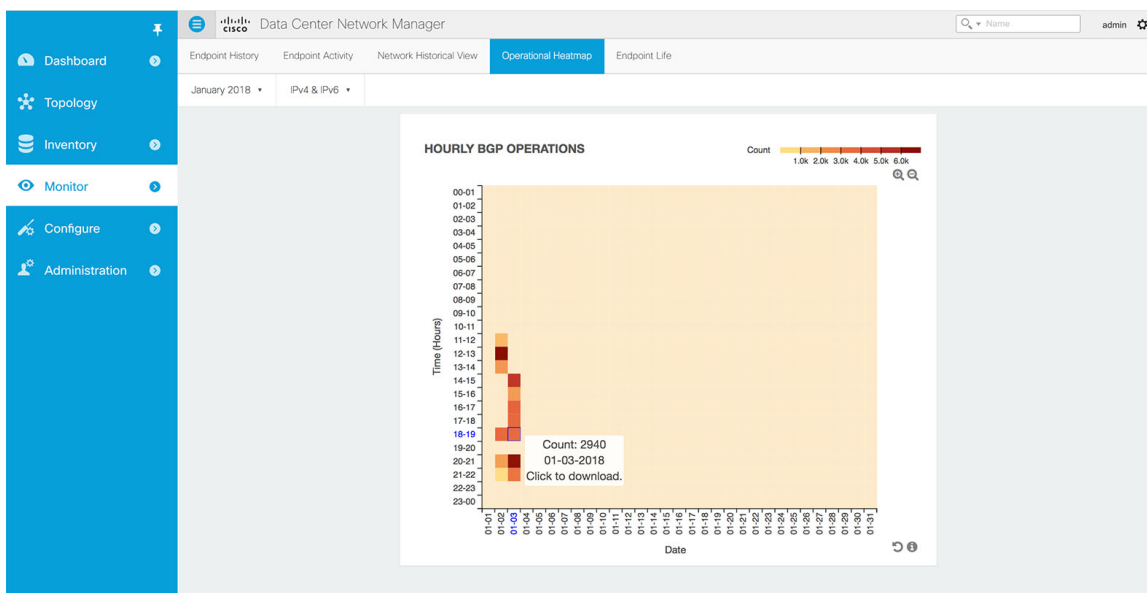
[Reset to default](#)
[Switch](#)
[VRF](#)
[IPv4 & IPv6](#)
Data refreshed as of: 2018-01-18 00:00:01.448

[Back to Graph](#)
[Download](#)

ADDED ENDPOINTS : 01-03-2018

| Date       | IP             | VNI   | VRF | Switch | Operation |
|------------|----------------|-------|-----|--------|-----------|
| 01-03-2018 | IPv4:1.0.13.32 | 10000 | All | All    | ADD       |
| 01-03-2018 | IPv4:1.0.11.31 | 10000 | All | All    | ADD       |
| 01-03-2018 | IPv4:51.1.1.99 | 30006 | All | All    | ADD       |
| 01-03-2018 | IPv4:40.1.1.81 | 30003 | All | All    | ADD       |
| 01-03-2018 | IPv4:51.1.1.19 | 30006 | All | All    | ADD       |
| 01-03-2018 | IPv4:1.0.13.45 | 10000 | All | All    | ADD       |
| 01-03-2018 | IPv4:1.0.15.20 | 10000 | All | All    | ADD       |
| 01-03-2018 | IPv4:1.0.11.44 | 10000 | All | All    | ADD       |
| 01-03-2018 | IPv4:1.0.5.166 | 10000 | All | All    | ADD       |
| 01-03-2018 | IPv4:40.1.1.14 | 30003 | All | All    | ADD       |

- **Operational Heatmap**—This view displays a heat-map of all endpoint operations occurring in the fabric.



The heat-map is color coded and the intensity of the color varies based on the number of endpoint operations captured on an hourly basis. The break down is available per hour across dates, and user can see the details of operations that occurred during a particular hour on a particular day by clicking on the appropriate square. The figure below depicts the endpoint operations reported by BGP on 01-02-2018 between 12 and 1pm.

< Back to Graph

Complete data set will be available in the downloaded csv. [Download](#)

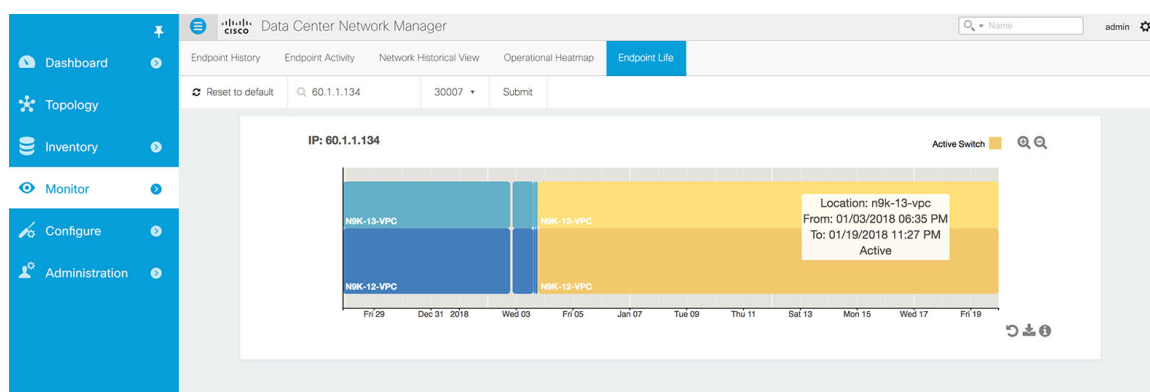
OPERATIONS: 01-02-2018 12:00PM - 1:00PM

| Time                | VRF | IP        | MAC               | Switch Name | Operation | VLAN |
|---------------------|-----|-----------|-------------------|-------------|-----------|------|
| 2018-01-02 12:00:20 | foo | 1.0.0.231 | 00:00:00:2e:ee:8b | n9k-13-vpc  | ADD       | 10   |
| 2018-01-02 12:00:20 | foo | 1.0.0.232 | 00:00:00:2e:ee:8d | n9k-13-vpc  | ADD       | 10   |
| 2018-01-02 12:00:24 | foo | 1.0.1.196 | 00:00:00:2e:f0:45 | n9k-13-vpc  | ADD       | 10   |
| 2018-01-02 12:00:25 | foo | 1.0.1.198 | 00:00:00:2e:f0:49 | n9k-13-vpc  | ADD       | 10   |
| 2018-01-02 12:00:08 | foo | 1.0.0.226 | 00:00:00:2e:ee:81 | n9k-13-vpc  | ADD       | 10   |
| 2018-01-02 12:00:17 | foo | 1.0.0.230 | 00:00:00:2e:ee:89 | n9k-13-vpc  | ADD       | 10   |
| 2018-01-02 12:00:26 | foo | 1.0.1.199 | 00:00:00:2e:f0:4b | n9k-13-vpc  | ADD       | 10   |
| 2018-01-02 12:00:28 | foo | 1.0.1.200 | 00:00:00:2e:f0:4d | n9k-13-vpc  | ADD       | 10   |
| 2018-01-02 12:00:32 | foo | 1.0.1.203 | 00:00:00:2e:f0:53 | n9k-13-vpc  | ADD       | 10   |
| 2018-01-02 12:00:33 | foo | 1.0.1.204 | 00:00:00:2e:f0:55 | n9k-13-vpc  | ADD       | 10   |

Again, as with the other views, the complete data set can be downloaded in csv format using the Download option. A sample screenshot of a downloaded csv file is shown below:

|    | A         | B         | C                 | D      | E      | F           | G         | H              | I         | J         | K         | L                 | M          | N         | O      | P         | Q         | R         | S       | T   | U         | V          | W     | X          | Y              | Z          | AA     | AB |
|----|-----------|-----------|-------------------|--------|--------|-------------|-----------|----------------|-----------|-----------|-----------|-------------------|------------|-----------|--------|-----------|-----------|-----------|---------|-----|-----------|------------|-------|------------|----------------|------------|--------|----|
|    | Fabric_ID | IP        | MAC               | L2_VNI | L3_VNI | Switch_Type | Switch_IP | Orig_Switch_IP | Orig_IP_1 | Orig_IP_2 | Orig_IP_3 | Switch_Nestlog_IP | Port       | VLAN      | L3_INT | Operation | EndpointT | Timestamp | Seq_Num | VSE | Br_Domain | Cluster    | Valid | Operation  | RouteID        | EndpointID | Filter |    |
| 1  | evpn      | 1.0.0.231 | 00:00:00:2e:ee:8b | 100000 | 50000  | n9k-13-vp   | N9K       | 24.21.0.13     | 30.1.1.14 | 0.0.0.0   | 0.0.0.0   | 0.0.0.0           | 30.1.1.200 | port-chan | 10     | 10        | ADD       | Wed Jan 2 | 0       | foo | 10        | 30.1.1.200 | 1     | 30.1.1.211 | IPv4-1.0.0.231 | 10000      |        |    |
| 2  | evpn      | 1.0.0.232 | 00:00:00:2e:ee:8d | 100000 | 50000  | n9k-13-vp   | N9K       | 24.21.0.13     | 30.1.1.14 | 0.0.0.0   | 0.0.0.0   | 0.0.0.0           | 30.1.1.200 | port-chan | 10     | 10        | ADD       | Wed Jan 2 | 0       | foo | 10        | 30.1.1.200 | 1     | 30.1.1.211 | IPv4-1.0.0.232 | 10000      |        |    |
| 3  | evpn      | 1.0.1.196 | 00:00:00:2e:f0:45 | 100000 | 50000  | n9k-13-vp   | N9K       | 24.21.0.13     | 30.1.1.14 | 0.0.0.0   | 0.0.0.0   | 0.0.0.0           | 30.1.1.200 | port-chan | 10     | 10        | ADD       | Wed Jan 2 | 0       | foo | 10        | 30.1.1.200 | 1     | 30.1.1.211 | IPv4-1.0.1.196 | 10000      |        |    |
| 4  | evpn      | 1.0.1.198 | 00:00:00:2e:f0:49 | 100000 | 50000  | n9k-13-vp   | N9K       | 24.21.0.13     | 30.1.1.14 | 0.0.0.0   | 0.0.0.0   | 0.0.0.0           | 30.1.1.200 | port-chan | 10     | 10        | ADD       | Wed Jan 2 | 0       | foo | 10        | 30.1.1.200 | 1     | 30.1.1.211 | IPv4-1.0.1.198 | 10000      |        |    |
| 5  | evpn      | 1.0.0.226 | 00:00:00:2e:ee:81 | 100000 | 50000  | n9k-13-vp   | N9K       | 24.21.0.13     | 30.1.1.14 | 0.0.0.0   | 0.0.0.0   | 0.0.0.0           | 30.1.1.200 | port-chan | 10     | 10        | ADD       | Wed Jan 2 | 0       | foo | 10        | 30.1.1.200 | 1     | 30.1.1.211 | IPv4-1.0.0.226 | 10000      |        |    |
| 6  | evpn      | 1.0.0.230 | 00:00:00:2e:ee:89 | 100000 | 50000  | n9k-13-vp   | N9K       | 24.21.0.13     | 30.1.1.14 | 0.0.0.0   | 0.0.0.0   | 0.0.0.0           | 30.1.1.200 | port-chan | 10     | 10        | ADD       | Wed Jan 2 | 0       | foo | 10        | 30.1.1.200 | 1     | 30.1.1.211 | IPv4-1.0.0.230 | 10000      |        |    |
| 7  | evpn      | 1.0.1.199 | 00:00:00:2e:f0:4b | 100000 | 50000  | n9k-13-vp   | N9K       | 24.21.0.13     | 30.1.1.14 | 0.0.0.0   | 0.0.0.0   | 0.0.0.0           | 30.1.1.200 | port-chan | 10     | 10        | ADD       | Wed Jan 2 | 0       | foo | 10        | 30.1.1.200 | 1     | 30.1.1.211 | IPv4-1.0.1.199 | 10000      |        |    |
| 8  | evpn      | 1.0.1.200 | 00:00:00:2e:f0:4d | 100000 | 50000  | n9k-13-vp   | N9K       | 24.21.0.13     | 30.1.1.14 | 0.0.0.0   | 0.0.0.0   | 0.0.0.0           | 30.1.1.200 | port-chan | 10     | 10        | ADD       | Wed Jan 2 | 0       | foo | 10        | 30.1.1.200 | 1     | 30.1.1.211 | IPv4-1.0.1.200 | 10000      |        |    |
| 9  | evpn      | 1.0.1.203 | 00:00:00:2e:f0:53 | 100000 | 50000  | n9k-13-vp   | N9K       | 24.21.0.13     | 30.1.1.14 | 0.0.0.0   | 0.0.0.0   | 0.0.0.0           | 30.1.1.200 | port-chan | 10     | 10        | ADD       | Wed Jan 2 | 0       | foo | 10        | 30.1.1.200 | 1     | 30.1.1.211 | IPv4-1.0.1.203 | 10000      |        |    |
| 10 | evpn      | 1.0.1.204 | 00:00:00:2e:f0:55 | 100000 | 50000  | n9k-13-vp   | N9K       | 24.21.0.13     | 30.1.1.14 | 0.0.0.0   | 0.0.0.0   | 0.0.0.0           | 30.1.1.200 | port-chan | 10     | 10        | ADD       | Wed Jan 2 | 0       | foo | 10        | 30.1.1.200 | 1     | 30.1.1.211 | IPv4-1.0.1.204 | 10000      |        |    |
| 11 | evpn      | 1.0.2.188 | 00:00:00:2e:f2:35 | 100000 | 50000  | n9k-13-vp   | N9K       | 24.21.0.13     | 30.1.1.14 | 0.0.0.0   | 0.0.0.0   | 0.0.0.0           | 30.1.1.200 | port-chan | 10     | 10        | ADD       | Wed Jan 2 | 0       | foo | 10        | 30.1.1.200 | 1     | 30.1.1.211 | IPv4-1.0.2.188 | 10000      |        |    |
| 12 | evpn      | 1.0.2.194 | 00:00:00:2e:f2:41 | 100000 | 50000  | n9k-13-vp   | N9K       | 24.21.0.13     | 30.1.1.14 | 0.0.0.0   | 0.0.0.0   | 0.0.0.0           | 30.1.1.200 | port-chan | 10     | 10        | ADD       | Wed Jan 2 | 0       | foo | 10        | 30.1.1.200 | 1     | 30.1.1.211 | IPv4-1.0.2.194 | 10000      |        |    |
| 13 | evpn      | 1.0.0.217 | 00:00:00:2e:ee:f  | 100000 | 50000  | n9k-12-vp   | N9K       | 24.21.0.12     | 30.1.1.14 | 0.0.0.0   | 0.0.0.0   | 0.0.0.0           | 30.1.1.200 | port-chan | 10     | 10        | ADD       | Wed Jan 2 | 0       | foo | 10        | 30.1.1.200 | 1     | 30.1.1.211 | IPv4-1.0.0.217 | 10000      |        |    |
| 14 | evpn      | 1.0.0.223 | 00:00:00:2e:ee:7b | 100000 | 50000  | n9k-12-vp   | N9K       | 24.21.0.12     | 30.1.1.14 | 0.0.0.0   | 0.0.0.0   | 0.0.0.0           | 30.1.1.200 | port-chan | 10     | 10        | ADD       | Wed Jan 2 | 0       | foo | 10        | 30.1.1.200 | 1     | 30.1.1.211 | IPv4-1.0.0.223 | 10000      |        |    |
| 15 | evpn      | 1.0.0.236 | 00:00:00:2e:ee:87 | 100000 | 50000  | n9k-13-vp   | N9K       | 24.21.0.13     | 30.1.1.14 | 0.0.0.0   | 0.0.0.0   | 0.0.0.0           | 30.1.1.200 | port-chan | 10     | 10        | ADD       | Wed Jan 2 | 0       | foo | 10        | 30.1.1.200 | 1     | 30.1.1.211 | IPv4-1.0.0.236 | 10000      |        |    |

- Endpoint Life**—This view displays a time line of a particular endpoint in its entire existence within the fabric. Specifically, given an identity of an endpoint in terms of its IP address and VRF/Network-identifier, the output displays the list of switches that an endpoint was present under including the associated start and end dates. This view is essentially the network life view of an endpoint. If the endpoint is viewed as active by the network, it will have a band here. If an endpoint is dual-homed, then there will be 2 horizontal bands reporting the endpoint existence, one band for each switch (typically the VPC pair of switches). As endpoints move within the network, for example with VM move, this view provides a succinct and intuitive pictorial view of this activity.



The underlying data that drives this view can also be downloaded in csv format (shown below) by clicking on download icon on right bottom corner.

|    | A           | B           | C                     | D                                                       | E                                                       | F      |
|----|-------------|-------------|-----------------------|---------------------------------------------------------|---------------------------------------------------------|--------|
| 1  | Switch Name | VRF         | EndPointIdentifier    | Start Timestamp                                         | End Timestamp                                           | Active |
| 2  | n9k-12-vpc  | Beer:Corona | IPv4:60.1.1.134:30007 | Wed Dec 27 2017 21:41:33 GMT+0530 (India Standard Time) | Tue Jan 02 2018 18:56:32 GMT+0530 (India Standard Time) |        |
| 3  | n9k-13-vpc  | Beer:Corona | IPv4:60.1.1.134:30007 | Wed Dec 27 2017 21:41:49 GMT+0530 (India Standard Time) | Tue Jan 02 2018 18:56:33 GMT+0530 (India Standard Time) |        |
| 4  | n9k-12-vpc  | Beer:Corona | IPv4:60.1.1.134:30007 | Tue Jan 02 2018 20:54:21 GMT+0530 (India Standard Time) | Wed Jan 03 2018 14:25:02 GMT+0530 (India Standard Time) |        |
| 5  | n9k-13-vpc  | Beer:Corona | IPv4:60.1.1.134:30007 | Tue Jan 02 2018 20:54:21 GMT+0530 (India Standard Time) | Wed Jan 03 2018 14:24:45 GMT+0530 (India Standard Time) |        |
| 6  | n9k-12-vpc  | Beer:Corona | IPv4:60.1.1.134:30007 | Wed Jan 03 2018 14:35:40 GMT+0530 (India Standard Time) | Wed Jan 03 2018 16:09:09 GMT+0530 (India Standard Time) |        |
| 7  | n9k-13-vpc  | Beer:Corona | IPv4:60.1.1.134:30007 | Wed Jan 03 2018 14:35:44 GMT+0530 (India Standard Time) | Wed Jan 03 2018 16:09:10 GMT+0530 (India Standard Time) |        |
| 8  | n9k-12-vpc  | Beer:Corona | IPv4:60.1.1.134:30007 | Wed Jan 03 2018 16:15:18 GMT+0530 (India Standard Time) | Wed Jan 03 2018 18:02:49 GMT+0530 (India Standard Time) |        |
| 9  | n9k-13-vpc  | Beer:Corona | IPv4:60.1.1.134:30007 | Wed Jan 03 2018 16:15:18 GMT+0530 (India Standard Time) | Wed Jan 03 2018 18:02:48 GMT+0530 (India Standard Time) |        |
| 10 | n9k-12-vpc  | Beer:Corona | IPv4:60.1.1.134:30007 | Wed Jan 03 2018 18:35:09 GMT+0530 (India Standard Time) |                                                         | TRUE   |
| 11 | n9k-13-vpc  | Beer:Corona | IPv4:60.1.1.134:30007 | Wed Jan 03 2018 18:35:12 GMT+0530 (India Standard Time) |                                                         | TRUE   |





## Media Controller

This section contains context sensitive online help content under the **Web Client > Media Controller** tab.



### Note

This feature is available only if you have enabled the Media Controller feature explicitly, after the Cisco DCNM OVA/ISO installation is complete. For more information, see the *Cisco DCNM Installation Guide*.

Logon to the DCNM OVA/ISO through SSH and use the **appmgr set-mode media-controller** command to enable the Media Controller feature. Ensure that you stop the DCNM application using the **appmgr stop dcnm** command before you execute the **appmgr set-mode media-controller** command.

This feature is available only if you have enabled Media Controller during the installation process. To enable Media Controller, you have to choose the **IP-Fabric Media Controller** installation option during the OVA/ISO installation for DCNM. The **appmgr set-mode media-controller** command, used in earlier releases, is not available in DCNM 10.4(2).

To bring up the devices from the basic configuration using POAP, you must define the templates and publish the POAP definition through Cisco DCNM **Web Client > Configure > Deploy > POAP Definitions**. For more information, see [POAP Launchpad, on page 124](#).



### Note

Specific POAP templates for Leaf and Spine for the Media Controller deployment are packaged with the Cisco DCNM Software.

If you have configured the Cisco DCNM server in Media Controller mode and performed the procedure mentioned in the "POAP Launchpad" section, you will be able to see the Media Controller templates. Cisco DCNM Web Client allows you to choose the required templates, edit them as required, and publish the POAP definition.

For information about the Media Controller APIs, see the [Cisco DCNM Media Controller API reference](#) on Cisco DevNet.

- [Media Controller Topology, page 96](#)
- [PMN Hosts, page 97](#)
- [Flow Alias, page 101](#)
- [Policies, page 103](#)

- [Flow Status, page 110](#)
- [Events, page 113](#)

## Media Controller Topology

You can view the Media Controller topology on the **Web Client > Media Controller > Topology** page. This topology is specific to the Media Controller.



### Note

This feature is available only if you have enabled Media Controller during the installation process. To enable Media Controller, you have to choose the **IP-Fabric Media Controller** installation option during the OVA/ISO installation for DCNM. The **appmgr set-mode media-controller** command, used in earlier releases, is not available in DCNM 10.4(2).

From release 10.3(2) onwards, vPC support for Media Controller is added in DCNM. If the vPC pair of switches is Cisco Nexus 9000 Series switches, the representation can be seen in the topology.

### Quick Search

Enter the search string to highlight relevant devices.

The following fields are available to search on: **switch or hostname, switch or host IP address, switch MAC, and switch serial number.**

### Multicast Group

Right-click (or press Return Key) in the field. A list of Multicast Addresses will be displayed. You can choose the multicast IP address for which you need to view the topology.

The devices under this multicast IP address, and links to spine and leaf are highlighted. The dotted moving lines depict the flow of traffic in the Media Controller topology.

You can search or filter based on flow alias name in the Topology. When you search for Multicast Group, you can search using the IP address or flow alias name.

### Show Panel > Bandwidth

Check the **Bandwidth** checkbox, the bandwidth consumed by the spine and leaf are displayed as color indicators.

- Green—Less than 40%
- Yellow—Between 40% and 80%
- Red—More than 80%

The display format is *Transmitted-Received*.

In a typical Media Controller Fabric, the ISL links are configured between the leaves and the spines, and ISL links help Cisco DCNM to calculate the bandwidth required to stitch flows. If there is a faulty configuration, the Cisco DCNM bandwidth manager may determine the wrong link.

The Cisco DCNM bandwidth computation algorithm attempts to find a common node between the sender and the receiver.

### Bandwidth Tracking on Host Facing Link

The senders and receivers can connect to Leaf switches of the PMN Fabric. The sender initiates a multicast flow and the receiver subscribes to a multicast flow. Since multicast is used, there can be multiple receivers subscribing to a flow. The senders are devices such as cameras, microphones, playback devices etc. The receivers are devices such as video monitors, speakers, multi-viewers etc.



#### Note

The host port bandwidth tracking can be enabled or disabled via the **pmn.host.port.policing.enabled** field in the **Web Client > Administration > DCNM Server > Server Properties** page. By default, the host port bandwidth tracking is disabled.

You can track the bandwidth on the host facing link. Using this functionality, DCNM do not allows the receiver to request for more flows or sender to send more flows than the available bandwidth on the host facing link.

## PMN Hosts

Cisco DCNM allows you to create hosts for Media Controller. The active transmitting and receiving devices are termed as hosts. The hosts can be configured on **Cisco Web Client > Media Controller > Hosts**.



#### Note

The PMN Hosts table is auto-populated once the traffic begins.

The following table describes the fields that appear on this page.

**Table 11: Operations on PMN Hosts**

| Field  | Description                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------|
| Add    | Allows you to add a new host.                                                                                     |
| Edit   | Allows you to view or edit the selected host parameters.                                                          |
| Delete | Allows you to remove the host from the fabric.                                                                    |
| Import | Allows you to import host parameters from your local directory.                                                   |
| Export | Allows you to export host parameters information to your local directory.<br>The exported file is in .csv format. |

**Table 12: PMN Hosts Table Field and Description**

| Field    | Description                                        |
|----------|----------------------------------------------------|
| Hostname | Specifies the configured name for the host device. |

| Field            | Description                                                                                                                                                                                                                                                                      |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP Address       | Specifies the IP address for the host.<br><b>Attention</b> You should not create a host using a WAN interface IP address since any host policy that is subsequently created using the WAN interface IP address may result in unexpected behavior.                                |
| MAC Address      | Specifies the MAC address of the host switch.                                                                                                                                                                                                                                    |
| Switch Name      | Specifies the name of the switch.<br><b>Note</b> Switches in the <b>Switch Name</b> and <b>Peer Switch Name</b> columns form a Virtual Port Channel (vPC) pair of switches. If the switch is not part of a vPC setup, the <b>Peer Switch Name</b> column will not have an entry. |
| Interface Name   | Specifies the name of switch interface which the host is associated with.                                                                                                                                                                                                        |
| Peer Switch Name | Specifies the vPC peer switch name, for a vPC setup.                                                                                                                                                                                                                             |
| Remote Host      | Specifies if the host is local to the DCNM managed fabric or belongs to an external fabric.<br><br>A remote host can be identified by the <b>Remote</b> label on the host icon in the Topology page.                                                                             |

vPC support—From the 10.3(2) release, the DCNM Media Controller provides vPC support for vPC topologies. Pointers:

- DCNM will display two local flows in the topology screen.
- For multicast traffic that passes through the vPC switch pair, DCNM elects the forwarder and non-forwarder switches. However, DCNM does not police the downstream link or vPC peer link for bandwidth management.
- Multicast traffic pertaining to a Layer-2 or Layer-3 host attached to an orphan port is not supported. DCNM 10.3(2) only supports a Layer-2 orphan host that is associated with a vPC VLAN.
- When vPC uplink and vPC peer link failures occur, DCNM will trigger the active flows that need to be migrated.

This section contains the following:



**Note**

Starting from DCNM 10.4(2), the multisite option is supported. With this option, flows can be provisioned across multiple sites. You need to enable multisite support and receiver bandwidth management by setting the `pmn.multi-site.enabled` and `pmn.host.port.policing.enabled` functions to true, using the **Administration > DCNM Server > Server Properties** option, and restarting DCNM. The sender side bandwidth management for multisite is enforced by the switch and is enabled by default. Multisite support is only available for Source Specific Multicast (SSM), and border leaf switches in a vPC setup are not supported. DCNM detects the PMN border leaf switch role during discovery and depicts the PMN border leaf switch separately on the topology screen.

## Add PMN Hosts

To add hosts, perform the steps below.

### Procedure

- Step 1** From the menu bar, select **Media controller > Hosts**.
- Step 2** Click **Add** host icon.
- Step 3** In the Add Hosts window, specify the parameters in the following fields.
  - **Name**—Specify a unique name for the host device.
  - **IP Address**—Specify the IP Address of the host device.
  - (Optional) **MAC Address**—Specify the MAC address of the host device.
- Step 4** Click **Save** to configure the host.

## Edit PMN Hosts

To edit or view the host parameters, perform the steps below.

### Procedure

- Step 1** From the menu bar, select **Media controller > Hosts**.
- Step 2** Check the check box next to the host name, that you need to edit.
- Step 3** Click **Edit** host icon.
- Step 4** In the Edit Hosts window, edit the parameters in the **Name** and **MAC Address** fields.
- Step 5** Click **Save** to save the changes. Click **Cancel** to revert the host with same parameters.

## Delete PMN Hosts

To delete a host, perform the steps below.

### Procedure

---

- Step 1** From the menu bar, select **Media controller > Hosts**.
  - Step 2** Check the check box next to the host name, that you need to delete.  
You can select more than one host to delete.
  - Step 3** Click **Delete** host icon.
  - Step 4** In the delete notification, click **Yes** to delete the host. Click **No** to cancel this action.  
A Delete Host successful message appears at the bottom of the page.
- 

## Import PMN Hosts

To import hosts, perform the steps below.

### Procedure

---

- Step 1** From the menu bar, select **Media Controller > Hosts**.
  - Step 2** Click **Import** host icon.
  - Step 3** Browse the directory and select the file which contains the Host configuration information.
  - Step 4** Click **Open**.  
The host(s) configuration is imported and displayed on **Media Controller > Hosts** on the Cisco DCNM Web Client.
- 

## Export PMN Hosts

To export hosts, perform the steps below.

### Procedure

---

- Step 1** From the menu bar, select **Media Controller > Hosts**.
- Step 2** Click **Export** host icon.  
A notification window appears.
- Step 3** Select a location on your directory to store the Hosts configuration file.
- Step 4** Click **OK**.

The host(s) configuration file is exported to your local directory. The file name is appended with the date on which the file is exported. The format of the exported file is `.csv`.

## Flow Alias

Using the Flow Alias feature, you can specify names for multicast groups. The multicast IP addresses are difficult to remember, thus by assigning a name to the multicast IP address, you can search and add policies based on the name.

You can configure flow alias on **Cisco Web Client > Media Controller > Flow Alias**.

The following table describes the fields that appear on this page.

**Table 13: Flow Alias Table Field and Description**

| Field                | Description                                                    |
|----------------------|----------------------------------------------------------------|
| Flow Alias           | Specifies the name of the Flow Alias.                          |
| Multicast IP Address | Specifies the multicast IP address for the traffic.            |
| Description          | Description added to the Flow Alias.                           |
| Last Updated at      | Specifies the date on which the flow alias was last updated. . |

This section contains the following:

## Add Flow Alias

To add flow alias, perform the steps below.

### Procedure

- Step 1** From the menu bar, select **Media controller > Flow Alias**.
- Step 2** Click **Add Flow Alias** icon.
- Step 3** In the Add Flow Alias window, specify the parameters in the following fields.
  - **Flow Name**—Specifies a unique flow alias name.
  - **Multicast IP Address**—Specifies the multicast IP Address for the flow alias.
  - **Description**—Specifies the description that you add for the flow alias.
- Step 4** Click **Save** to save the flow alias.

## Edit Flow Alias

To edit a flow alias, perform the steps below.

### Procedure

---

- Step 1** From the menu bar, select **Media controller > Flow Alias**.
  - Step 2** Check the check box next to the flow alias name, that you need to edit.
  - Step 3** Click **Edit** Flow Alias icon.
  - Step 4** In the Edit Flow Alias window, edit the **Name**, **Multicast IP**, **Description** fields.
  - Step 5** Click **Save** to save the new configuration.
- 

## Delete Flow Alias

To delete flow alias, perform the steps below.

### Procedure

---

- Step 1** From the menu bar, select **Media controller > Flow Alias**.
  - Step 2** Check the check box next to the flow alias, that you need to delete.  
You can select more than one flow alias to delete.
  - Step 3** Click **Delete** Flow Alias icon.  
The flow alias is deleted.
- 

## Export Flow Alias

To export host alias, perform the steps below.

### Procedure

---

- Step 1** From the menu bar, select **Media controller > Flow Alias**.
- Step 2** Click **Export** flow alias icon.  
A notification window appears.
- Step 3** Select a location on your directory to store the Alias details file.
- Step 4** Click **OK**.

The flow alias file is exported to your local directory. The file name is appended with the date on which the file is exported. The format of the exported file is `.csv`.

## Import Flow Alias

To import flow alias, perform the steps below.

### Procedure

- Step 1** From the menu bar, select **Media controller > Flow Alias**.
- Step 2** Click **Import** flow alias icon.
- Step 3** Browse the directory and select the file which contains the Flow Alias configuration information.
- Step 4** Click **Open**.  
The flow alias configuration is imported and displayed on **Media Controller > Flow Alias** on the Cisco DCNM Web Client.

## Policies

### Host Policies

You can add policies to the host devices. The hosts policies are can be configured on **Cisco Web Client > Media Controller > Policies > Host Policies**.



#### Note

A non-default host policy can only be created for a known host.

The following table describes the fields that appear on this page.

**Table 14: Host Policies Operations**

| Field  | Description                                                                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Add    | Allows you to add a new host policy.                                                                                                           |
| Edit   | Allows you to view or edit the selected host policy parameters.                                                                                |
| Delete | Allows you to delete the user-defined host policy.<br><b>Note</b> You cannot edit the default policy, if it is already applied to the devices. |

| Field  | Description                                                 |
|--------|-------------------------------------------------------------|
| Import | Allows you to import host policies from your directory.     |
| Export | Allows you to export host policies to your local directory. |

**Table 15: Host Policies Table Field and Description**

| Field              | Description                                                                                                                                                         |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policy Name        | Specifies the policy name for the host.<br>By default, the default host policies will have the Operation set to permit.                                             |
| Host               | Specifies the host ID.                                                                                                                                              |
| Multicast IP       | Specifies the multicast IP address for the host.                                                                                                                    |
| Flow Alias         | Specifies the name of the Flow Alias.                                                                                                                               |
| Host Acting As     | Specifies the host device role. The host device role is either one of the following: <ul style="list-style-type: none"> <li>• Sender</li> <li>• Receiver</li> </ul> |
| Operation          | Specifies if the operation of the host policy. The policy has the following operations: <ul style="list-style-type: none"> <li>• Permit</li> <li>• Deny</li> </ul>  |
| Devices Applied To | Specifies the number of devices to which this policy is applied.                                                                                                    |
| PIM Policy         | Specifies if Protocol Independent Multicast (PIM) configuration is applicable for the host policy.                                                                  |
| Last Updated       | Specifies the date and time at which the host policy was last updated.<br>The format is <i>Day MMM DD YYYY HH:MM:SS Timezone</i> .                                  |

This section contains the following:

## Add Host Policy

To add Host policy, perform the steps below.

### Procedure

---

- Step 1** From the menu bar, select **Media controller > Policies > Host Policies**.
- Step 2** Click **Add** Host policy icon.
- Step 3** In the Add Host Policy window, specify the parameters in the following fields.
- **Policy Name**—Specifies a unique policy name for the flow policy.
  - **Host Role**—Specifies the host as a multicast sender or multicast receiver. Select **Sender** or **Receiver** from the drop-down list.
  - **PIM Policy**—Select the check box if PIM configuration is needed for the host policy. The PIM Policy checkbox is only applicable for the receiver role. If PIM policy is enabled, the Host field will be disabled since the PIM policy is only applicable for the receiver and it is applied to the multicast group.
  - **Host**—Specifies the host to which the policy is applied. The value can be chosen from the drop-down list.  
**Note** You should not select hosts that are discovered as remote receivers to create receiver/sender host policies. However, hosts that are discovered as remote senders can be used for creating sender host policies.
  - **Multicast IP**—Specifies the multicast IP Address for the flow policy.
  - **Allow/Deny**—Click the radio button to choose, if the policy must **Allow** or **Deny** the traffic flow.
- Step 4** Click **Save** to configure the host policy.
- 

## Edit Host Policy

To add host policy, perform the steps below.

### Procedure

---

- Step 1** From the menu bar, select **Media controller > Policies > Host Policies**.
- Step 2** Check the check box next to the host policy name, that you need to edit.
- Step 3** Click **Edit** Host policy icon.
- Step 4** In the Edit Host Policy window, edit to specify if the policy will **Allow** or **Deny** traffic.  
**Note** The changes made to Host Policy is applied immediately. If the policy is already applied to any device, the changes may impact the existing flows.
- Step 5** Click **Save** to save the new configuration.
- 

## Delete Host Policy

To delete host policy, perform the steps below.



---

**Note** You can delete only user-defined Host Policies.

---

### Procedure

---

- Step 1** From the menu bar, select **Media controller > Policies > Host Policies**.
- Step 2** Check the check box next to the host policy name, that you need to delete.  
You can select more than one host policy to delete.
- Step 3** Click **Delete** Host policy icon.
- Step 4** In the delete notification, click **OK** to delete the host policy. Click **Cancel** to return to the Host Policies page.
- Note** Deleting the host policy results in Policy Enforcement on the Leaf to which this policy is applied.  
A Delete Host policy successful message appears at the bottom of the page.
- 

## Import Host Policy

To import host policies, perform the steps below.

### Procedure

---

- Step 1** From the menu bar, select **Media controller > Policies > Host Policies**.
- Step 2** Click **Import** host policy icon.
- Step 3** Browse the directory and select the file which contains the Host Policy configuration information.
- Step 4** Click **Open**.  
The host policy configuration is imported and displayed on **Media Controller > Hosts > Host Policies** on the Cisco DCNM Web Client.
- 

## Export Host Policy

To export host policies, perform the steps below.

### Procedure

---

- Step 1** From the menu bar, select **Media controller > Policies > Host Policies**.
- Step 2** Click **Export** host policy icon.  
A notification window appears.
- Step 3** Select a location on your directory to store the Host Policy details file.
- Step 4** Click **OK**.



The host policy file is exported to your local directory. The file name is appended with the date on which the file is exported. The format of the exported file is `.csv`.

## Flow Policies

You can configure flow policies on **Cisco Web Client > Media Controller > Policies > Flow Policies**.

The following table describes the fields that appear on this page.

**Table 16: Flow Policies Operations**

| Field  | Description                                                     |
|--------|-----------------------------------------------------------------|
| Add    | Allows you to add a new flow policy.                            |
| Edit   | Allows you to view or edit the selected flow policy parameters. |
| Delete | Allows you to delete the user-defined flow policy.              |
| Import | Allows you to import flow policies from your directory.         |
| Export | Allows you to export flow policies to your local directory.     |

**Table 17: Flow Policies Table Field and Description**

| Field        | Description                                                                                                                        |
|--------------|------------------------------------------------------------------------------------------------------------------------------------|
| Policy Name  | Specifies the flow policy name.<br>By default, the default host policies will have the Operation set to permit.                    |
| Multicast IP | Specifies the multicast IP address for the traffic.                                                                                |
| Flow Alias   | Specifies the name of the Flow Alias.                                                                                              |
| Bandwidth    | Specifies the bandwidth allotted for the traffic.                                                                                  |
| QoS/DSCP     | Specifies the Switch-defined QoS Policy.                                                                                           |
| Last Updated | Specifies the date and time at which the host policy was last updated.<br>The format is <i>Day MMM DD YYYY HH:MM:SS Timezone</i> . |

**Note**

A new flow policy or a edited flow policy will be effective only under the following circumstances.

- If the new flow matches the existing flow policy.
- If the flow expires and reforms, while the new policy is already added or edited, that matches with the flow policy.

This section contains the following:

## Add Flow Policy

To add flow policy, perform the steps below.

### Procedure

- Step 1** From the menu bar, select **Media controller > Policies > Flow Policies**.
- Step 2** Click **Add** Flow policy icon.
- Step 3** In the Add Flow Policy window, specify the parameters in the following fields.
  - **Policy Name**—Specifies a unique policy name for the flow policy.
  - **Multicast IP**—Specifies the multicast IP Address for the flow policy.
  - **Bandwidth**—Specifies the bandwidth allocated for the flow policy. Select of the radio buttons to choose **Gbps** or **Mbps**.
- Step 4** From the **QoS/DSCP** drop-down list, choose an appropriate ENUM value.
- Step 5** Click **Save** to configure the flow policy.

## Edit Flow Policy

To add flow policy, perform the steps below.

### Procedure

- Step 1** From the menu bar, select **Media controller > Policies > Flow Policies**.
- Step 2** Check the check box next to the flow policy name, that you need to edit.
- Step 3** Click **Edit** Flow policy icon.
- Step 4** In the Edit Flow Policy window, edit the **Multicast IP**, **Bandwidth**, **QoS/DSCP** fields.
- Step 5** Click **Save** to save the new configuration.

## Delete Flow Policy

To delete flow policy, perform the steps below.

### Procedure

---

- Step 1** From the menu bar, select **Media controller > Policies > Flow Policies**.
  - Step 2** Check the check box next to the flow policy name, that you need to delete.  
You can select more than one flow policy to delete.
  - Step 3** Click **Delete** Flow policy icon.  
The flow policy is deleted.
- 

## Import Flow Policy

To import flow policies, perform the steps below.

### Procedure

---

- Step 1** From the menu bar, select **Media controller > Policies > Flow Policies**.
  - Step 2** Click **Import** flow policy icon.
  - Step 3** Browse the directory and select the file which contains the Flow Policy configuration information.
  - Step 4** Click **Open**.  
The flow policy configuration is imported and displayed on **Media Controller > Hosts > Flow Policies** on the Cisco DCNM Web Client.
- 

## Export Flow Policy

To export host policies, perform the steps below.

### Procedure

---

- Step 1** From the menu bar, select **Media controller > Policies > Flow Policies**.
- Step 2** Click **Export** flow policy icon.  
A notification window appears.
- Step 3** Select a location on your directory to store the Flow Policy details file.
- Step 4** Click **OK**.  
The flow policy file is exported to your local directory. The file name is appended with the date on which the file is exported. The format of the exported file is `.csv`.

# Flow Status

Cisco DCNM allows you to view the flow status pictorially and statistically. The flow status is available on **Cisco Web Client > Media Controller > Flow Status**.



## Note

The flow status collection frequency and cache size can be specified via **cisco.pmn-stats-interval** and **cisco.pmn-stats-cache-size** respectively in the **Web Client > Administration > DCNM Server > Server Properties** page.

The following table describes the fields that appear on the Active tab.

**Table 18: Active Tab**

| Field              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Multicast IP       | Specifies the multicast IP address for the flow.<br><b>Note</b> You can click the wave link next to the Multicast IP address to view the pictorial representation of flow statistics.                                                                                                                                                                                                                                                                                                |
| Flow Alias         | Specifies the name of the Flow Alias.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Sender             | Specifies the IP address of the Source Specific Multicast (SSM) sender for the multicast group.                                                                                                                                                                                                                                                                                                                                                                                      |
| Receiver           | Specifies the name of the receiver.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| vPC Local Receiver | Specifies the name of the receiver host if the flow is a vPC local flow (the sender and receiver are on the same switch.)                                                                                                                                                                                                                                                                                                                                                            |
| Bandwidth          | Specifies the bandwidth allotted for the traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| QOS/DSCP           | Specifies the Switch-defined QoS Policy.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Flow Link State    | Click on the <b>READY</b> link state to view the network diagram of the Sender and Receiver.<br><br>The dotted line displays the direction of the flow of traffic.<br><br><b>vPC flow</b> —For multicast flows local to the vPC switch pair, the screen shows two identical flows. Click the READY link to see the actual path. For a multicast flow between a host attached to a vPC switch pair and a remote host, only one flow is displayed along with the vPC pair of switches. |

| Field               | Description                                                      |
|---------------------|------------------------------------------------------------------|
| Policy ID           | Specifies the policy ID applied to the multicast IP.             |
| Receiver Start Time | Displays the time from when the receiver begins to receive data. |

The following table describes the fields that appear on the Inactive tab.

**Table 19: Inactive Tab**

| Field             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Multicast IP      | Specifies the multicast IP address of the flow.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Flow Alias        | Specifies the name of the Flow Alias.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Sender            | Specifies the IP address of the Source Specific Multicast (SSM) sender for the multicast group.                                                                                                                                                                                                                                                                                                                                                                                            |
| Waiting Receivers | Specifies the potential multicast receivers that have subscribed to this group.                                                                                                                                                                                                                                                                                                                                                                                                            |
| Bandwidth         | Specifies the bandwidth allotted for the traffic.                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Flow Link State   | <p>Click on the <b>READY</b> link state to view the network diagram of the Sender and Receiver.</p> <p>The dotted line displays the direction of the flow of traffic.</p> <p><b>vPC flow</b>—For multicast flows local to the vPC switch pair, the screen shows two identical flows. Click the READY link to see the actual path. For a multicast flow between a host attached to a vPC switch pair and a remote host, only one flow is displayed along with the vPC pair of switches.</p> |
| Policy ID         | Specifies the policy ID applied to the multicast IP.                                                                                                                                                                                                                                                                                                                                                                                                                                       |

The following table describes the fields that appear on the Sender Only tab.

**Table 20: Sender Only Tab**

| Field        | Description                                      |
|--------------|--------------------------------------------------|
| Multicast IP | Specifies the multicast IP address for the flow. |
| Flow Alias   | Specifies the name of the Flow Alias.            |

| Field                    | Description                                                               |
|--------------------------|---------------------------------------------------------------------------|
| Name                     | Specifies the name of the sender.                                         |
| Sender Leaf IP           | Specifies the IP address of the sender that initiates the multicast flow. |
| Sender Leaf Name         | Specifies the name of the sender leaf.                                    |
| Sender Ingress Interface | Specifies the name of the sender ingress interface.                       |
| Policy ID                | Specifies the policy ID applied to the multicast IP.                      |
| Bandwidth                | Specifies the bandwidth allotted for the traffic.                         |
| State                    | Specifies the state of the flow link.                                     |

The following table describes the fields that appear on the Receiver Only tab.

**Table 21: Receiver Only Tab**

| Field                  | Description                                                                                                           |
|------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Multicast IP           | Specifies the multicast IP address for the flow.                                                                      |
| Flow Alias             | Specifies the name of the Flow Alias.                                                                                 |
| Name                   | Specifies the receiver ID. If the multicast receiver is remote, the <b>Remote</b> label can be seen next to its name. |
| Receiver Leaf IP       | Specifies the IP address of the destination switch that receives the multicast flow.                                  |
| Receiver Interface     | Specifies the name of the destination switch interface.                                                               |
| Receiver Leaf Name     | Specifies the name of the leaf switch to which the multicast receiver is attached.                                    |
| Source Specific Sender | Specifies the IP address of the multicast sender.                                                                     |
| Policy ID              | Specifies the policy ID applied to the multicast IP.                                                                  |
| Bandwidth              | Specifies the bandwidth allotted for the traffic.                                                                     |
| Number of Receivers    | Specifies the number of receivers allotted for the traffic.                                                           |
| State                  | Specifies the state of the flow link.                                                                                 |

Click on the **Show** drop-down list in the statistical representation area to display the statistical data in various formats.

Click on the arrow to export the statistical data. you can export it in .csv or .pdf formats.


**Note**

Cisco DCNM holds the Flow statistics values in the DCNM server internal memory. Therefore, after a DCNM Restart or HA switch over, the Flow statistics will not show previously collected values. However, you can see the Flow statistics that are collected after the server Restart or HA switch over.

If the new flow joins before the uplinks between the switches that are detected in DCNM, a message BW\_UNAVAIL appears. This is resolved after the uplinks between the switches are detected by DCNM after discovery of the devices.

## Events

Cisco DCNM allows you to view and purge the various events between the Host and Flow. The Events are recorded on **Cisco Web Client > Media Controller > Events**.

The PMN Events table is updated real-time.

The maximum stored PMN events and cleanup frequency can be specified via **pmn.rows.limit** and **pmn.delete.interval** respectively in the **Web Client > Administration > DCNM Server > Server Properties** page.

The following table describes the fields that appear on this page.

| Field    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Purge    | <p>Click to remove the old/unwanted events.</p> <p>Click one of the radio buttons to choose the Purge options.</p> <ul style="list-style-type: none"> <li>• <b>Max # of Records</b>—Enter the maximum number of records that you need to delete.</li> <li>• <b># of Days</b>—Enter the number of days for which you need to delete the events.</li> <li>• <b>Delete all data from the previous date</b>—Specifies a date before which all the data will be deleted.</li> </ul> <p>Click <b>Purge</b> to delete/retain PMN events information.</p> |
| Category | Specifies if the event category.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Severity | Specifies the severity of the event.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Field            | Description                                                                                                                                                                                                                                                                                                                                            |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description      | <p>Specifies the description of the event.</p> <p>The sample description appears as:</p> <pre>Creating flow for FlowRequest:The flowRequest is for hostId:&lt;&lt;IP_Address&gt;&gt; hostInterface:&lt;&lt;Host_Int_ID&gt;&gt; mcastIp:&lt;&lt;Multicast IP&gt;&gt; Is sender role:false originating from switch:&lt;&lt;Host IP Address&gt;&gt;</pre> |
| Impacted Flows   | Specifies the impacted flows due to this event.                                                                                                                                                                                                                                                                                                        |
| Last Update Time | <p>Specifies the date and time at which the event was last modified.</p> <p>The format is <i>Day MMM DD YYYY HH:MM:SS Timezone</i>.</p>                                                                                                                                                                                                                |
| Export           | <p>Allows you to download the events to a local directory path.</p> <p>The filename is appended with the date on which the file is exported. The format of the exported file is <i>.xls</i>.</p>                                                                                                                                                       |
|                  |                                                                                                                                                                                                                                                                                                                                                        |
|                  |                                                                                                                                                                                                                                                                                                                                                        |





## Configure

---

This section contains context-sensitive Online Help content for the **Web Client > Configure** tab.

- [Deploy, page 115](#)
- [Templates, page 141](#)
- [Backup, page 160](#)
- [Image Management, page 171](#)
- [Credentials Management, page 187](#)
- [LAN Fabric Settings, page 190](#)
- [LAN Fabric Provisioning, page 200](#)
- [LAN Fabric Auto-Configuration, page 245](#)
- [Endpoint Locator , page 260](#)
- [SAN, page 275](#)

## Deploy

The Deploy menu includes the following submenus:

### Configuring vPC Peer

A virtual PortChannel (vPC) allows links that are physically connected to two different Cisco Nexus devices to appear as a single PortChannel to a third device. The third device can be a Cisco Nexus 2000 Series Fabric Extender or a switch, server, or any other networking device. A vPC can provide Layer 2 multipathing, which allows you to create redundancy by increasing bandwidth, enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.

After you enable the vPC function, you create a peer keepalive link, which sends heartbeat messages between the two vPC peer devices.

The vPC domain includes both vPC peer devices, the vPC peer keepalive link, the vPC peer link, and all the PortChannels in the vPC domain connected to the downstream device. You can have only one vPC domain ID on each device.

vPC creation is divided into two steps, vPC Peer creation and vPC creation. In order to configure vPC user first needs to configure vPC domain. To create vPC Peer, navigate to **Configure > Deploy > vPC Peer**.


**Note**

After you configure the vPC peer, select vPC peer using the radio button and click **Add vPC**. For information about how to add a vPC to the selected vPC peer, see [Add vPC, on page 121](#).

You can view the history of tasks performed, navigate to **Configure > Deploy > vPC Peer > History** tab. For more information, see [vPC Peer History, on page 116](#).

You can view the list of vPC domains in the **Pre Configured Peers** table.

**Table 22: Pre Configured Peers**

| Column                    | Description                                                                                                     |
|---------------------------|-----------------------------------------------------------------------------------------------------------------|
| Search box                | Enter any string to filter the entries in their respective column.                                              |
| Domain ID                 | Displays the domain ID of the vPC peer switches.                                                                |
| Primary Switch            | Displays the vPC Primary device name.                                                                           |
| Primary Port Channel ID   | Displays the peer-link port channel for vPC primary device.                                                     |
| Secondary Switch          | Displays the vPC secondary device name.                                                                         |
| Secondary Port Channel ID | Displays the peer-link port channel for vPC secondary device.                                                   |
| Consistency               | Displays the vPC Consistency status. Corresponds vPC peer-link configuration and Global Consistency parameters. |

This feature supports add, delete and edit option for Domain. You can also view vPC Peer History.

## vPC Peer History

To view the deployed jobs on the vPC peers, navigate to **Configure > Deploy > vPC Peer > History** tab. You can view the list **vPC Peer History** information in the [Table 23: vPC Peer History, on page 117](#).

**Table 23: vPC Peer History**

| Column               | Description                                                                                                                                                                                                                           |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Domain Id            | Specifies the domain ID for the vPC peer                                                                                                                                                                                              |
| Primary Switch       | Specifies the Primary Switch associated with the vPC Peer.                                                                                                                                                                            |
| Secondary Switch     | Specifies the Secondary Switch associated with the vPC Peer.                                                                                                                                                                          |
| Created By           | Specifies the DCNM username, who deployed this task.                                                                                                                                                                                  |
| Started At           | Specifies the time at which the task was performed on the vPC peer.<br><br>The time is displayed in the format YYYY-MM-DD HH:MM:SS.                                                                                                   |
| Task Performed       | Specifies the task performed on the vPC peer.                                                                                                                                                                                         |
| Status               | Species the status of the task performed on the vPC Peer. The status can be Failed, Success, or in_progress.                                                                                                                          |
| View Command History | Select an activity, click <b>View Command History</b> .<br><br>The Command History page displays the commands executed, status and error message on the <b>Primary Switch</b> and <b>Secondary Switch</b> , in their respective tabs. |
| Delete vPC Peer Job  | Select a vPC Peer History entry and click <b>Delete</b> to delete the task history.                                                                                                                                                   |

## Add vPC Peer Wizard

You can launch the vPC Peer configuration wizard by clicking the **Add vPC Peer** icon in the toolbar.

### Procedure

- 
- Step 1** From the menu bar, choose **Configure > Deploy > vPC Peer** tab.
- Step 2** Click the **Add vPC Peer** icon in the toolbar.  
You are directed to the vPC Peer creation wizard. There are five steps to complete the vPC Peer creation.
- Step 3** On the Select Devices screen:

Click to choose the device that you want to be the primary and device secondary device on the vPC peer link. You can also filter the devices using the **Scope** drop-down list.

**Note** The licensed devices with configured LAN credentials are displayed.

**Note** If vPC is already configured on the device that you chose as primary, the secondary device information and the domain ID are populated automatically. You can also modify, as required.

In the **Domain ID** field, enter the vPC domain ID.

To enable LACP on peer link, check the **Enable lacp on peer link** checkbox.

For VXLAN VTEP device, **Loopback Interface** and **Loopback Secondary IP** address can be specified in the Domain Setting table.

Click **Next** to configure peer link.

#### Step 4 On the Configure Peer-Link screen:

For configuring the peer-link, you have two options. You can either select an existing port-channel or create a new port-channel. If Peer link is already configured on device, on selection of peer link port-channel automatically populates secondary peer-link port-channel.

Perform the following steps on both the primary and the secondary devices.

##### 1 Click **Existing Port Channel** or **Create New port Channel** radio button to configure port channel.

A port channel bundles physical links into a channel group to create a single logical link that provides the aggregate bandwidth of up to 8 physical links on the M series module. If a member port within a port channel fails, the traffic previously carried over the failed link switches to the remaining member ports within the port channel.

##### 2 If you choose **Existing Port Channel**:

- Click the search icon next to the **Port Channel Id** field to select the Port channel ID for the device peer link.
- From the list of port channels for the device, check the **Port Channel ID** check box.
- Click **OK**.

The Port channels selected for the device is displayed in the below area. The interfaces and the port channel to which they are connected to are displayed in the **Existing Port Channel** under the **Configure Secondary Device Peer Link** area.

##### 3 If you choose **Create New Port Channel**:

- In the **Port Channel Id** field, enter the port channel number for each device that you want to use as the vPC peer link.

You can use different numbers for the two port channels on the two vPC devices that you are designating as the vPC peer link.

- In the interface table below, choose the interfaces that you want to use for the vPC peer link.

Click **Next** to configure peer link port-channel setting.

#### Step 5 On the Configure Peer-Link Port Channel Settings screen:

Edit the Description, Port Mode and Native VLAN for the primary and the secondary devices. We recommend that you configure the Layer 2 port channels that you are designating as the vPC peer link in trunk mode and use two ports on separate modules on each vPC peer device for redundancy.

If you did not check the **Enable lacp on peer link** in the Select Devices screen, the Protocol field will display NONE.

If you want to create VLANs, the **Allowed VLANs** value must be a valid VLAN ID or range.

Click **Next** to view the summary information.

- Step 6** On the **Summary** screen:  
You can view the CLI configuration for the for the Primary Switch and Secondary Switch.  
You can copy and save the configuration this configuration to your local directory.
- Step 7** Click **Previous** to change any configurations.
- Step 8** Click **Deploy** to configure vPC Peers.  
After the deployment is complete, a status message shows whether the deployment is successful or a failure.  
Click **Know More** to view the status of each command deployed.
- 

## Delete vPC Peer

You can delete the vPC peer by clicking the **Delete vPC Peer** icon in the toolbar.

### Procedure

---

- Step 1** From the menu bar, choose **Configure > Deploy > vPC Peer** tab.
- Step 2** Select the vPC domain which you want to delete, and click the **Delete vPC Peer** icon in the toolbar.  
Click **Yes** when the confirmation window pops out.
- 

## Edit vPC Peer Configuration

You can edit the vPC domain by clicking the **Edit vPC Peer** icon in the toolbar.

### Procedure

---

- Step 1** From the menu bar, choose **Configure > Deploy > vPC Peer** tab.
- Step 2** Select the vPC domain which you want to edit, and click the **Edit vPC Peer** icon in the toolbar.  
You can edit the vPC Peer configuration by following the wizard as [Add vPC Peer Wizard, on page 117](#).
- 

## Configuring vPC

After you finish configuring the vPC Peers, navigate to **Configure > Deploy > vPC** to configure the vPC.

You can view the history of tasks performed, navigate to **Configure > Deploy > vPC > History**. For more information, see [vPC History](#), on page 121.

You can view the list of virtual port-channels (vPC) in the **Virtual Port-Channel(vPC)** table.

**Table 24: Virtual Port-Channel(vPC)**

| Column                                               | Description                                                                                                    |
|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Search box                                           | Enter any string to filter the entries in their respective column.                                             |
| <b>vPC ID</b>                                        | Displays vPC ID's configured device.                                                                           |
| <b>Domain ID</b>                                     | Displays the domain ID of the vPC peer switches.                                                               |
| <b>Primary vPC Peer - Device Name</b>                | Displays the vPC Primary device name.                                                                          |
| <b>Primary vPC Peer - Port Channel</b>               | Displays the vPC port channel for primary vPC device connected to the multi-chassis endpoint or access switch. |
| <b>Primary vPC Peer - Peer Port Channel</b>          | Displays the peer-link port channel for vPC primary device.                                                    |
| <b>Primary vPC Peer - Operational Mode</b>           | Displays the operational mode of the primary vPC end points.                                                   |
| <b>Secondary vPC Peer - Device Name</b>              | Displays the vPC secondary device name.                                                                        |
| <b>Secondary vPC Peer - Port Channel</b>             | Displays the vPC port channel for secondary device connected to the multi-chassis endpoint or access switch.   |
| <b>Secondary vPC Peer - Peer Port Channel</b>        | Displays the peer-link port channel for vPC secondary device.                                                  |
| <b>Secondary vPC Peer - Operational Mode</b>         | Displays the operational mode of the secondary vPC end points.                                                 |
| <b>Multi Chassis vPC EndPoints - Device Name</b>     | Displays the multi-chassis vPC endpoints for each vPC ID under a vPC domain.                                   |
| <b>Multi Chassis vPC EndPoints - Port Channel ID</b> | Displays the port channel on multi chassis vPC devices or access devices connected to the vPC peer switches.   |
| <b>vPC Consistency</b>                               | Displays the vPC Consistency status. Corresponds vPC port channel and vPC.                                     |

This feature supports add, delete and edit option for vPC.

## vPC History

To view the deployed jobs on the created vPC peers, navigate to **Configure > Deploy > vPC > History** tab. You can view the list **vPC Peer History** information in the table.

**Table 25: vPC Peer History**

| Column               | Description                                                                                                                                                                                                                                                                             |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vPC Id               | Specifies the domain ID for the vPC peer.                                                                                                                                                                                                                                               |
| Primary Switch       | Specifies the Primary Switch associated with the vPC.                                                                                                                                                                                                                                   |
| Secondary Switch     | Specifies the Secondary Switch associated with the vPC.                                                                                                                                                                                                                                 |
| Access Switch        | Specifies the Access Switch associated with the vPC.                                                                                                                                                                                                                                    |
| Created By           | Specifies the DCNM username who deployed this task.                                                                                                                                                                                                                                     |
| Started At           | Specifies the time at which the task was performed on the vPC peer.<br>The time is displayed in the format YYYY-MM-DD HH:MM:SS.                                                                                                                                                         |
| Task Performed       | Specifies the task performed on the vPC.                                                                                                                                                                                                                                                |
| Status               | Species the status of the task performed on the vPC.                                                                                                                                                                                                                                    |
| View Command History | Select an activity, click <b>View Command History</b> .<br><br>The <b>Command History</b> page displays the commands executed, status and error message for every command on the <b>Primary Switch</b> , <b>Secondary Switch</b> , and <b>Access Switch</b> , in their respective tabs. |
| Delete vPC Job       | Select a vPC history and click <b>Delete</b> to delete the task history.                                                                                                                                                                                                                |

## Add vPC

You can launch the vPC configuration wizard by clicking the **Add vPC** icon in the toolbar.

### Procedure

**Step 1** From the menu bar, choose **Configure > Deploy > vPC** tab.

**Step 2** Click the **Add vPC** icon in the toolbar.

You are directed to the vPC creation wizard. There are five steps to complete the vPC creation.

**Note** Before configuring vPC we need to configure vPC domain. Once the Domain is configured, we can select the vPC peer, to create vPCs.

- Step 3** In the Select Devices page, click on search button next to the Primary Switch text box to open a list of vPC peers.  
After selection, click OK. Once the domain is selected the vPC domain page gets pre-populated with vPC domain information.
- Note** You cannot select a peer link if a switch associated is not a licensed device with configured LAN credentials.  
Click **Ok**.
- Step 4** In the **vPC ID** field, enter the value for this vPC.  
By default, this field is auto-populated when selecting Devices.  
Select the option to **Configure Access Switch/Fex**, **Configure New Fex** or **Configure Host** and specify the **Access Switch/Fex**.  
A dual-home FEX will be created after you successfully deploy the vPC.
- Step 5** To enable LACP on VPC port-channels, check **Create LACP Based Port Channels For Setting Up vPC** checkbox.
- Note** LACP based port-channel will be created. By default, LACP is not enabled on vPC port channel. We recommend that you create and use LACP for all these port channels. If you do not want to use LACP, deselect the option. Ensure that the LACP is configured with active mode on the interfaces on each port channel on the vPC peer devices. This configuration allows you to more easily detect compatibility between devices, unidirectional links, and multihop connection, and provides dynamic reaction to run-time changes and link failures.
- Step 6** In the Configure links with vPC Primary and vPC Secondary page, configure the port channel for the Primary and Secondary vPC.
- Step 7** Select or create the port-channel to configure the vPC. Click **Existing Port Channel** or **Create New port Channel** radio button to configure port channel.  
A port channel bundles physical links into a channel group to create a single logical link that provides the aggregate bandwidth of up to 8 physical links on the M series module. If a member port within a port channel fails, the traffic previously carried over the failed link switches to the remaining member ports within the port channel.
- If you choose **Existing Port Channel**:
    - 1 Click the search icon next to the **Port Channel Id** field to select the Port channel ID for the device peer link.  
All the discovered port channels is displayed. The non-LACP port channel will be disabled and you cannot select only LACP enabled Port-channels.
    - 2 From the list of port channels for the device, check the **Port Channel ID** check box.
    - 3 Click **OK**.  
The Port channels selected for the device is displayed in the below area. The interfaces and the port channel to which they are connected to are displayed in the **Existing Port Channel** under the **Configure Secondary Device Peer Link** area.
  - If you choose **Create New Port Channel**:
    - 1 In the **Port Channel Id** field, enter the port channel number for each device that you want to use as the vPC peer link.  
This field is auto-populated by default.



You can use different numbers for the two port channels on the two vPC devices that you are designating as the vPC peer link.

- 2 In the interface table below, choose the interfaces that you want to use for the vPC peer link.

Click **Next** to review and modify other vPC port channel settings.

- Step 8** In the Configure vPC Port Channel Settings, review and configure parameters for the port channel for both Primary and Secondary switches.  
Edit the Description, Port Mode, Native VLAN and Protocol for the port channels of the primary and the secondary devices.  
If you did not check the **Create LACP based Port Channels for setting up vPC** in the Select Devices screen, the Protocol field will display NONE.  
If you want to create VLANs, the **Allowed VLANs** value must be a valid VLAN ID or range.  
Click **Next**.
- Step 9** In the **Summary** page, you can view the summary of your configuration for the Primary Switch, Secondary Switch, and Access Switch.  
You can copy and save the configuration this configuration to your local directory.
- Step 10** Click **Previous** to change any configurations.
- Step 11** Click **Deploy** to configure vPC on the devices.  
After the deployment is complete, a status message shows whether the deployment is successful or a failure.  
Click **Know More** to view the status of each command deployed.
- 

## Delete vPC

You can delete the virtual Port-Channel by clicking the **Delete vPC** icon in the toolbar.

### Procedure

---

- Step 1** From the menu bar, choose **Configure > Deploy > vPC** tab.
- Step 2** Select the vPC which you want to delete, and click the **Delete vPC** icon in the toolbar.  
Click **Yes** when the confirmation window pops out.
- 

## Edit vPC Configuration

You can edit the vPC configuration by clicking the **Edit vPC** icon in the toolbar.

### Procedure

- 
- Step 1** From the menu bar, choose **Configure > Deploy > vPC** tab.
- Step 2** Select the vPC which you want to edit, and click the **Edit vPC** icon in the toolbar.  
You can edit the selected vPC configuration by following the [Add vPC, on page 121](#).
- 

## POAP Launchpad



**Note** These features appear on your Cisco DCNM Web Client application only if you have deployed the Cisco DCNM installer in the Unified Fabric mode.

The POAP launchpad contains the following configuration steps:

### Procedure

- 
- Step 1** Create and manage scopes for POAP creation.
- Step 2** Set a server for images and configuration files.
- Step 3** Generate from template or upload existing configuration.
- Step 4** Create, Publish and Deploy Cable Plans.
- 

## Power-On Auto Provisioning (POAP)

Power-On Auto Provisioning (POAP) automates the process of upgrading software images and installing configuration files on Cisco Nexus switches that are being deployed in the network for the first time.

When a Cisco Nexus switch with the POAP feature boots and does not find the startup configuration, the switch enters POAP mode, locates a DHCP server and bootstraps itself with its interface IP address, gateway, and DNS server IP addresses. It also obtains the URL of an SCP server and downloads a configuration script that is run on the switch to download and install the appropriate software image and configuration file.



**Note** When you move the mouse cursor over an error identified in a specific parameter in any window, it will display the exact error message before you move to the next screen.

## DHCP Scopes

DHCP scope is a well-defined term in DHCP arena. It is used to define a policy for giving out IP addresses and other options to host on a specific IP subnet. In DCNM, we use the DHCP scope to distribute IPv4 address, PYTHON bootscript, (or other supported protocol + access credential + server) which stores the bootscript.

From the menu bar, select **Configure > Deploy > POAP**.

The following table details the columns in the display.

**Table 26: DHCP Scopes display fields**

| DHCP Scopes           | Comment                                                                                                                         |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Scope Name            | The DHCP scope name must be unique amongst the switch scopes. This name is not used by ISC DHCP but used to identify the scope. |
| Scope Subnet          | The IPv4 subnet used by the DHCP servers.                                                                                       |
| IP Address Range      | The IP address ranges allocated to the POAP switches. Multiple IP addresses can be used, separated by comma.                    |
| Lease Time            | Maximum lease time for the DHCP lease.                                                                                          |
| Default Gateway       | The default gateway for the DHCP scope. You must enter a valid IP as the default gateway.                                       |
| Domain Name Servers   | The domain name server for the DHCP scope.                                                                                      |
| Bootscrip Name        | The Python Bootup script.                                                                                                       |
| TFTP/Bootscrip Server | The server that holds the bootscrip.                                                                                            |

## Adding a DHCP Scope

### Procedure

- Step 1** From the menu bar, select **Configure > Deploy > POAP > DHCP Scopes**.
- Step 2** Click Add scope icon.
- Step 3** In the Add DHCP Scope window, specify values in the fields according to the information in [Table 26: DHCP Scopes display fields, on page 125](#).
- Step 4** Click **OK** to add a DHCP scope.

## Editing an existing DHCP Scope



### Note

Once the DCNM is accessed for the first time, you must edit the default scope named **enhanced\_fab\_mgmt** and add free IP address ranges.

### Procedure

- 
- Step 1** From the menu bar, select **Configure > Deploy > POAP > DHCP Scopes**.
  - Step 2** Use the checkbox to select the DHCP scope.
  - Step 3** Click Edit scope icon.
  - Step 4** In the Edit DHCP Scope window, edit the DHCP scopes.
  - Step 5** Click **Apply** to save the changes.
- 

## Deleting a DHCP Scope

### Procedure

- 
- Step 1** From the menu bar, select **Configure > Deploy > POAP > DHCP Scopes**.
  - Step 2** Use the checkbox to select the DHCP scope.
  - Step 3** Click Delete scope icon.
  - Step 4** In the delete notification, click **Yes** to delete the DHCP scope.
- Note** You may click the Refresh icon to refresh the DHCP Scopes list.
- 

## Image and Configuration Servers

The Image and Configuration Servers page allows you to specify the servers and credentials used to access the device images and the uploaded or Cisco DCNM generated or published device configuration. The server that is serving the images could be different from the one serving the configurations. If the same server is serving both images and configurations, you need to specify the server IP address and credentials twice for each server because the root directory holding the images or configuration files could be different. By default, the Cisco DCNM server will be the default image and configuration server. There will be two Cisco DCNM server addresses, one for configuration, one for image.

From the menu bar, choose **Configure > Deploy > POAP**. The Power-On Auto Provisioning (POAP) page appears. Click **Images and Configuration**.

The following table details the columns in the display.

**Table 27: DHCP Scopes display fields**

| Image and Configuration Servers | Description                                  |
|---------------------------------|----------------------------------------------|
| Name                            | Name of the image and configuration server.  |
| URL                             | URL shows where images and files are stored. |

| Image and Configuration Servers | Description                       |
|---------------------------------|-----------------------------------|
| Username                        | Indicates the username.           |
| Last Modified                   | Indicates the last modified date. |

You can add your own image and configuration servers if they are different from the default.

### Add Image or Configuration Server URL

Perform the following task to add an image or a configuration server URL:

#### Procedure

- Step 1** On the Image and Configuration Servers page, click the Add icon.
- Step 2** In the Add Image or Configuration Servers URL window, specify a name for the image.
- Step 3** Click the **scp** radio button to select the SCP protocol for POAP and Image Management.
- Step 4** Enter Hostname/Ipaddress and Path.
- Step 5** Specify the Username and Password.
- Step 6** Click **OK** to save.

### Editing an Image or Configuration Server URL

Perform the following task to edit an image or a configuration server URL to the repository.

#### Procedure

- Step 1** On the Image and Configuration Servers page, select an existing Image and Configuration Server from the list, and click the Edit icon.
- Step 2** In the **Edit Image or Configuration Servers URL** window, edit the required fields.  
The Default\_SCP\_Repository cannot be edited.
- Step 3** Click **OK** to save or click **Cancel** to discard the changes.

### Deleting an Image or Configuration Server URL

Perform the following task to delete an image or a configuration server URL to the repository.

## Procedure

- 
- Step 1** On the Image and Configuration Servers page, select an existing Image and Configuration Server from the list, and click the Delete icon.
- Step 2** In the delete notification, click **Yes** to delete the image and configuration server.
- Note** The default SCP Repository cannot be deleted.
- 

## POAP Templates

Templates can be created or imported into the template builder of DCNM. There are some predefined Fabric specific POAP templates bundled with DCNM. The template builder can be invoked from the GUI, **Configure > Templates > Deploy**. The templates dedicated to POAP will be used to generate many different POAP device configurations

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

- Use the Show Filter icon to filter the templates.
- Use the Print icon to print the list of templates and their details.
- Use the Export icon to export the list of templates to a Microsoft Excel spreadsheet.

This section contains the following:

### Add POAP template

## Procedure

- 
- Step 1** From the menu bar, select **Configure > Deploy > POAP > POAP Definitions**.
- Step 2** In the Configuration Steps, click the template hyperlink in the POAP Definitions section.
- Step 3** Click **Add template** icon.
- Step 4** Specify the Template Name, Template Description and Tags.
- Step 5** Use the checkbox to specify the Supported Platforms.
- Step 6** Select the template type from the drop-down list.  
By default, CLI template type is selected.
- Step 7** Select the Published checkbox if you want the template to have 'Read Only' access.
- Step 8** In the Template Content pane, you can specify the content of the template.  
For help on creating the template content, click the Help icon next to the Template Content header. For information about POAP template annotations see the [POAP Template Annotation](#), on page 130 section.

- Step 9** Click **Validate Template Syntax** to validate syntax errors.
  - Step 10** Click **Save** to save the template.
  - Step 11** Click **Save and Exit** to save the template and exit the window.
  - Step 12** Click **Cancel** to discard the template.
- 

## Editing a Template

### Procedure

---

- Step 1** From the menu bar, select **Configure > Deploy > POAP > POAP Definitions**.
  - Step 2** In the Configuration Steps, click the template hyperlink in the POAP Definitions section.
  - Step 3** Select a template from the list and click Modify/View template icon.
  - Step 4** Edit the template content and click **Save** to save the template or **Save and Exit** to save and exit the screen.
- 

## Cloning a Template

### Procedure

---

- Step 1** From the menu bar, select **Configure > Deploy > POAP > POAP Definitions**.
  - Step 2** In the Configuration Steps, click the template hyperlink in the POAP Definitions section.
  - Step 3** Select a template from the list and click **Save Template As** icon.
  - Step 4** Edit the template and click **Save** to save the template or **Save and Exit** to save and exit the screen.
- 

## Importing a Template

### Procedure

---

- Step 1** From the menu bar, select **Configure > Deploy > POAP > POAP Definitions**.
  - Step 2** In the Configuration Steps, click the template hyperlink in the POAP Definitions section.
  - Step 3** Select a template from the list and click Import template icon.
  - Step 4** Select the template file and upload.
-

## Exporting a Template

### Procedure

- 
- Step 1** From the menu bar, select **Configure > Deploy > POAP > POAP Definitions**.
- Step 2** In the Configuration Steps, click the template hyperlink in the POAP Definitions section.
- Step 3** Select a template from the list and click Export template icon.
- Step 4** Select a location for the file download.
- 

## Deleting a Template



---

**Note** Only user-defined templates can be deleted.

---

### Procedure

- 
- Step 1** From the menu bar, select **Configure > Deploy > POAP > POAP Definitions**.
- Step 2** In the Configuration Steps, click the template hyperlink in the POAP Definitions section.
- Step 3** Select a template from the list and click Remove template icon.
- Step 4** Click **Yes** to confirm.
- 

## POAP Template Annotation

Annotation is used to add semantic, validation logic and description to the template variable.

The Annotation for a given template variable is required to precede the given template variable. Only one annotation statement is required for each template variable. When a template variable has an associated annotation statement, the template variable has to be declared on a single line, Multiple variables cannot be declared under the same annotation statement.

Format of an annotation statement is as follows:

@(<key1>=<value1>,<key2>=<value2>, ..., <keyN>=<valueN>)



---

**Note** Each annotation statement is composed of one or more key-values pair.

---

- The value can be true, false, or a string.
- If the value is a string, it should be double quoted.



The following is a sample template variable, “hostname”, with annotation statement with the keys “DisplayName”, and “Description”:

```
@(DisplayName="Host Name", Description = "Description of the host")
```

String hostname;

The table displays the supported keys in the annotation statement:

**Table 28: Annotation Keys**

| Key Name            | Default Value | Description                                                                                                                                                                                                                                |
|---------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DisplayName         | Empty String  | The value is displayed as a variable label in the template form GUI, on POAP definition screen.                                                                                                                                            |
| Description         | Empty String  | Displays the description next or below the template variable field in the template form GUI.                                                                                                                                               |
| IsManagement        | false         | The associated variable is of IP Address type. This will be used as the management IP address. DCNM used this IP address to manage the devices.                                                                                            |
| IsMultiplicity      | false         | If true, this single value can take multiple values. For example; when it is used with IsManagement annotation, it allows you to type in multiple IP addresses and assign each IP address to a device.                                     |
| IsSwitchName        | false         | The associated variable value is used as the device host name.                                                                                                                                                                             |
| IsMandatory         | true          | It marks the field as mandatory if the value is set as 'true'.                                                                                                                                                                             |
| UseDNSReverseLookup | false         | This annotation compliments the IsSwitchName annotation. Once they are associated with a variable. The variable is populated with the reverse DNS name, if available during the creation time of the corresponding POAP definition record. |

| Key Name                 | Default Value | Description                                                                                                                                             |
|--------------------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| IsFabricPort             | false         | The associated variable value contains a list of the ports used as fabric ports. The variable value will be used by the cable plan generation from POAP |
| IsHostPort               | false         | Trunk ports connected to host/servers.                                                                                                                  |
| IsVPCDomainID            | false         | Used as the vPC Domain ID.                                                                                                                              |
| IsVPCPeerLinkSrc         | false         | Used as the VPC IPv4 source address.                                                                                                                    |
| IsVPCPeerLinkDst         | false         | Used as the VPC IPv4 peer address.                                                                                                                      |
| IsVPCPeerLinkPortChannel | false         | Used for VPC port channel.                                                                                                                              |
| IsVPCLinkPort            | false         | Used for VPC interface.                                                                                                                                 |
| IsVPC                    | false         | Used as a VPC record.                                                                                                                                   |
| IsVPCID                  | false         | Individual VPC ID.                                                                                                                                      |
| IsVPCPortChannel         | false         | Individual VPC port channel.                                                                                                                            |
| IsVPCPort                | false         | VPC Interface.                                                                                                                                          |

## POAP Definitions

The POAP switch definition has two major functions:

- Monitoring switch POAP process
- Managing POAP switch configuration

You must copy the Cisco DCNM license files to the `/var/lib/dcnm/license` directory to install as part of the POAP process.

You must also copy the device licenses to the `/var/lib/dcnm/licenses` folder.



### Note

The device licenses refers to the devices monitored by the Cisco DCNM.

The following fields and icons are listed at the menu bar of the window to customize the view of the information in the window:

| Fields and Icons   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Serial Number      | Specifies the serial number for the switch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Switch ID          | Specifies the ID defined for the switch                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Management IP      | Specifies the Management IP for the switch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Status             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Switch Status      | Indicates if the switch is published or not.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Publish Status     | Indicates if this POAP template has been published successfully to the TFTP site.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Bootscrip Status   | Indicates the Bootscrip execution state when the device executed POAP. For details, view the “Boot Log” file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Diff State         | <p>Specifies if the configuration defined in POAP is different from the running configuration on the device. If a difference is detected, the user has an option to make changes to the device configuration, thereby ensuring that the configuration on the device in sync with the POAP configuration. The different states are:</p> <ul style="list-style-type: none"> <li>• NA—Specifies that no POAP definition is configured on DCNM for the particular device; therefore, no difference computation can be made.</li> <li>• Diff Detected—Specifies that few configuration differences are detected between POAP definition in DCNM and the running configuration on the switch. You can review the difference statements and choose the commands to deploy to the device, and synchronize the running configuration with the POAP definition.</li> <li>• No Diff Detected—Specifies that there was no configuration diff perceived between POAP definition and the running configuration on the switch.</li> <li>• Error—Specifies that an error has occurred during diff computation. Refer to the logs to troubleshoot the issue.</li> </ul> |
| Model              | Specifies the model of the switch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Template File Name | <p>Specifies the template used for creating the POAP definition.</p> <p>Fabric and IPFabric POAP templates are available.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Fields and Icons                     | Description                                                                                                                           |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Bootscrip<br>Last<br>Updated<br>Time | Specifies the last updated time for bootscrip.                                                                                        |
| Last<br>Published                    | Specifies the last published time for the POAP definition.                                                                            |
| POAP<br>Creation<br>Time             | Specifies the time when the POAP definition was created.                                                                              |
| System<br>Image                      | Specifies the System Image used while creating the POAP definition.                                                                   |
| Kickstart<br>Image                   | Specifies the kickstart image used the POAP definition.                                                                               |
| Icons                                |                                                                                                                                       |
| Add                                  | Allows you to add a POAP definition. For more information, see <a href="#">Creating a POAP definition</a> , on page 135.              |
| Edit                                 | Allows you to edit a POAP definition. For more information, see <a href="#">Editing a POAP Definition</a> , on page 137.              |
| Delete                               | Allows you to delete a POAP definition. For more information, see <a href="#">Deleting POAP Definitions</a> , on page 137.            |
| Write<br>Erase and<br>Reload         | Allows you to reboot and reload a POAP definition. For more information, see <a href="#">#unique_244</a> .                            |
| Change<br>Image                      | Allows you to change the image for the defined POAP definition. For more information, see <a href="#">Change Image</a> , on page 138. |
| Boot Log                             | Display the list and view log files from the device bootflash.                                                                        |
| Update<br>Serial<br>Number           | Allows the user to modify the serial number of the POAP definition.                                                                   |
| Refresh<br>Switch                    | Refreshes the list of switches.                                                                                                       |
| Refresh<br>Diff State                | Refreshes the Diff state.                                                                                                             |

| Fields and Icons | Description                                                                     |
|------------------|---------------------------------------------------------------------------------|
| Show Filter      | Filters list of switches based on the defined value for each column.            |
| Print            | Prints the list of devices and their details.                                   |
| Export           | Exports the list of devices and their details to a Microsoft Excel spreadsheet. |
| Select Columns   | Displays the columns to be displayed. You can choose to show/hide a column.     |

**Note**

Each annotation statement is composed of one or more key-values pair. The value can be true, false or a string. If the value is a string, it should be mentioned in double-quotes.

This section contains the following:

## Creating a POAP definition

### Procedure

- Step 1** From the menu bar, select **Configure > Deploy > POAP > POAP Definitions**.
  - Step 2** From the **Scope** drop-down list, select the scope for POAP definition.
  - Step 3** Click **Add** to add a new POAP definition.
  - Step 4** Click on **Generate Definition** radio button to generate POAP definition from a template, and click **Next** to specify the switch details.
  - Step 5** Enter the serial number of switches separated by comma. Alternatively, you can click **Import from CSV File** to import the list of switches.
- Note** The serial number cannot be changed after you create the POAP definition. Verify that the serial numbers do not contain spaces, the POAP will not work otherwise.

- Step 6** Use the drop-down list to select the Switch Type.
  - Step 7** Use the drop-down list to select the Image Server.
  - Step 8** Use the drop-down list to select the System Image and Kickstart image.
  - Step 9** Specify the Switch User Name and Switch Password.
  - Step 10** Click **Next** to Select the Switch Config Template.
  - Step 11** Use the drop-down to select the Template and click View to specify the Template Parameters.
  - Step 12** Enter Template Parameters.
  - Step 13** From the **Settings File** drop-down list to select the file. If the settings file is unavailable, click **Save Parameter** as New Settings File button to specify a name for the settings file.
  - Step 14** Select the variables and click **Manage**.
  - Step 15** Click Add to see the variables to be saved. Specify a name for the settings file and click **Save**.
  - Step 16** Click **Manage** to modify the settings file parameters.
  - Step 17** Click **Preview CLI** to view the generated configuration.
  - Step 18** Click **Finish** to publish the POAP definition.
  - Step 19** Click **Next** to generate the configuration.
- 

## Uploading a POAP Definition

### Procedure

---

- Step 1** From the menu bar, select **Configure > Deploy > POAP > POAP Definitions**.
  - Step 2** Click **Upload Startup Config** radio button to upload startup configuration to the POAP repository Server, and click **Next** to enter the switch details.
  - Step 3** Enter the serial number of switches separated by comma.
  - Step 4** Use the drop-down to select the Switch Type.
  - Step 5** Use the drop-down to select the Image Server.
  - Step 6** Use the drop-down to select the System Image and Kickstart Image.
  - Step 7** Specify the Switch User Name and Password.
  - Step 8** Click **Browse** to select the upload configuration file.
  - Step 9** Click **Finish** to publish the POAP definition.
-

## Editing a POAP Definition

### Procedure

---

- Step 1** From the menu bar, select **Configure > Deploy > POAP > POAP Definitions**.
- Step 2** Select the POAP switch definitions from the list and click the Edit icon.
- Step 3** Follow the steps listed in [Creating a POAP definition, on page 135](#) and [Uploading a POAP Definition, on page 136](#) sections.
- Note** You can select multiple POAP definitions with similar parameters to edit POAP definition.
- 

## Deleting POAP Definitions

### Procedure

---

- Step 1** From the menu bar, select **Configure > Deploy > POAP > POAP Definitions**.
- Step 2** Select the POAP switch definitions from the list and click the Delete icon.
- Step 3** Click **Yes** to delete the switch definitions.  
A prompt appears to delete the device from the data source. Check or uncheck the checkbox based if you want to delete the switches associated with the POAP Definition.
- Step 4** Click **OK** to confirm to delete the device. Based on the check box, the device will be deleted from the data source also.
- 

## Publishing POAP definitions

### Procedure

---

- Step 1** From the menu bar, select **Configure > Deploy > POAP > POAP Definitions**.
- Step 2** Select the POAP switch definitions from the list and click the Publish icon.
- Step 3** Click **Yes** to publish the switch definitions.
-

## Write, Erase and Reload the POAP Switch Definition

### Procedure

---

- Step 1** From the menu bar, select **Configure > Deploy > POAP > POAP Definitions**.
- Step 2** Select the POAP switch definitions from the list and click the Edit icon.
- Step 3** Click the **Write Erase and Reload** button.  
The **Write Erase and Reload** button works only when the selected switch(es) are listed in the Inventory > Discovery > LAN Switches screen. Also, valid credentials must be specified in the Configure > Credentials Management > LAN Credentials screen.
- Step 4** Click **Continue** to reboot and reload the switch definitions.
- 

## Change Image

### Procedure

---

- Step 1** From the menu bar, select **Configure > Deploy > POAP > POAP Definitions**.
- Step 2** Select the POAP switch definitions from the list and click the Edit icon.
- Step 3** Select the switch for which you need to change the image. Click **Change Image**.  
**Note** You can select multiple POAP definitions with similar parameters to change the image for booting the device.  
The Multi Device Image Change screen appears.
- Step 4** From the **Image Server** drop down list, select the server where the new image is stored.
- Step 5** From the **System Image** drop down list, select the new system image.
- Step 6** From the **Kickstart Image** drop down list, select the new image which will replace the old image.
- Step 7** Click **OK** to apply and change the image.
- 

## Updating the Serial Number of a Switch for an existing POAP Definition

You will want to update the serial number of a switch when performing an RMA. To do this, perform the following tasks:



## Procedure

- 
- Step 1** Ensure that the old switch is in place with POAP definition and discovered.
  - Step 2** Manually update serial number in Cisco DCNM on the POAP screen. Note: this button may be hidden underneath a >> button. Now two devices in Cisco DCNM will have the same IP address.
  - Step 3** Physically remove the old switch from the network.
  - Step 4** Place the new switch in the rack and connect network cables and power. Bring up the new switch. The new switch reboots several times so that it comes up with necessary configurations.
  - Step 5** Manually rediscover the switches in Cisco DCNM. Now there will be one device in Cisco DCNM with the same IP.
- 

## Cable Plan



### Note

If you are generating POAP definitions from the uploaded configuration, then generation of cable plan using the option of “Generate Cable Plan from POAP definition” will not work as the POAP definitions generated from the uploaded configuration will not have the required meta-data to generate the cable plans. You must select either “Capture from Existing Deployment” or “Import Cable plan file” to create a cable plan.

The Cable plan configuration screen has the following options:

## Create a Cable Plan

### Procedure

- 
- Step 1** From the menu bar, select **Configure > Deploy > POAP > Cable Plan**.
  - Step 2** Click **Create Cable Plan**.  
In the Create Cable Plan pop-up, use the radio button to select the options.
  - Step 3** If you select:
    - a) **Capture from existing deployment:** You can ascertain the Inter-Switch Links between existing switches managed by DCNM and “lock down” the cable plan based on the existing wiring.
    - b) **Import Cable Plan File:** You decide how to wire the switches (or how they are already wired) and select an XML file for import into DCNM.
-

## Viewing an Existing Cable Plan Deployment

### Procedure

---

- Step 1** From the menu bar, select **Configure > Deploy > POAP > Cable Plan**.
  - Step 2** Click **View**.
  - Step 3** In the Cable Plan – Existing\_Deployment window, you can view the existing cable plan deployments.
  - Step 4** You can use the Table View and XML View icons to change the view of the cable plan deployments table.
- 

## Deleting a Cable Plan

### Procedure

---

- Step 1** From the menu bar, select **Configure > Deploy > POAP > Cable Plan**.
  - Step 2** Click **Delete** from DCNM.
  - Step 3** Click **Yes** to confirm deletion.
- 

## Deploying a Cable Plan

### Procedure

---

- Step 1** From the menu bar, select **Configure > Deploy > POAP > Cable Plan**.
  - Step 2** In the Switches table, use the checkbox to select cable plan(s) and click **Deploy a Cable Plan**.
  - Step 3** Click **Yes** to confirm deployment.
- 

## Revoking a Cable Plan

### Procedure

---

- Step 1** From the menu bar, select **Configure > Deploy > POAP > Cable Plan**.
  - Step 2** In the Switches table, use the checkbox to select cable plan(s) and click **Revoke a Cable Plan**.
  - Step 3** Click **Yes** to confirm.
-

## Viewing a Deployed Cable Plan from Device

### Procedure

- 
- Step 1** From the menu bar, select **Configure > Deploy > POAP > Cable Plan**.
- Step 2** In the Switches table, click **In Sync** or **Out of Sync** hyperlink in the cable plan status column.
- Step 3** You can use the Table View and XML View icons to change the view of the cable plan table.
- 

# Templates

The Templates menu includes the following submenus:

## Deploying Templates

Cisco DCNM allows you to add, edit or delete user-defined templates configured across different Cisco Nexus and Cisco MDS platforms. The following parameters are displayed for each template configured on the Web Client of the Cisco DCNM **Configure > Templates > Deploy**. This uses the Java runtime provided Java script environment to perform arithmetic operations, string manipulations in the template syntax.

The following table describes the fields that appear on this page.

**Table 29: Templates Operations**

| Field                      | Description                                                                                          |
|----------------------------|------------------------------------------------------------------------------------------------------|
| Add Template               | Allows you to add a new template.                                                                    |
| Launch job creation wizard | Allows you to create jobs.                                                                           |
| Modify/View Template       | Allows you to view the template definition and modify as required.                                   |
| Save Template As           | Allows you to save the selected template in a different name. You can edit the template as required. |
| Delete Template            | Allows you to Delete a template                                                                      |
| Import Template            | Allows you to import a template from your local directory, one at a time.                            |
| Export template            | Allows you tot export the template configuration to a local directory location.                      |

| Field                    | Description                                                                                                                                                                                               |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Import Template Zip File | Allows you to import .zip file, that contains more than one template bundled in a .zip format<br><br>All the templates in the zip file will be extracted and listed in the table as individual templates. |

**Table 30: Templates Table Field and Description**

| Field             | Description                                                                                        |
|-------------------|----------------------------------------------------------------------------------------------------|
| Name              | Displays the name of the configured template.                                                      |
| Description       | Displays the description provided while configuring templates.                                     |
| Platforms         | Displays the supported Cisco Nexus platforms compatible with the template.                         |
| Tags              | Displays the tag assigned for the template and aids to filter templates based on the tags.         |
| Template Type     | Displays the type of the template.                                                                 |
| Template Sub Type | Specifies the sub type associated with the template.                                               |
| Published         | Specifies if the template is published or not.                                                     |
| Modified Time     | Displays the date and time when the template was last modified, in the format YYYY-MM-DD HH:MM:SS. |

Additionally, from the menu bar, select **Configure > Delivery > Templates** and you can also:

- Click the **Launch Job Creation** icon to configure and schedule jobs for individual templates. For more information, see [Configuring Template Job](#), on page 157.
- Click the Show Filter icon to filter the templates based on the headers.
- Click the Print icon to print the list of templates.
- Click the Export to Excel icon to export the list of template to a Microsoft Excel spreadsheet.

This section contains the following:

## Template Structure

The configuration template content mainly consists of four parts. You can click on the Help icon next to the Template Content window for information about editing the content of the template. Click on the Help icon next to the Template Content window for information about editing the content of the template.

This section contains the following:

## Template Format

This section describes the basic information of the template. The possible fields are as detailed in the table below.

| Property Name      | Description                                                                                            | Valid Values                                                                                                                 | Optional? |
|--------------------|--------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|-----------|
| name               | The name of the template                                                                               | Text                                                                                                                         | No        |
| description        | Brief description about the template                                                                   | Text                                                                                                                         | Yes       |
| userDefined        | Indicates whether the user created the template. Value is 'true' if user created.                      | "true" or "false"                                                                                                            | Yes       |
| supportedPlatforms | List of device platforms supports this configuration template. Specify 'All' to support all platforms. | N1K, N3K, N3500, N4K, N5K, N5500, N5600, N6K, N7K, N9K, MDS, VDC list separated by comma.                                    | No        |
| configType         | Specifies the type of Template used.                                                                   | <ul style="list-style-type: none"> <li>• CLI</li> <li>• POAP</li> <li>• POLICY</li> <li>• SHOW</li> <li>• PROFILE</li> </ul> | Yes       |

| Property Name     | Description                                          | Valid Values | Optional? |
|-------------------|------------------------------------------------------|--------------|-----------|
| Template Sub Type | Specifies the sub type associated with the template. |              |           |

| Property Name | Description | Valid Values                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Optional? |
|---------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
|               |             | <ul style="list-style-type: none"> <li>• CLI               <ul style="list-style-type: none"> <li>◦ N/A</li> </ul> </li> <li>• POAP               <ul style="list-style-type: none"> <li>◦ N/A</li> <li>◦ VXLAN</li> <li>◦ FABRICPATH</li> <li>◦ VLAN</li> <li>◦ PMN</li> </ul> </li> <li>• POLICY               <ul style="list-style-type: none"> <li>◦ VLAN</li> <li>◦ INTERFACE_VLAN</li> <li>◦ INTERFACE_ETHERNET</li> <li>◦ INTERFACE_BD</li> <li>◦ <del>INTERFACE_PORT_CHANNEL</del></li> <li>◦ INTERFACE_FC</li> <li>◦ INTERFACE_MGMT</li> <li>◦ INTERFACE_LOOPBACK</li> <li>◦ INTERFACE_NVE</li> <li>◦ INTERFACE_VFC</li> <li>◦ <del>INTERFACE_SNMP_CHANNEL</del></li> <li>◦ DEVICE</li> <li>◦ FEX</li> <li>◦ INTERFACE</li> </ul> </li> <li>• SHOW               <ul style="list-style-type: none"> <li>◦ VLAN</li> <li>◦ INTERFACE_VLAN</li> <li>◦ INTERFACE_ETHERNET</li> <li>◦ INTERFACE_BD</li> <li>◦ <del>INTERFACE_PORT_CHANNEL</del></li> <li>◦ INTERFACE_FC</li> </ul> </li> </ul> |           |

| Property Name | Description                                                      | Valid Values                                                                                                                                                                                                                                                                               | Optional? |
|---------------|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
|               |                                                                  | <ul style="list-style-type: none"> <li>◦ INTERFACE_MGMT</li> <li>◦ INTERFACE_LOOPBACK</li> <li>◦ INTERFACE_NVE</li> <li>◦ INTERFACE_VFC</li> <li>◦ <del>INTERFACE_NPORT_CHANNEL</del></li> <li>◦ DEVICE</li> <li>◦ FEX</li> <li>◦ INTERFACE</li> <li>• PROFILE</li> <li>◦ VXLAN</li> </ul> |           |
| published     | Used to Mark the template as read only and avoids changes to it. | “true” or “false”                                                                                                                                                                                                                                                                          | Yes       |
| timestamp     | Shows the template modified time                                 | Modified date and time in the format YYYY-MM-DD HH:MM:SS                                                                                                                                                                                                                                   | Yes       |

### Example: Template Properties

```
##template properties
name =FCOE template;
description = This file specifies the template configuration for FCOE;
userDefined= false;
supportedPlatforms = N7K, N6K, N5K, N5500, MDS;
templateType = CLI;
templateSubType=NA;
published = false;
timestamp = 2013-05-16 07:11:37;
##
```

### Template Variables

This section contains declared variables, the data type, default values, and valid values conditions for the parameters that are used in the template. These declared variables are used for value substitution in the template content section during the dynamic command generation process. Also these variables are used in decision making and in iteration blocks in the template content section. Variables have predefined data types. You can also add a description about the variable. The following table describes the syntax and usage for the available datatypes.



| Variable Type          | Valid Value                                                                                                | Iterative? |
|------------------------|------------------------------------------------------------------------------------------------------------|------------|
| string                 | Free text<br><br>Example: Description for the variable                                                     | No         |
| boolean                | true false                                                                                                 | No         |
| enum                   | Example: running-config, startup-config                                                                    | No         |
| float                  | Floating number format                                                                                     | No         |
| Integer                | Any number                                                                                                 | No         |
| ipAddress              | IPv4 OR IPv6 address                                                                                       | No         |
| ipV4Address            | IPv4 address                                                                                               | No         |
| ipV6Address            | IPv6 address                                                                                               | No         |
| ipV4AddressWithSubnet  | Example: 192.168.1.1/24                                                                                    | No         |
| ipV4AddressWithSubnet  | Example: 1:2:3:4:5:6:7:8/22                                                                                | No         |
| ipV6AddressWithPrefix  | Example: 1:2:3:4:5:6:7:8<br>22                                                                             | No         |
| ipAddressWithoutPrefix | Example: 192.168.1.1<br>or<br>Example: 1:2:3:4:5:6:7:8                                                     | No         |
| macAddress             | 14 or 17 character length MAC address format                                                               | No         |
| interface              | Format: <if type><slot>[/<sub slot>]/<port><br><br>Example: eth1/1, fa10/1/2 etc.                          | No         |
| integerRange           | Contiguous numbers separated by “-”<br><br>Discrete numbers separated by “,”<br><br>Example: 1-10,15,18,20 | Yes        |

| Variable Type                             | Valid Value                                                         | Iterative? |
|-------------------------------------------|---------------------------------------------------------------------|------------|
| floatRange                                | Example: 10.1,50.01                                                 | Yes        |
| ipV4AddressRange                          | Example: 172.22.31.97 - 172.22.31.99, 172.22.31.105 - 172.22.31.109 | Yes        |
| interfaceRange                            | Example: eth10/1/20-25, eth11/1-5                                   | Yes        |
| string[]                                  | Example: {a,b,c,str1,str2}                                          | Yes        |
| ipAddress[]                               | Example: {192.168.1.1, 192.168.1.2, 10.1.1.1}                       | Yes        |
| wwn<br>(Available only in the Web Client) | Example:<br>20:01:00:08:02:11:05:03                                 | No         |

### Example: Template Variables

```
##template variables
integer VSAN_ID;
string SLOT_NUMBER;
integerRange PORT_RANGE;
integer VFC_PREFIX;
##
```

### Variable Meta Property

Each variable defined in the template variable section has a set of meta properties. The meta properties are mainly the validation rules defined for the variable.

The following table describes the various meta properties applicable for the available variable types.

| Variable Type | Description                          | Variable Meta Property |              |                |     |     |          |          |          |          |            |            |              |
|---------------|--------------------------------------|------------------------|--------------|----------------|-----|-----|----------|----------|----------|----------|------------|------------|--------------|
|               |                                      | default Value          | valid Values | decimal Length | min | max | min Slot | max Slot | min Port | max Port | min Length | max Length | regular Expr |
| string        | literal string                       | Yes                    |              |                |     |     |          |          |          |          | Yes        | Yes        | Yes          |
| boolean       | A boolean value.<br>Example:<br>true | Yes                    |              |                |     |     |          |          |          |          |            |            |              |
| enum          |                                      |                        | Yes          |                |     |     |          |          |          |          |            |            |              |

| Variable Type | Description                                      | Variable Meta Property |              |                |     |     |          |          |          |          |            |            |              |
|---------------|--------------------------------------------------|------------------------|--------------|----------------|-----|-----|----------|----------|----------|----------|------------|------------|--------------|
|               |                                                  | default Value          | valid Values | decimal Length | min | max | min Slot | max Slot | min Port | max Port | min Length | max Length | regular Expr |
| float         | signed real number<br>Example:<br>75.56,<br>-8.5 | Yes                    | Yes          | Yes            | Yes | Yes |          |          |          |          |            |            |              |
| integer       | signed number<br>Example:<br>50,<br>-75          | Yes                    | Yes          |                | Yes | Yes |          |          |          |          |            |            |              |
| ipAddrs       | IP address in IPv4 or IPv6 format                | Yes                    |              |                |     |     |          |          |          |          |            |            |              |
| ipV4Addrs     | IPv4 address                                     | Yes                    |              |                |     |     |          |          |          |          |            |            |              |
| ipV6Addrs     | IPv6 address                                     | Yes                    |              |                |     |     |          |          |          |          |            |            |              |
| ipV4Subnet    | IPv4 Address with Subnet                         | Yes                    |              |                |     |     |          |          |          |          |            |            |              |
| ipV6Prefix    | IPv6 Address with Prefix                         | Yes                    |              |                |     |     |          |          |          |          |            |            |              |
| ipV4V6Addrs   | IPv4 or IPv6 Address (does not require prefix)   |                        |              |                |     |     |          |          |          |          |            |            |              |

| Variable Type | Description                                                                | Variable Meta Property |              |                |     |     |          |          |          |          |            |            |              |
|---------------|----------------------------------------------------------------------------|------------------------|--------------|----------------|-----|-----|----------|----------|----------|----------|------------|------------|--------------|
|               |                                                                            | default Value          | valid Values | decimal Length | min | max | min Slot | max Slot | min Port | max Port | min Length | max Length | regular Expr |
| macAddrs      | MAC address                                                                |                        |              |                |     |     |          |          |          |          |            |            |              |
| interface     | specifies interface<br>Example:<br>Ethernet 5/10                           | Yes                    | Yes          |                |     |     | Yes      | Yes      | Yes      | Yes      |            |            |              |
| intRange      | Range of signed numbers<br>Example:<br>50-65                               | Yes                    | Yes          |                | Yes | Yes |          |          |          |          |            |            |              |
| floatRange    | range of signed real numbers<br>Example:<br>50.5 - 54.75                   | Yes                    | Yes          | Yes            | Yes | Yes |          |          |          |          |            |            |              |
| ipAddrs       |                                                                            | Yes                    |              |                |     |     |          |          |          |          |            |            |              |
| intRange      |                                                                            | Yes                    | Yes          |                |     |     | Yes      | Yes      | Yes      | Yes      |            |            |              |
| string[]      | string literals separated by a comma (,)<br>Example:<br>{string1, string2} | Yes                    |              |                |     |     |          |          |          |          |            |            |              |
| ipAddrs[]     | List of IP addresses separated by a comma (,)                              | Yes                    |              |                |     |     |          |          |          |          |            |            |              |

| Variable Type | Description                                                 | Variable Meta Property |              |                |     |     |          |          |          |          |            |            |              |
|---------------|-------------------------------------------------------------|------------------------|--------------|----------------|-----|-----|----------|----------|----------|----------|------------|------------|--------------|
|               |                                                             | default Value          | valid Values | decimal Length | min | max | min Slot | max Slot | min Port | max Port | min Length | max Length | regular Expr |
| wwn           | WWN address                                                 |                        |              |                |     |     |          |          |          |          |            |            |              |
| struct        | set of <del>params</del><br>bundled under a single variable |                        |              |                |     |     |          |          |          |          |            |            |              |

### Example: Meta Property usage

```
##template variables

integer VLAN_ID {
min = 100;
max= 200;
};

string USER_NAME {
defaultValue = admin123;
minLength = 5;
};

##
```

### Variable Annotation

You can configure the variable properties marking the variables using annotations.



#### Note

Variable Annotations are available for POAP only. However, the annotations do not impact on the template type 'CLI'.

The following annotations can be used in the template variable section.

| Annotation Key | Valid Values                                                                                   |
|----------------|------------------------------------------------------------------------------------------------|
| DisplayName    | Text<br><b>Note</b> You must enclose the text with quotes, if there is space.                  |
| Description    | Text                                                                                           |
| IsManagementIP | "true" or "false"<br><b>Note</b> This annotation must be marked only for variable "ipAddress". |

| Annotation Key | Valid Values      |
|----------------|-------------------|
| IsDeviceID     | "true" or "false" |
| IsInternal     | "true" or "false" |
| IsMandatory    | "true" or "false" |
| UsePool        | "true" or "false" |
| Username       | Text              |
| Password       | Text              |
| DataDepend     | Text              |

### Example: Variable Annotation

```
##template variables
@(DisplayName="Host Name", Description = "Description of the host")
String hostname;
@(DisplayName="Host Address", Description = " test description" IsManagementIP=true)
ipAddress hostAddress;
##
```

### Example: IsMandatory Annotation

```
##template variables
@(IsMandatory="ipv6!=null")
ipV4Address ipv4;
@(IsMandatory="ipv4!=null")
ipV6Address ipv6;
##
```

### IsShowAnnotation

```
##template variables
boolean isVlan;
@(IsShow="isVlan==true")
integer vlanNo;
##
```

## Templates Content

This section includes the configuration commands and any parameters that you want to include in the template. These commands can include the variables declared in the template variables section. During the command generation process the variable values are substituted appropriately in the template content.



#### Note

You must specify the commands that you include as if you were entering them in the global configuration command mode on any device. You must consider the command mode when you include commands.

Template content is governed by the usage of variables.

- **Scalar variables**—does not take a range or array of values which cannot be used for iteration (In the variable types table those marked iterate-able as 'No'). Scalar variables must be defined inside the template content.

Syntax: \$\$<variable name>\$\$  
 Example: \$\$USER\_NAME\$\$

- **Iterative variables**—used for block iteration. These loop variable must be accessed as shown below inside the iteration block.

Syntax: @<loop variable>  
 Example:  
 foreach val in \$\$INTEGER\_RANGE\_VALUE\$\$ {  
 @val  
 }

- **Scalar Structure Variable**—Structure member variables can be accessed inside the template content.

Syntax: \$\$<structure instance name>.<member variable name>\$\$  
 Example: \$\$myInterface.inf\_name\$\$

- **Array Structure Variable**—Structure member variables can be accessed inside the template content.

Syntax: \$\$<structure instance name>.<member variable name>\$\$  
 Example: \$\$myInterface.inf\_name\$\$

In addition to the template variables, you can use the conditional and iterative command generation using the following statements:

- **if-else if-else Statement**—makes a logical decision in inclusion/exclusion of set of configuration command based on the value assigned for the variable in it.

Syntax: if(<operand 1> <logical operator> <operand 2>){  
 command1 ..  
 command2..  
 ..  
 } else if (<operand 3> <logical operator> <operand 4> )  
 {  
 Command3 ..  
 Command4..  
 ..  
 } else  
 {  
 Command5 ..  
 Command6..  
 ..  
 }  
 Example: if-else if-else statement  
 if(\$\$USER\_NAME\$\$ == 'admin'){  
 Interface2/10  
 no shut  
 } else {  
 Interface2/10  
 shut  
 }

- **foreach Statement**—used for iterating a block of commands. The iteration is performed based on the assigned loop variable value.

Syntax:  
 foreach <loop index variable> in \$\$<loop variable>\$\$ {  
 @<loop index variable> ..  
 }  
 Example: foreach Statement  
 foreach ports in \$\$MY\_INF\_RANGE\$\$ {  
 interface @ports  
 no shut  
 }

- **Optional parameters**—By default all parameters are mandatory. To make a parameter optional, you must annotate the parameter.

In the variable section, you can include the following command:

- **@(IsMandatory=false)**
- **Integer frequency;**

In the template content section, a command can be excluded or included without using “if” condition check, by assigning a value to the parameter. The optional command can be framed as below:

- **probe icmp [frequency frequency-value] [timeout seconds] [retry-count retry-count-value]**

## Advanced Features

The following are the advanced features available to configure templates.

- **Assignment Operation**

Config template supports assignment of variable values inside the template content section. The values are validated for the declared data type of the variable. If there is a mismatch, the value is not assigned.

Assignment operation can be used under the following guidelines:

- The operator on the left hand side must be any of the template parameter or a for loop parameter.
- The operator on the right hand side values can be any of value from template parameter, for loop parameter, literal string values surrounded by quotes or simple string values.

If a statement does not follow these guidelines, the does not suit this format would not be considered as assignment operation. It is substituted during command generation like other normal lines.

```
Example: Template with assignment operation
##template properties
name =vlan creation;
userDefined= true;
supportedPlatforms = All;
templateType = CLI;
published = false;
##
##template variables
integerRange vlan_range;
@(internal=true)
integer vlanName;
##
##template content
foreach vlanID in $$vlan_range$$ {
 vlan @vlanID
 $$vlanName$$=@vlanID
 name myvlan$$vlanName$$
}
##
```

- **Evaluate methods**

Config template uses the Java runtime provided Java script environment to perform arithmetic operations (such as ADD, SUBTRACT, and so on), string manipulations, and so on.

Locate the javascript file in the template repository path. This file contains primary set of arithmetic, string functions. You can also add custom Javascript methods.



These methods can be called from config template content section in below format:

```
Example1:
$$somevar$$ = evalscript(add, 100, $$anothervar$$)
```

Also the evalscript can be called inside if conditions as below:

```
if($$range$$ > evalscript(sum, $$vlan_id$$, -10)){
do something...
}
```

You can call a method located at the backend of the Java script file.

- Dynamic decision

Config template provides a special internal variable “LAST\_CMD\_RESPONSE”. This variable stores the last command response from the device during the execution of the command. This can be used in the config template content to make dynamic decisions to deliver the commands based on the device condition.




---

**Note** The if block must be followed by an else block in a new line, which can be empty.

---

An example use case to create a VLAN, if it is does not exist on the device.

```
Example: Create VLAN
##template content
show vlan id $$vlan_id$$
if($$LAST_CMD_RESPONSE$$ contains "not found"){
vlan $$vlan_id$$
}
else{
}
}
##
```

This special implicit variable can be used only in the “IF” blocks.

- Template referencing

You can have a base template with all the variables defined. This base template can be imported to multiple templates. The base template content is substituted in the appropriate place of the extending template. The imported template parameters and the contents can be accessed inside the extending template.

```
Example: Template Referencing
Base template:
##template properties
name =a vlan base;
userDefined= true;
supportedPlatforms = All;
templateType = CLI;
published = false;
timestamp = 2015-07-14 16:07:52;
imports = ;
##
##template variables
integer vlan_id;
##
##template content
vlan $$vlan_id$$
##
```

```
Derived Template:
##template properties
name =a vlan extended;
userDefined= true;
supportedPlatforms = All;
templateType = CLI;
```

```

published = false;
timestamp = 2015-07-14 16:07:52;
imports = a vlan base,template2;
##
##template variables
interface vlanInterface;
##
##template content
<substitute a vlan base>
interface $$vlanInterface$$
<substitute a vlan base>
##

```

When you launch the extended template, the parameter inputs for the base template are also obtained. Additionally, the substituted content is used for complete CLI command generation.

- Solution POAP Templates for VXLAN and FabricPath

From Cisco DCNM Release 10.0(1), Cisco provides you a set of defined templates to aid in POAP operations. You can download Cisco-defined templates from <https://software.cisco.com/download/release.html>.

For instructions on how to download and install POAP templates, refer to *Cisco DCNM Installation Guide, Release 10.0(x)*.

## Adding a Template

You can add user-defined templates and schedule jobs.

### Procedure

- 
- Step 1** From the menu bar, select **Configure > Templates > Deploy**.  
You see the name of the template along with its description, Platforms and Tags.
- Step 2** Click the **Add** icon to add a new template.
- Step 3** Specify a **Template Name**, **Template Description** and **Tags** for the new template.
- Step 4** From the **Imports > Template Name** list, check the template check box.  
The base template content is displayed in the Template content window. The base template displays the template properties, template variables and template content. This can be imported in to another template and the base template content is substituted in the appropriate place of the extending template. When the user launches the extended template, the parameter inputs for the base template are also obtained. Additionally, the substituted content is used for complete CLI command generation.
- Note** The Base templates are CLI templates.
- Step 5** Select the Supported Platforms that the template must support.
- Step 6** Click in the Template Content window to edit the template syntax.  
For information about the structure of the Configuration Template, see [Template Structure](#), on page 142.
- Step 7** Select **POAP** to make this template available when you power on the application.  
**Note** The template will be considered as a CLI template if POAP is not selected.
- Step 8** Select **Published** to make the template read-only. You cannot edit a published template.
- Step 9** Click **Validate Template Syntax** to validate the template values.  
If an error or a warning message appears, you can check the validation details in the **Validation Table**.

**Note** You can continue to save the template if there are warnings only. However, if there is an error, you must edit the templates to fix the errors before you proceed.

**Step 10** Click **Save** to save the template.

**Step 11** Click **Save and Exit** to save the configuration and go back to the configuring templates screen.

---

## Configuring Template Job

You can configure and schedule jobs for individual templates from the **Config > Delivery > Templates** page.

### Procedure

---

**Step 1** From the menu bar, select **Config > Templates**.

You see the name of the template along with its description, Platforms and Tags.

**Step 2** Use the checkbox to select a template from the list.

**Step 3** Click the **Launch Job Creation Wizard** icon and click **Next**.

**Step 4** Use the drop-down to select the Device Scope.

The devices configured under the selected Device Scope are displayed.

**Note** If no devices are displayed, check if the device LAN credentials are configured from Cisco DCNM **Web Client > Configure > Credentials Management > LAN Credentials**.

**Step 5** Use the arrows to move the devices to the right column for job creation and click **Next**.

**Step 6** Specify the VSAN\_ID, VLAN\_ID, ETH\_SLOT\_NUMBER, VFC\_SLOT\_NUMBER, SWITCH\_PORT\_MODE, ETH\_PORT\_RANGE and ALLOWED\_VLANS values.

**Step 7** Use the checkbox Edit variables per device to edit the variables for specific devices and click **Next**.

**Step 8** If you have selected multiple devices, use the drop-down to select a specific device and preview its configuration. Click **Back** to edit the configuration or click **Next**.

**Step 9** Specify a Job Description.

The Device Credentials will be populated from **Configure > Credentials Management > LAN Credentials**.

**Step 10** Use the radio button to select **Deliver Instantly** or **Choose time to deliver**.

If you select **Choose time to deliver**, specify the date and time for the job delivery.

**Step 11** Use the checkbox to select **Copy Run to Start**.

**Step 12** If you want to configure additional Transaction and Delivery options, use the checkbox to select **Show more options**.

**Step 13** Under Transaction Options (Optional), if you have a device with rollback feature support, select **Enable Rollback** checkbox and select the appropriate radio button.

**Step 14** Under Delivery Options (Optional), specify the Timeout in seconds and use the radio button to select the Delivery Order.

**Step 15** Click **Finish** to create the job.

A confirmation message is displayed that the job has been successfully created.

---

## Modifying a Template

You can edit the user-defined templates. However, the pre-defined templates cannot be edited. You cannot edit a template if it is already Published.

### Procedure

- 
- Step 1** From the menu bar, select **Config > Templates**.  
You can see the name of the template along with its description, Platforms and Tags.
- Step 2** Select a template from the list and click the **Modify/View template** icon.
- Step 3** Edit the Template Description, Tags.  
The edited Template content is displayed in the right-hand pane.
- Step 4** From the **Imports > Template Name** list, check the template check box.  
The base template content is displayed in the Template content window. You can edit the template content based on your requirement in the Template Content window. Click on the Help icon next to the Template Content window for information about editing the content of the template.
- Step 5** Edit the Supported Platforms for the template.
- Step 6** Click **Validate Template Syntax** to validate the template values.
- Step 7** Click **Save** to save the template.
- Step 8** Click **Save and Exit** to save the configuration and go back to the configuring templates screen.
- 

## Importing a Template

Perform the following task to import a template to the Web Client.



### Note

You can import Cisco-defined FabricPath and IP VXLAN Programmable Fabric POAP Templates to the Cisco DCNM Web Client. For more information, see [Installing POAP Templates, on page 159](#).

---

### Procedure

- 
- Step 1** From the menu bar, select **Config > Templates** and click on the **Import template** icon.
- Step 2** Browse and select the template saved on your computer.  
You can edit the template parameters, if required. For information, see [Modifying a Template, on page 158](#).
- Step 3** Click **Validate Template Syntax** to validate the template.
- Step 4** Click **Save** to save the template or **Save and Exit** to save the template and exit.
-

## Installing POAP Templates

Cisco DCNM allows you to add, edit or delete user-defined templates configured across different Cisco Nexus platforms. From Cisco DCNM Release 10.0(x), Cisco-defined FabricPath and IP VXLAN Programmable Fabric POAP Templates are provided as a separate download on the official Cisco website. These templates are compatible for use with the DCNM Virtual Appliance (OVA or ISO) for use with Nexus 2000, Nexus 5000, Nexus 6000, Nexus 7000, and Nexus 9000 Series switches.

You can download the Cisco-defined templates from <https://software.cisco.com/download/release.html>.

Perform the following task to install the POAP templates from the Cisco DCNM Web Client.

### Procedure

- 
- Step 1** Navigate to [www.cisco.com/go/dcnm](http://www.cisco.com/go/dcnm), and download the latest file.  
You can choose one of the following:
- `dcnm_ip_vxlan_fabric_templates.10.0.1a.zip`
  - `dcnm_fabricpath_fabric_templates.10.0.1a.zip` file
- Step 2** Unzip and extract the files to the local directory on your computer.
- Step 3** Launch the Cisco DCNM Web Client and navigate to **Configure > Templates > Deploy**.
- Step 4** Click on the Import template icon.
- Step 5** Browse and select the template saved on your computer. You can edit the template parameters, if required.
- Step 6** Check **POAP** and **Publish** checkbox to designate these templates as POAP templates.
- Step 7** Click **Validate Template Syntax** to validate the template.
- Step 8** Click **Save** to save the template or **Save and Exit** to save the template and exit.
- 

## Exporting a Template

### Procedure

- 
- Step 1** From the menu bar, select **Configure > Templates > Deploy**.
- Step 2** Use the checkbox to select a template(s) and click the **Export template** icon.  
The browser will request you to open or save the template to your directory.
- 

## Deleting a Template

You can delete the user-defined templates. However, you cannot delete the pre-defined templates.

### Procedure

- 
- Step 1** From the menu bar, select **Configure > Templates > Deploy**.
- Step 2** Use the checkbox to select a template(s) and click the Remove template icon.  
The template will be deleted without any warning message.
- 

### What to Do Next

The template will be deleted from the list of templates on the Web Client. However, when you restart the DCNM services, the deleted templates will be displayed on the **Web Client > Configure > Templates > Deploy**.

To delete the template permanently, delete the template under in your local directory: `C:\Cisco Systems\dcn\dcnm\data\templates\`.

## Configuring Jobs

### Procedure

- 
- Step 1** From the menu bar, select **Configure > Templates > Jobs**.  
The jobs are listed along with the Job ID, description and status.
- Step 2** Click the **Show Filter** icon to filter the jobs by Job ID, Description, Devices and Status.  
In the Status column, use the drop-down to select the job status.
- Step 3** Select a job and click the **Delete** icon to delete the job.
- Step 4** To view the status of a job, click the **Job ID** radio button and click **Status**.
- Step 5** To view the command execution status for a device, click the radio button of a device name from the **Devices** table in the **Job Execution Status** window.
- 

## Backup

The Backup menu includes the following submenus:

## Switch Configuration

This feature allows you to backup device configurations from running configuration as a regular text file in the file system. However, you can also perform operations on startup configuration. The backup files can be stored in the DCNM server host or on a file server.

You can also configure the archive system to support scheduling of jobs for the selected list of devices. You can configure only one job for a switch.

**Note**

When FCoE is enabled for the Cisco Nexus 5000 or 6000 Series Switches, the configuration archive feature cannot generate archives for these switches as the checkpoint files work only when FCOE is disabled.

The following tables describe the icons and fields that appear on **Configure > Backup > Switch Configuration**.

**Table 31: Switch Configuration Operations**

| Icon      | Description                                                                                                            |
|-----------|------------------------------------------------------------------------------------------------------------------------|
| Import    | Allows you to import a user-defined configuration file to the DCNM server.                                             |
| Compare   | Allows you to compare two configuration files, from different devices or on the same device.                           |
| Copy      | Allows you to Copy a configuration file of a switch to the bootflash of the selected destinations switch(es).          |
| Restore   | Allows you to restore configuration from the selected devices.<br>You can also choose to restore from a Golden backup. |
| View/Edit | Allows you to view or edit the configuration file.                                                                     |
| Delete    | Allows you to delete the configuration file.                                                                           |

**Table 32: Switch Configuration Field and Description**

| Field         | Description                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------|
| Device Name   | Displays the device name<br>Click on the arrow next to the device to view the configuration files.              |
| IP Address    | Displays the IP address of the device.                                                                          |
| Group         | Displays the group of the device.                                                                               |
| Configuration | Displays the configuration files archived for that device.                                                      |
| Archive Time  | Displays the time when the device configuration files were archived.<br>The format is Day:Mon:DD:YYYY HH:MM:SS. |
| Size          | Displays the size of the archived file.                                                                         |

| Field  | Description                                                |
|--------|------------------------------------------------------------|
| Golden | Displays if the current version is a Golden backup or not. |

This section contains the following:

## Import Configuration File

You can import the configuration file from the file server to the Cisco Prime DCNM.

Perform the following task to import a single or multiple configuration files.

### Procedure

- 
- Step 1** From Cisco Prime DCNM **Web Client > Configure > Backup**, click **Import**.  
The file server directory opens.
- Step 2** Browse the directory and select the configuration file you want to import. Click **Open**.  
A confirmation screen appears.
- Step 3** Click **Yes** to import the selected file.  
The imported configuration file appears as User Imported file on the **Configure > Backup > Switch Configuration** page.
- 

## Compare Configuration Files

This feature allows you to compare the configuration file with another version of the same device or with the configuration file of another device.

Perform the following task to compare the configuration files.

### Procedure

- 
- Step 1** From Cisco DCNM **Web Client > Configure > Backup > Switch Configuration**, click on the arrow next to the device name to view the configuration files on the device.
- Step 2** Check the checkbox and select two configuration files to compare.  
The first file you selected is designated as Source and the second configuration file is designated as the Target file.
- Step 3** Click **Compare**.  
**View Config Diff** page appears, displaying the difference between the two configuration files.  
The Source and Target configuration files content is displayed in two columns. From the drop-down list in the right-top corner, choose **All** to view the entire configuration or choose **Changed** to view the configuration differences of the configuration files.  
The differences in the configuration file are show in the table, with legends.



Red ☐ Deleted configuration details

Green ☐ New added configuration

Blue ☐ Modified configuration details

**Step 4** Click **Copy to Target** to copy the source configuration to the target configuration file. Click **Cancel** to revert to the configuration details page.

The Copy Configuration window displays the source configuration preview and the target device of the destination configuration. The selected devices area shows the following fields:

- Device Name—Specifies the target device name to which the source configuration will be copied.
- IP Address—Specifies the IP Address of the destination device.
- Group—Specifies the group to which the device belongs.
- Golden Config—Specifies the version of the destination configuration.
- Status—Specifies the status of the device.

**Step 5** Click **Yes** to copy the configuration to the destination device configuration.

---

## Copy Configuration

You can copy the configuration files to the same device, to another device, or multiple devices concurrently. Perform the following task to view the status of tasks.

### Procedure

---

**Step 1** From Cisco DCNM Web Client > **Configure** > **Backup** > **Switch Configuration**, select any startup/running/archive configuration of the device that you need to copy.

**Step 2** Click Copy icon.

Copy Configuration page appears, displaying the Source Configuration preview and Selected Devices area..

Source Configuration Preview area shows the contents of running/startup/version configuration file which will be copied to the devices.

**Step 3** In the Selected Devices area, check device name checkbox to copy the configuration to the device.

**Note** You can select multiple destination devices to copy the configuration.

The selected devices area shows the following fields:

- Device Name—Specifies the target device name to which the source configuration will be copied.
- IP Address—Specifies the IP Address of the destination device.
- Group—Specifies the group to which the device belongs.
- Golden Config—Specifies the version of the destination configuration.
- Status—Specifies the status of the device.

- Step 4** Click **Copy**.  
A confirmation window appears.
- Step 5** Click **Yes** to copy the configuration to the destination device configuration.
- 

## Restore Configuration

You can restore the configuration file from the selected switches or from the Golden backup.



**Note** You cannot restore the configuration for SAN switches.

---

Perform the following task to restore the configuration from the selected devices.

### Procedure

---

- Step 1** From Cisco DCNM **Web Client** > **Configure** > **Backup** > **Switch Configuration**, select any startup/running/archive configuration. Click **Restore**.
- Step 2** Check the Device Name check box from which you want to restore the configuration. Click **Restore**. In the Restore Settings area, select the following based on the requirement.
- Copy to Startup—Check this check box to copy the configuration to the startup configuration.
  - Rollback on Error—Check this check box to revert the configuration file to the previous version, if an error occurs.

The selected devices area shows the following fields:

- Device Name—Specifies the device name from the which the configuration file will be restored.
- IP Address—Specifies the IP Address of the device.
- Group—Specifies the group to which the device belongs.
- Golden Config—Specifies the version of the destination configuration.
- Status—Specifies the status of the device.

**Note** You can restore the configuration only from the same device.

If you select user imported configuration files, you can restore configuration for any number of devices.

---

## Golden Backup

You can restore the configuration file from a Golden Backup.

Perform the following task to restore the configuration from a Golden Backup.

### Procedure

- 
- Step 1** From Cisco DCNM Web Client > **Configure** > **Backup** > **Switch Configuration**, click **Golden Backup**.
- Step 2** In the **Copy/Restore Settings** area, choose from the following:
- **Copy to Startup**—Check this check box to copy the configuration to the startup configuration.
  - **Rollback on Error**—Check this check box to revert the configuration file to the previous version, if an error occurs.
- Step 3** In the **Selected Devices** areas, check the **Device Name** check box to select the device as golden backup. By default, DCNM selects golden configuration.  
The selected devices area shows the following fields:
- **Device Name**—Specifies the device name from the which the configuration file will be restored.
  - **IP Address**—Specifies the IP Address of the device.
  - **Group**—Specifies the group to which the device belongs.
  - **Golden Config**—Specifies the version of the destination configuration.
  - **Status**—Specifies the status of the device.
- Step 4** Click **Restore**.
- 

## View or Edit Configuration

You can view or edit the configuration file on the device.

Perform the following task to view or edit the configuration file for the devices.

### Procedure

- 
- Step 1** From Cisco DCNM Web Client > **Configure** > **Backup** > **Switch Configuration**, click the arrow next to the device name to view the configuration files on the device. Click the configuration file radio button to view or edit the selected configuration file.
- Step 2** Click the **View/Edit Configuration** icon.  
The **View/Edit configuration** window appears showing the configuration file content in the right column.
- Step 3** Edit the configuration file as required.
- Step 4** Click **Save** to apply the changes or click **Cancel** to discard changes.
- 

## Delete Configuration

Perform the following task to delete the configuration file from the device.

**Note**

Ensure that you take a backup of the configuration file before you delete.

**Procedure**

- Step 1** From Cisco Prime DCNM **Web Client** > **Configure** > **Backup** > **Switch Configuration**, click on the arrow next to the device name to view the configuration files on the device.
- Step 2** Click the configuration file radio button to be deleted.  
**Note** You can delete multiple configuration files. However, you cannot delete startup, running, or golden configuration files.
- Step 3** Click **Yes** to delete the configuration file.

**Archive Jobs**

This section contains context sensitive online help content under Cisco DCNM **Web Client** > **Configure** > **Backup** > **Archive Jobs**.

The following table describes the fields that appear on **Configure** > **Backup** > **Switch Configuration** > **Archive Jobs** window.

| Field          | Description                                                              |
|----------------|--------------------------------------------------------------------------|
| User           | Specifies the who created this job                                       |
| Group          | Specifies the group to which this job belongs.                           |
| Schedule       | Specifies the schedule of the job. Also show the recurrence information. |
| Last Execution | Specifies the date and time at which this job was last executed.         |
| Job Status     | Specifies if the job was successful or failure.                          |

**Note**

When you upgrade the Cisco DCNM to Release 10.0.x, the Archive Jobs will not be migrated. You will have to create new jobs. Navigate to **Cisco DCNM Web Client** > **Configure** > **Backup** > **Switch Configuration** > **Archive Jobs** > **Archive Jobs** tab to create new jobs. The Archive files created for a device before upgrading to Cisco DCNM Release 10.0.x, will be visible only after you create a new job for the device after upgrading.

**Archive Jobs**

You can add, delete or view the job.

**Note**

You must set the SFTP/TFTP credentials before you configure Jobs. On the DCNM Web Client, navigate to **Administration > DCNM Server > SFTP/TFTP Credentials** to set the credentials.

**Procedure**

- Step 1** To add a job, from the Cisco DCNM Web Client > **Configure > Backup > Archive Jobs > Archive Jobs** tab, click **Add Job**.  
The Create Job screen displays the Schedule, Device Selection and Selected Devices.  
A backup will be scheduled as defined.
- a) In the **Schedule** area, configure the start time, repeat interval and repeat days.
- **Start At**—Configure the start time using the hour:minutes:second drop-down lists.
    - **Once**—Configure the job to be executed once, on the particular day. The time at which this job will be executed is determined by the **Start At** field.
    - **Now**—Configure the job to be executed immediately. Cisco DCNM will consider the default date and time as configured on the server.
    - **Daily**—Check the check box on the days you want this job to be executed. The time at which this job will be executed is determined by the **Start At** field.
    - **Real Time**—Configure the job to be executed if there is any configuration changes in the device. The device must be quiet for 5 minutes, after which the DCNM Sever will execute this job.
  - **Repeat Interval**—Check the Repeat Interval check box to repeat the job at scheduled intervals. Configure the intervals using either days or hours drop-down list.
  - **Comments**—Enter
- b) In the **Device Selection** area, use the radio button to choose one of the following:
- **Device Group**—Click the Device Group radio button to select the entire group of devices for this job.  
Select the Device Group from the drop-down list.

**Note** When the devices are not licensed, they will not be shown under the group on the Cisco DCNM Web Client > **Configure > Backup > Switch Configuration > Archive Jobs**. When none of the devices under a group is licensed, the group alone will be shown with no devices, until a device under that group is licensed.

When the SAN and LAN credentials are not configured for a Switch, it will not be listed in the Selected Devices drop-down list. To configure, navigate to **Configure > Credentials Management > SAN Credentials** and **Configure > Credentials Management > LAN Credentials**.
  - **Selected Devices**—Click the **Selected Devices** radio button to select one of multiple devices from various groups for this job.  
Select the devices from the drop-down list.

**Note** When the SAN and LAN credentials are not configured for a Switch, it will not be listed in the Selected Devices drop-down list. To configure, navigate to **Configure > Credentials Management > SAN Credentials** and **Configure > Credentials Management > LAN Credentials**.

c) In the **Selected Devices** area, the following fields are shown:

- Name—Specifies the name of the device on which the job is scheduled.
- IP Address—Specifies the IP Address of the device.
- Group—Specifies the group to which the device belongs.

**Note** If a job for a device exists under device level, you can create a group level job which includes this switch as part of that group. However, this switch will be excluded during the execution of the job.

d) Click **Create** to add a new job.

**Step 2** To view the details of the job, from the Cisco DCNM Web Client > **Configure > Backup > Archive Jobs > Archive Jobs**, check the job check box.

a) Click **View Job**.

The Schedule, Device Selection and the Selected devices for this job is displayed.

b) Click **OK** to revert to view the list of jobs.

### What to Do Next

You can also configure the Cisco DCNM to retain the number of archived files per device. On the Cisco DCNM Web Client > **Administration > DCNM Server > Server Properties**, update the **archived.versions.limit** field.

### Job Execution Details

The Cisco Prime DCNM Web Client > **Configure > Backup > Switch Configuration > Archive Jobs > Archive Jobs > Job Execution Details** tab shows the following tabs in the Job Execution History table.

| Field        | Description                                                                         |
|--------------|-------------------------------------------------------------------------------------|
| Job Name     | Displays the system-generated job name.                                             |
| User         | Specifies the persona of the person who created the job.                            |
| Device Group | Specifies fabric or the LAN group under which the job was created.                  |
| Device       | Specifies the IP Address of the Device.                                             |
| Server       | Specifies the IP Address of the DCNM Server to which the device is associated with. |

| Field          | Description                                                                                                                                                                                                                                                                                                                  |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol       | Specifies if the SFTP or TFTP protocol is applied.                                                                                                                                                                                                                                                                           |
| Execution time | Specifies the time at which the job was last executed.                                                                                                                                                                                                                                                                       |
| Status         | <p>Specifies the status of the job.</p> <ul style="list-style-type: none"><li>• Skipped</li><li>• Failed</li><li>• Successful</li></ul>                                                                                                                                                                                      |
| Error Cause    | <p>Specifies the error if the job has failed. The categories are as follows:</p> <ul style="list-style-type: none"><li>• No change in the configuration.</li><li>• Switch is not managed by this server.</li></ul> <p><b>Note</b> If the error cause column is empty, it implies that the job was executed successfully.</p> |

## Network Config Audit

Cisco DCNM provides auditing for the configuration changes across the network switches. The Network Audit Reporting feature enables you to generate an audit report so that you can track the added, deleted, or modified configurations. You will be able to generate network audit reports only when you have existing archival jobs. Using the generated reports, you can view the configuration differences on a device for a specified period.

This section contains the following:

### Generating Network Config Audit Reports

#### Procedure

- Step 1** From Cisco Prime DCNM **Web Client** > **Configure** > **Backup**, click **Network Config Audit**. The Network Audit Report page appears.
- Step 2** In the **Devices** drop-down list, choose the devices for which you want to generate a report.
- Step 3** Specify the **Start Date** and **End Date**.
- Step 4** Click the **Generate Report** button to view the configuration differences. The configuration differences are shown using colors.
  - Red—Deleted Configuration
  - Green—Newly Added Configuration

- Blue—Changed configuration
- Strikethrough—Old configuration

After you generate a report, you can export the configuration reports into a HTML file.

---

## Creating a Network Config Audit Report

### Procedure

---

- Step 1** From Cisco DCNM Web Client, choose **Monitor > Report > Generate**. The left pane of the page shows various reports that you can create.
- Step 2** Choose **Common > Network Config Audit**.
- Step 3** In the **Report Name** field, enter the name of the report.
- Step 4** In the **Repeat** field, choose the appropriate repeat interval, that is, Daily, Weekly or Monthly. Daily job generates report of configuration differences for all the selected devices for last 1 day. Weekly job generates a report for the last 7 days and the monthly job generates a report for the last 30 days.
- Step 5** In the **Start** and **End** date fields, specify the start and end date for the report.
- Step 6** In the **Email Report** field specify the email delivery options.
- No—If you do not want to send the report through email, select this option.
  - Link Only—Select this option if you want to send the link to the report.
  - Contents—Select this option if you want to send the report content.

If you select Link Only or Contents option, enter the email address and subject in the **To** and **Subject** fields.

---

## Monitoring Network Config Audit Report

### Procedure

---

- Step 1** From Cisco DCNM Web Client, choose **Monitor > Report > View**.
- Step 2** Choose **Common > Network Config Audit** on the left pane to the network config audit reports.
-



## Deleting a Network Config Audit Report

### Procedure

- 
- Step 1** From Cisco DCNM Web Client, choose **Monitor > Report > View**.
- Step 2** Choose **Common > Network Config Audit**. The View Reports page displays the reports you have created.
- Step 3** Select the reports that you want to delete, and then click the **Delete** button.
- 

# Image Management

The Image Management menu includes the following submenus:

## Upgrade [ISSU]

The Upgrade [ISSU] menu includes the following submenus:

### Upgrade History [ISSU]

This feature enables you to upgrade the Cisco Nexus Platform Switches using In-Service Software Upgrade (ISSU). This upgrade procedure may be disruptive or non-disruptive based on the device configuration. You can select the Kickstart, System, or SSI images required for the upgrade from a remote server using SFTP, SCP, TFTP, FTP or from the file system on the device. In order to select the images from the server, the same needs to be configured from **Web Client > Configure > Image Management > Repositories** tab.

The following table describes the fields that appear on **Configure > Image Management > Upgrade [ISSU] > Upgrade History**.

| Field     | Description                                                                                                         |
|-----------|---------------------------------------------------------------------------------------------------------------------|
| Task Id   | Specifies the serial number of the task. The latest task will be listed in the top.                                 |
| Task Type | Specifies the type of task. <ul style="list-style-type: none"><li>• Compatibility Check</li><li>• Upgrade</li></ul> |
| Owner     | Based on the Role-Based Authentication Control (RBAC), specifies the owner who initiated this task.                 |
| Devices   | Displays all the devices that were selected for this task.                                                          |

| Field        | Description                                                                                                                                                                   |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Job Status   | Specifies the status of the job. <ul style="list-style-type: none"> <li>• Planned</li> <li>• In Progress</li> <li>• Completed</li> <li>• Completed with Exceptions</li> </ul> |
| Created Time | Specifies the time when the task was created.                                                                                                                                 |
| Scheduled At | Specifies the time when the task is specified to be executed. You can also choose to schedule a task to be executed at a later time.                                          |
| Comment      | Shows any comments that the Owner has added while performing the task.                                                                                                        |

**Note**

After a fresh Cisco DCNM installation, this page will have no entries.

You can perform the following:

**New Installation**

Perform the following task to upgrade the devices discovered by Cisco DCNM.

**Procedure**

- 
- Step 1** From Cisco DCNM **Web Client** > **Configure** > **Upgrade**, click **New Installation** to install or upgrade the kickstart and the system images on the devices.  
The devices with default VDCs are displayed in the Select Switches page.
- Step 2** Select the check box to the left of the Switch Name.  
You can select more than one device and move the devices to the right column.
- Step 3** Click on Add or Remove icons to include the appropriate switches for upgrade.  
The selected switches appear in the right hand column.
- Step 4** Click **Next** to navigate to Specify Software Images page. This tab displays the switches you selected in the previous screen and allows you to choose the images for upgrade.
- The **Auto File Selection** check box enables you to specify a file server, image version, and path whereby you can apply the upgrade image to the selected devices.
  - In the **Select File Server** drop-down list, select the one of the file servers that is created in the Cisco DCNM repositories.

- In the **Image Version** field, specify the image version. For example, enter 7.3.9.D1.1 in the Image Version field if you have selected m9700-sf3ek9-kickstart-mz.7.3.0.D1.1.bin as the image version.
- In the **Path** field, specify the image path. In the case of SCP and SFTP, you need to specify an absolute path. For example, //root/images/. In the case of FTP and TFTP, you need to specify a relative path with respect to FTP/TFTP home directory. If you are using TFTP server provided by Cisco DCNM (local DCNM TFTP), then you need to specify the absolute path of the image. You cannot use the same DCNM TFTP server for creating another job when the current job is in progress.

**Step 5** Click **Select Image** in the Kickstart image column.  
Software Image Browser screen appears.

**Note** Cisco Nexus 3000 Series and Cisco Nexus 9000 Series Switches require only the System image to load the Cisco NX-OS operating system. Therefore, the option to select Kickstart images for these devices will be disabled.

**Step 6** Click on the Select Image in the System image column.  
Software Image Browser screen appears.

**Step 7** (Optional) Click on the Storage Services Interface (SSI) Image in the System image column. Determine the correct Cisco MDS Software release and SSI image version.  
This step is applicable only for Cisco MDS devices.

**Step 8** On the Software Image Browser screen, you can choose the Kickstart image from File Server or Switch File System.

If you choose File Server:

- From the **Select the File server** list, choose the appropriate file server on which the Kickstart image is stored.  
The servers at **Configure > Image Management > Repositories** are displayed in the drop-down list.
- From the **Select Image** list, choose the appropriate Kickstart image. Click the check box to use the same image for all other selected devices of the same platform.  
Example: For platform types N7K-C7009 and N7K-C7010, logic matches platform(N7K) and three characters (C70) from sub-platform. The same logic is used across all platform switches.
- Click **OK** to choose the Kickstart image or **Cancel** to revert to the Specify Software Images page.  
If the File Server selected is either `ftp` or `tftp`, in the text box, enter the relative path of the file from the home directory.

If you choose Switch File System:

- From the Select Image list, choose the appropriate image located on the flash memory of the device.
- Click **OK** to choose the Kickstart image or **Cancel** to revert to the Specify Software Images page.

**Step 9** The **Vrf** column indicates the name of the virtual routing and forwarding (VRF).  
VRF is not applicable for Cisco MDS devices.

**Step 10** In the **Available Space** column specify the available space for the **Primary Supervisor** and **Secondary Supervisor** modules of the switch.  
Available Space column shows the available memory in MB on the switch (for less than 1 MB, it is shown and marked as KB).

Bootflash browser shows the File Name, Size and Last Modified Date for all the files and directories on the switch bootflash. You can delete the files(s) by selecting files(s) and clicking 'Delete' to increase the available space on switch.

**Step 11** Selected Files Size column shows the size of images selected from the SCP or SFTP server.

If the total size of selected images is greater than available space on switch, the file size is marked in red. We recommend that you create more space on switch to copy images to switch and install.

**Step 12** Drag and drop the switches to reorder the upgrade task sequence.

**Step 13** Select **Skip Version Compatibility** if you are sure that the version of the Cisco NX-OS software on your device is compatible with the upgrade images that you have selected.

**Step 14** Select **Select Parallel Line Card upgrade** to upgrade all the line cards at the same time.  
Upgrade of parallel line card is not applicable for Cisco MDS devices.

**Step 15** Click **Next**.

If you did not select **Skip Version Compatibility**, the Cisco DCNM performs a Compatibility check.

You can choose to wait until the check is complete or click **Finish Installation Later**. The installation wizard is closed and a Compatibility task is created in **Web Client > Configure > Image Management > Upgrade** tasks. The time taken to check the compatibility of the image depends on the configuration and the load on the device.

The Version Compatibility Verification status column displays the status of verification.

Click on the arrow next to the device Name to view the response from the device for the task.

If you choose to **Skip Version Compatibility**, the Cisco DCNM displays all the devices and the images for upgrade.

**Step 16** Click **Finish Installation Later** to perform the upgrade later.

**Step 17** Click **Next**.

**Step 18** Check **Next** check box to put device in maintenance mode before upgrade.

**Step 19** Select the check box to save the running configuration to the startup configuration before upgrading the device.

**Step 20** You can schedule the upgrade process to occur immediately or at a later date.

- 1 Select **Deploy Now** to upgrade the device immediately.
- 2 Select **Choose time to Deploy** and specify the time in MMM/DD/YYYY HH:MM:SS format to perform the upgrade later.

This is relative to the server time. If the selected time to deploy is in the past, the job is executed immediately

**Step 21** You can choose the execution mode based on the devices and the line cards you have chosen to upgrade.

- 1 Select **Sequential** to upgrade the devices in the order in which they were chosen.
- 2 Select **Concurrent** to upgrade all the devices at the same time.

**Step 22** Click **Finish** to begin the upgrade process.

The Installation wizard closes and a task to Upgrade is created on the **Web Client > Configure > Image Management > Upgrade** page.

---

## Finish Installation

You can choose to complete the installation for tasks which was completed on the **Compatibility Check** page. Perform the following task to complete the upgrade process on the devices.

### Procedure

---

- Step 1** From Cisco DCNM **Web Client > Configure > Upgrade**, select a task for which the compatibility check is complete.  
Select only one task at a time.
- Step 2** Click **Finish Installation**.  
Software Installation Wizard appears.
- Step 3** Select the checkbox to save the running configuration to the startup configuration before upgrading the device.
- Step 4** Select the checkbox to put device in maintenance mode before upgrade. This option is valid only for the devices that support maintenance mode.
- Step 5** You can schedule the upgrade process to occur immediately or at a later date.
- 1 Select **Deploy Now** to upgrade the device immediately.
  - 2 Select **Choose time to Deploy** and specify the time in DD/MM/YYYY HH:MM:SS format to perform the upgrade later.
- Step 6** You can choose the execution mode based on the devices and the line cards you have chosen to upgrade.
- 1 Select **Sequential** to upgrade the devices in the order in which they were chosen.
  - 2 Select **Concurrent** to upgrade the devices at the same time.
- Step 7** Click **Finish** to complete the upgrade process.
- 

### View

Perform the following task to view the status of tasks.

### Procedure

---

- Step 1** From Cisco DCNM **Web Client > Configure > Upgrade**, select the task id check box.  
Select only one task at a time.
- Step 2** Click **View**.  
Installation Task Details screen appears.
- Step 3** Click on the Settings icon drop-down list. Select Columns and choose the column details options.  
This displays the location of the kickstart and system images, compatibility check status, installation status, descriptions and logs.
- Step 4** Select the device.  
The detailed status of the task is displayed below. For the completed tasks, the response from the device is displayed.  
If the upgrade task is in progress, a live log of the installation process appears.

**Note** This table is refreshed every 30secs for jobs in progress, when you are on this screen.

## Delete

Perform the following task to delete a task.

### Procedure

- Step 1** From Cisco DCNM Web Client > **Configure** > **Upgrade**, select the task id checkbox.
- Step 2** Click **Delete**.
- Step 3** Click **OK** to confirm deletion of the job.

## Switch Level History

You can view the history of the upgrade process at a switch level. You can view the current version of the switch and other details.

The following table describes the fields that appear on **Configure** > **Image Management** > **Upgrade [ISSU]** > **Switch Level History**.

| Field           | Description                                          |
|-----------------|------------------------------------------------------|
| Switch Name     | Specifies the name of the Switch                     |
| IP Address      | Specifies the IP Address of the Switch               |
| Platform        | Specifies the Cisco Nexus Switch platform            |
| Current Version | Specifies the current version on the switch software |

Click the radio button next to the Switch Name to select the switch for which you need to view the upgrade history. Click **View** to view the upgrade task history for the selected switch.

The following table describes the fields that appear on **Configure** > **Image Management** > **Upgrade [ISSU]** > **Switch Level History** > **View** > **Upgrade Tasks History**

| Field | Description                                    |
|-------|------------------------------------------------|
| Owner | Specifies the owner who initiated the upgrade. |

| Field           | Description                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Job Status      | Specifies the status of the job. <ul style="list-style-type: none"> <li>• Planned</li> <li>• In Progress</li> <li>• Completed</li> </ul> |
| KickStart Image | Specifies the KickStart image used to upgrade the Switch.                                                                                |
| System Image    | Specifies the System image used to upgrade the Switch.                                                                                   |
| Completed Time  | Specifies the date and time at which the upgrade was successfully completed.                                                             |

## Patch [SMU]

The Patch [SMU] menu includes the following submenus:

### Patch Installation History

This feature allows you to activate or deactivate packages using Software Maintenance Update (SMU). Personnel with Admin privileges can perform this operation.

The following table describes the fields that appear on **Configure > Image Management > Patch [SMU] > Installation History**.

| Field       | Description                                                                                                                             |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Task Id     | Specifies the serial number of the task. The latest task will be listed in the top.<br>The tasks are performed in the sequential order. |
| Switch Name | Specifies the name of the switch for which the patch file is installed.                                                                 |
| IPAddress   | Specifies the IP Address of the device.                                                                                                 |
| Task        | Specifies if the patch is installed or uninstalled on this device.                                                                      |
| Package     | Specifies the name of the patch file.                                                                                                   |
| Status      | Specifies the status of installation or uninstallation of the patch files.                                                              |

| Field              | Description                                                                |
|--------------------|----------------------------------------------------------------------------|
| Status Description | Describes the status of installation or uninstallation of the patch files. |

This section contains the following:

## Install Patch

Perform the following task to install the patch on your devices via Cisco DCNM Web Client.

### Before You Begin

### Procedure

- 
- Step 1** From Cisco DCNM **Web Client > Configure > Patch**, click **Install**.  
The SMU Installation Wizard appears. Cisco Nexus licensed switches discovered by Cisco DCNM are displayed.
- Step 2** Select the checkbox to the left of the Switch Name.  
You can select more than one device.
- Step 3** Click on Add or Remove icons to include the appropriate switches for installing patch.  
The selected switches appear in the right hand column.
- Step 4** Click **Next**.
- Step 5** Click on **Select Packages** in the Packages column.  
SMU Package Browser screen appears.
- Step 6** On the SMU Package Browser screen, you can choose the patch file from File Server or Switch File System.  
If you choose File Server:
- From the Select the File server list, choose the appropriate file server on which the patch is stored.  
The servers at **Configure > Image Management > Repositories** are displayed in the drop-down list.
  - From the Select Image list, choose the appropriate patch that must be installed on the device.  
You can select more than 1 patch file to be installed on the device.
- Note** If the patch installation requires a restart of the device, select only one patch file.  
Click the checkbox to use the same patch for all other selected devices of the same platform.
- Click **OK** to choose the patch image or **Cancel** to revert to the SMU Installation Wizard.
- If you choose Switch File System:
- From the Select Image list, choose the appropriate patch file image located on the flash memory of the device.  
You can select more than 1 patch files to be installed on the device.
  - Click **OK** to choose the Kickstart image or **Cancel** to revert to the Specify Software Images page.
- Step 7** Click **Finish**.  
You can view the list of patches installed on the switch, on the **Web Client > Inventory > Switches** page.



---

## Uninstall Patch

Perform the following task to uninstall the patch on your devices via Cisco DCNM Web Client.

### Procedure

---

- Step 1** From Cisco DCNM **Web Client** > **Configure** > **Patch [SMU]**, click **Uninstall**.  
The SMU Installation Wizard appears. Cisco Nexus licensed switches discovered by Cisco DCNM are displayed.
- Step 2** Select the radio button to the left of the Switch Name.  
You can select more than one image device.
- Step 3** Click on Add or Remove icons to include the appropriate switches for installing patch.  
The selected switches appear in the right hand column.
- Step 4** Click **Next**.
- Step 5** Select the check box to the left of the Switch Name.  
The patches applied to the switch is displayed in the right column.
- Step 6** Select the patches that you want to uninstall from this device.  
You can select more than one patch applied on the device.
- Note** If the patch installation requires you to restart the device, select only one patch file.
- Step 7** Click **Finish** to uninstall the patch from the device.  
You can uninstall more than one patch at a time.
- 

## Delete Patch Installation Tasks

Perform the following steps to delete the patch installation tasks.

### Procedure

---

- Step 1** From Cisco DCNM **Web Client** > **Configure** > **Image Management** > **Patch [SMU]** > **Installation History**, select the task id checkbox.
- Step 2** Click **Delete**.
- Step 3** Click **OK** to confirm deletion of the patch installation task.
-

## Switch Installed Patches

You can view the patches installed on all the Switches in the network. You can refresh the view to see the latest installed patches.

The following table describes the fields that appear on **Configure > Image Management > Patch [SMU] > Switch Installed Patches**.

| Field             | Description                                                         |
|-------------------|---------------------------------------------------------------------|
| Switch Name       | Specifies the name of the Switch.                                   |
| IP Address        | Specifies the IP Address of the Switch.                             |
| Platform          | Specifies the Cisco Nexus Switch platform.                          |
| Installed Patches | Specifies the currently installed patches on the licensed switches. |

Click **Refresh** to refresh the table.

## Package [RPM]

The Package [RPM] menu includes the following submenus:

### Package Installation [RPM]

The package [RPM] feature allows you to install RPM packages. This feature is available for the Nexus 9000 switches only.

The following table describes the fields that appear on **Configure > Image Management > Package (RPM) > Installation History**.

| Field       | Description                                                                                                                                 |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Task Id     | Specifies the serial number of the task. The latest task will be listed in the top.<br><br>The tasks are performed in the sequential order. |
| Switch Name | Specifies the name of the switch for which the package file is installed.                                                                   |
| IPAddress   | Specifies the IP Address of the device.                                                                                                     |
| Task        | Specifies if the package is installed or uninstalled on this device.                                                                        |
| Package     | Specifies the name of the package file.                                                                                                     |

| Field              | Description                                                                    |
|--------------------|--------------------------------------------------------------------------------|
| Status             | Specifies the status of installation or uninstallation of the package files.   |
| Completed Time     | Specifies the time at which the installation or uninstallation task completed. |
| Status Description | Describes the status of installation or uninstallation of the package files.   |

This section contains the following:

### Install Package (RPM)

Perform the following task to install the package on your devices via Cisco DCNM Web Client.

#### Before You Begin

#### Procedure

- 
- Step 1** From Cisco DCNM **Web Client** > **Configure** > **Package (RPM)**, click **Install**.  
The RPM Installation Wizard appears.
  - Step 2** Select the checkbox to the left of the Switch Name.  
You can select more than one device.
  - Step 3** Click on Add or Remove icons to include the appropriate switches for installing packaging.  
The selected switches appear in the right hand column.
  - Step 4** Click **Next**.
  - Step 5** Click on **Select Packages** in the Packages column.  
The RPM Package Browser screen appears.
  - Step 6** On the RPM Package Browser screen, you can choose the package file from File Server or Switch File System.  
If you choose File Server:
    - a) From the Select the File server list, choose the appropriate file server on which the package is stored.  
The servers at **Configure** > **Image Management** > **Repositories** are displayed in the drop-down list.
    - b) From the Select Image list, choose the appropriate package that must be installed on the device.  
You can select only one package file to be installed on the device.  
Click the checkbox to use the same package for all other selected devices of the same platform.
    - c) Click **OK** to choose the patch image or **Cancel** to revert to the RPM Installation Wizard.  
If you choose Switch File System:
    - a) From the Select Image list, choose the appropriate package file image located on the flash memory of the device.  
You can select only one package file to be installed on the device.

b) Click **OK**.

**Step 7** In the Installation Type drop-down list, choose one of the installation types:

- Normal—Fresh installation
- Upgrade—Upgrading the existing RPM
- Downgrade—Downgrading the existing RPM

**Step 8** Click **Finish**.

You can view the list of packages installed on the switch, on the **Web Client > Inventory > Switches** page.

**Note** If you are using Cisco DCNM Release 10.1(2), in case of installation of reload RPMs, a manual "install commit" needs to be performed on the switch once the switch is reloaded.

---

## Uninstall Package [RPM]

Perform the following task to uninstall the RPM on your devices via Cisco DCNM Web Client.

### Procedure

---

**Step 1** From Cisco DCNM **Web Client > Configure > Package [RPM]**, click **Uninstall**.  
The RPM Uninstallation Wizard appears.

**Step 2** Select the check box to the left of the Switch Name.  
You can select more than one switch.

**Step 3** Click the Add or Remove icons to include the appropriate switches for uninstalling the package.  
The selected switches appear in the right hand column.

**Step 4** Click **Next**.

**Step 5** Select the radio button to choose active packages on devices for uninstallation.  
The packages applied to the switch is displayed in the right column.

**Step 6** Click **Finish** to uninstall the package from the device.  
You can uninstall more than one package at a time.

**Note** If you are using Cisco DCNM Release 10.1(2), in case of uninstallation of reload RPMs, a manual "install commit" needs to be performed on the switch once the switch is reloaded.

---

## Delete Package Installation Tasks

Perform the following tasks to delete the package installation tasks from the history view.

### Procedure

- 
- Step 1** From Cisco DCNM Web Client > **Configure** > **Image Management** > **Package [RPM]** > **Installation History**, select the task id checkbox.
- Step 2** Click **Delete**.
- Step 3** Click **OK** to confirm deletion of the task.
- 

## Switch Installed Packages

You can view the RPM packages installed on all the Switches in the network. You can refresh the view to see the latest installed packages.

The following table describes the fields that appear on **Configure** > **Image Management** > **Packages [RPM]** > **Switch Installed Packages**.

| Field              | Description                                                                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch Name        | Specifies the name of the Switch.                                                                                                                                                  |
| IP Address         | Specifies the IP Address of the Switch.                                                                                                                                            |
| Platform           | Specifies the Cisco Nexus Switch platform.                                                                                                                                         |
| Installed Packages | Specifies the currently installed packages on the licensed switches.If there are multiple RPM packages installed on the switch, the names of the packages are separated by commas. |

Click **Refresh** to refresh the table.

## Maintenance Mode [GIR]

The Maintenance Mode [GIR] menu includes the following submenus:

### Maintenance Mode [GIR]

This feature allows you to isolate the Cisco Nexus Switch from the network in order to perform an upgrade or debug, using Graceful Insertion and Removal (GIR). When the switch maintenance is complete, you can return the switch to normal mode. When the switch is in the maintenance mode, all protocols are gracefully brought down and all physical ports are shut down. When the normal mode is restored, all the protocols and ports are initiated again.

Perform the following to change the system mode of the devices.

## Procedure

- 
- Step 1** From Cisco DCNM Web Client > **Configure** > **Maintenance Mode [GIR]**, check the Switch Name check box.  
You can select multiple switches.
- Step 2** For Cisco Nexus 9000 and 3000 Series Switches, Mode Selection allows you to choose from one of the following options.
- Shutdown
  - Isolate
- Note** Click the appropriate option before you change the mode.
- Step 3** Click **Change System Mode**.  
A confirmation message appears.
- Step 4** Click **OK** to confirm to change the maintenance mode of the device.  
The status of operation can be viewed in the **System Mode** and the **Maintenance Status**.
- 

## Switch Maintenance History

You can view the history of the maintenance mode changes executed from the Cisco DCNM.

The following table describes the fields that appear on **Configure** > **Image Management** > **Maintenance Mode [GIR]** > **Switch Maintenance History**.

| Field              | Description                                                                         |
|--------------------|-------------------------------------------------------------------------------------|
| Task Id            | Specifies the serial number of the task. The latest task will be listed in the top. |
| Switch Name        | Specifies the name of the Switch for which the maintenance mode was changed.        |
| IP Address         | specifies the IP Address of the Switch.                                             |
| User               | Specifies the name of the user who initiated the maintenance.                       |
| System Mode        | Specifies the mode of the System.                                                   |
| Maintenance Status | Specifies the mode of the maintenance process.                                      |
| Status             | Specifies the status of the mode change.                                            |
| Completed Time     | Specified the time at which the maintenance mode activity was completed.            |

Click the radio button next to the Switch Name to select the switch for which you need to view the upgrade history. Click **View** to view the upgrade task history for the selected switch.

The following table describes the fields that appear on **Configure > Image Management > Upgrade [ISSU] > Switch Level History > View > Upgrade Tasks History**

| Field           | Description                                                                                                                          |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Owner           | Specifies the owner who initiated the upgrade.                                                                                       |
| Job Status      | Specifies the status of the job. <ul style="list-style-type: none"><li>• Planned</li><li>• In Progress</li><li>• Completed</li></ul> |
| KickStart Image | Specifies the KickStart image used to upgrade the Switch.                                                                            |
| System Image    | Specifies the System image used to upgrade the Switch.                                                                               |
| Completed Time  | Specifies the date and time at which the upgrade was successfully completed.                                                         |

## Repositories

This feature allows you add image servers and configuration servers information to fetch images for Upgrade, Patch and POAP mode operations.

You need to specify valid servers for SFTP/FTP/TFTP. DCNM does not perform the validation for SFTP/FTP/TFTP servers while creating or updating the servers. DCNM performs validation only for the SCP servers.

**Note**

The SCP repositories use SSH protocol for directory listing and therefore you need to enable SSH on the SCP repository server. The SFTP repository uses SFTP protocol for directory listing. The TFTP and FTP repositories do not support directory listing. You need to manually provide the file path.

### Add Image or Configuration Server URL

Perform the following task to add an image or a configuration server URL to the repository.

### Procedure

---

- Step 1** On the Image and Configuration Servers page, click the Add icon.
- Step 2** Click the radio button to select the protocol.  
The available protocols are **scp**, **ftp**, **sftp**, and **tftp**.  
You can use both IPv4 and IPv6 addresses with these protocols.
- Step 3** In the Add Image or Configuration Servers URL window, specify a Name for the image.
- Step 4** Enter Hostname/Ipaddress and Path to download or upload files.
- Step 5** Specify the Username and Password.
- Step 6** Click **OK** to save.
- 

## Editing an Image or Configuration Server URL

Perform the following task to edit an image or a configuration server URL to the repository.

### Procedure

---

- Step 1** On the Image and Configuration Servers page, select an existing Image and Configuration Server from the list, and click the Edit icon.
- Step 2** In the **Edit Image or Configuration Servers URL** window, edit the required fields.
- Step 3** Click **OK** to save or click **Cancel** to discard the changes.
- 

## Deleting an Image or Configuration Server URL

Perform the following task to delete an image or a configuration server URL to the repository.

### Procedure

---

- Step 1** On the Image and Configuration Servers page, select an existing Image and Configuration Server from the list, and click the Delete icon.
- Step 2** In the delete notification, click **Yes** to delete the image and configuration server.
- Note** The default SCP Repository cannot be deleted.
- 

## File Browser

You can view the contents of the server on the Image and Configuration Servers page.



On the **Image and Configurations**, check the **Server Name** check box to view the content.  
Click **File Browser** to view the contents of this server.

## Image Upload

Perform the following task to upload different types of images to the server. These images will be used by the devices during POAP.

### Procedure

- 
- Step 1** On the Image and Configuration Servers page, check the server name check box to select the server for uploading images.  
The Select Image File window appears.
  - Step 2** Click **Browse** to select the image file from the directory.
  - Step 3** From the **Platform** drop-down list, select the device to which you need to upload this image.
  - Step 4** From the **Type** drop-down list, select the type of the image you are uploading to the device.
  - Step 5** Click **OK**.  
The image is uploaded to the repository.
- 

# Credentials Management

The Credential Management menu includes the following submenus:

## SAN Credentials

The Cisco DCNM **Web Client > Configure > Credentials Management > SAN Credentials** displays the SNMP access details to the fabric seed switch. If the Web Client user has validated the access to all the fabrics, the SNMP credentials for all the seed switches of the fabrics is displayed.

The Switch Credentials for the DCNM User table has the following fields.

| Field       | Description                                                                                |
|-------------|--------------------------------------------------------------------------------------------|
| Fabric Name | The fabric name to which the switch belongs.                                               |
| Seed Switch | IP Address of the switch.                                                                  |
| User Name   | Specifies the username of the switch DCNM user.                                            |
| Password    | Displays the encrypted form of the switch snmp user.                                       |
| SNMPv3/SSH  | Specifies if the SNMP protocol is validated or not.<br>The default value is <b>false</b> . |

| Field        | Description                                                                    |
|--------------|--------------------------------------------------------------------------------|
| Auth/Privacy | Specifies the Authentication protocol<br>The default value is <b>NOT_SET</b> . |
| Status       | Displays the status of the switch                                              |

Before the Cisco DCNM user configures the Fabric using SNMP, the user must furnish and validate SNMP credentials on the seed switch of the fabric. If the user does not provide valid credentials for the fabric seed switch, the Switch Credentials table shows the default values for SNMPv3/SSH and AuthPrivacy fields.

Click on the switch row and enter correct credentials information. Click **Save** to commit the changes.

If the user changes the configuration, but does not provide a valid switch credential, the user action will be rejected. You must validate the switch credentials to commit your changes.

You can perform the following operations on this screen.

- To Revalidate the credentials:
  - 1 From the Cisco DCNM **Web Client > Configure > Credentials Management > SAN Credentials**, click on the **Fabric Name** radio button to select a seed switch whose credentials are not validated.
  - 2 Click **Revalidate**.  
A confirmation message appears, stating if the operation was successful or a failure.
- To clear the switch credentials:
  - 1 From the Cisco DCNM **Web Client > Configure > Credentials Management > SAN Credentials**, click on the **Fabric Name** radio button to select a seed switch to delete.
  - 2 Click **Clear**.  
A confirmation message appears.
  - 3 Click **Yes** to delete the switch credential from the DCNM server.

## LAN Credentials

While changing the device configuration, Cisco DCNM uses the device credentials provided by the user. However, if the LAN Switch credentials are not provided, Cisco DCNM prompts you to open the **Web Client > Configure > Credentials Management > LAN Credentials > Default Credentials** page to configure LAN credentials.

Cisco DCNM uses two sets of credentials to connect to the LAN devices:

- **Discovery Credentials**—Cisco DCNM uses this credentials during discovery and periodic polling of the devices.
- **Configuration Change Credentials**—Cisco DCNM uses this credentials when user tries to use the features that change the device configuration.

LAN Credentials Management allows you to specify configuration change credentials. Before changing any LAN switch configuration, you must furnish *Configuration Change* SSH credentials for the switch. If you do not provide the credentials, the configuration change action will be rejected.

These features get the device write credentials from LAN Credentials feature.

- Upgrade (ISSU)
- Maintenance Mode (GIR)
- Patch (SMU)
- Template Deployment
- POAP-Write erase reload, Rollback
- Interface Creation/Deletion/Configuration
- VLAN Creation/Deletion/Configuration
- VPC Wizard

You must specify the configuration change credentials irrespective of whether the devices were discovered initially or not. This is a one-time operation. Once the credentials are set, that will be used for any configuration change operation.

### Default Credentials

Default credentials is used to connect all the devices that the user has access to. You can override the default credentials by specifying credentials for each of the devices in the Switch Table below.

Cisco DCNM tries to use individual switch credentials in the Switch Table, to begin with. If the credentials (username/password) columns are empty in the Switch Table, the default credentials will be used.

### Switch Table

Switch table lists all the LAN switches that user has access. You can specify the switch credentials individually, that will override the default credentials. In most cases, you need to provide only the default credentials.

You can perform the following operations on this screen.

- [Edit Credentials, on page 190](#)
- [Validate Credentials, on page 190](#)
- [Clear Switch Credentials, on page 190](#)

The LAN Credentials for the DCNM User table has the following fields.

| Field      | Description                                      |
|------------|--------------------------------------------------|
| Switch     | Displays the LAN switch name.                    |
| IP Address | Specifies the IP Address of the switch.          |
| User Name  | Specifies the username of the switch DCNM user.  |
| Password   | Displays the encrypted form of the SSH password. |

| Field | Description                                     |
|-------|-------------------------------------------------|
| Group | Displays the group to which the switch belongs. |

### Edit Credentials

Perform the following task to edit the credentials.

- 1 From the **Cisco DCNM Web Client > Configure > Credentials Management > LAN Credentials**, check the **Switch** check box for which you need to edit the credentials.
- 2 Click Edit icon.
- 3 Specify **User Name** and **Password** for the switch.

### Validate Credentials

Perform the following task to validate the credentials.

- 1 From the **Cisco DCNM Web Client > Configure > Credentials Management > LAN Credentials**, check the **Switch** check box for which you need to validate the credentials.
- 2 Click **Validate**.  
A confirmation message appears, stating if the operation was successful or a failure.

### Clear Switch Credentials

Perform the following task to clear the switch credentials.

- 1 From the **Cisco DCNM Web Client > Configure > Credentials Management > LAN Credentials**, check the **Switch** check box for which you need to clear the credentials.
- 2 Click **Clear**.
- 3 Click **Yes** to clear the switch credentials from the DCNM server.

## LAN Fabric Settings

The LAN Fabric Settings menu includes the following submenus:

### LAN Fabrics

You can use Cisco DCNM Web Client to edit and update the LAN Fabric Settings.

The following table describes the fields that appear on **Configure > LAN Fabric Settings > LAN Fabrics**.

| Field       | Description                                                          |
|-------------|----------------------------------------------------------------------|
| Fabric Name | Specifies the name of the fabric provided while adding a new fabric. |

| Field                 | Description                                                                                                                                                                            |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fabric Provision Mode | Specifies the provision mode for the fabric.                                                                                                                                           |
| Fabric Encapsulation  | Specifies the fabric encapsulation you choose for this fabric.<br><br>The options are: <ul style="list-style-type: none"> <li>• FabricPath</li> <li>• VXLAN</li> <li>• VLAN</li> </ul> |
| Allowed Leaf Switches | Specifies the type(s) of leaf switches in this fabric.                                                                                                                                 |
| ASN                   | Specifies the Fabric Autonomous System Number .                                                                                                                                        |
| Description           | Displays the description that you provided while you created the fabric.                                                                                                               |

This section contains the following:

## Add LAN Fabric

Perform the following task to add LAN fabric.

### Procedure

- 
- Step 1** From Cisco DCNM **Web Client** > **Configure** > **LAN Fabric Settings** > **LAN Fabrics**, click add icon to add a LAN fabric.  
The Add/Edit LAN Fabric screen appears.
- Step 2** On the General Settings tab, configure the general settings for the LAN fabric.
- In the Fabric Name field, enter the name for the fabric.  
Use only alphanumeric characters such as A-Z, a-z, 0-9 and special characters underscore (\_) and hyphen (-) are allowed.
  - In the Description field, enter a description for the fabric.
  - In the Fabric Provision Mode drop-down, select the fabric provision mode.
    - DCNM Orchestrated (Top down)
    - Non-DCNM Orchestrated (Top down)
    - Auto Configuration (Bottom up)
    - Manual

If Fabric provision Mode is selected as DCNM Orchestrated (Top down), and Allowed Leaf Switches is selected as N9K Leaf Switches, then you can select either Multicast Replication or Ingress Replication

from the Replication Mode drop-down. If you select Multicast Replication in the Replication Mode drop-down, you can configure the VXLAN Encapsulation Settings.

- d) In the Fabric Technology drop-down, select the fabric technology for your fabric. Based on the fabric technology option, the following profiles will be loaded in Border Leaf/BorderPE/Edge Router screens.

- FabricPath—The profiles from profilesBridgeDomain(FPBD) table
- VXLAN—The profiles from profilesIPBridgeDomain(IPBD) table

**Note** If you choose VXLAN, you can configure the VXLAN Encapsulation Settings for the allowed leaf switches.

- e) In the Allowed Leaf Switches drop-down, based on the Fabric Technology, choose the switches for the leaf.
- f) In the Fabric Autonomous System Number (ASN) field, enter the ASN number for all the switches within this fabric.  
The valid range is from 1 to 65536.

**Step 3** On the Fabric Provision Settings tab, configure the various parameters for provisioning this fabric.

- a) In the Image Servers block, click on Add icon, Edit icon or Delete icon to add, edit or delete user-defined servers for image files.  
These server details are fetched from **Configure > Image Management > Repositories**.
- b) Click **Save** to add the new server.
- c) In the LDAP block, you can retain the default settings or edit the fields appropriately.
- LDAP Server—Edit the default IP Address or specify the IP Address of the LDAP Server.
  - Fabric Organization Unit (OU)—This is an auto-generate value. The fabric-related data will be created under this OU.
  - LDAP User Name—Specifies the username to access the LDAP server. .
  - LDAP Password—Displays the encrypted LDAP password.
  - Use SSL—Check Use SSL checkbox to enable Cisco DCNM to communicate with LDAP server via secure channel.
- d) In the DHCP block, update the subnet and DNS information.
- Primary (Backbone) Subnet—Enter a valid IPv4 or an IPv6 address of the subnet.  
If you have entered an IPv4 address for the subnet, also enter the subnet mask.
  - Primary DNS—Enter a valid IPv4 or an IPv6 address of the Primary DNS server.
  - Secondary DNS—Enter a valid IPv4 or an IPv6 address of the Secondary DNS server.
- e) In the AMQP block, enable and configure the AMQP server.  
Advanced Message Queuing Protocol (AMQP) message broker helps in hypervisor manager synchronization and REST API event messaging. The AMQP event bus facilitates automation and synchronization with external agents.
- Enable AMQP Notification—Check this option to generate AMQP notifications.
  - AMQP Server—Enter the IP Address of the AMQP Server

- AMQP Port— Specifies the AMQP port value. The default value is 5672.
- AMQP Virtual Host— Specifies the AMQP virtual host. The default host is /root.
- AMQP User Name—Specifies the username for the AMQP server.
- AMQP Password—Displays the encrypted AMQP server password.
- AMQP Exchange Name—Specifies the AMQP exchange name.

Exchanges are AMQP entities where messages are sent. Exchanges take a message and route it into zero or more queues. The routing algorithm used depends on the exchange type and rules called bindings.

**Step 4** On the Pool Settings tab, configure L2 Segment, L3 partition and VLAN range information.

- a) In the L2 Segment ID block, click on Add icon, Edit icon or Delete icon to add, edit or delete user-defined orchestrator for L2 segment.

- Orchestrator—Specifies the Orchestrator name.
- Segment ID Range—Specifies the segment ID range for that Orchestrator.

The Segment ID range is unique for all Orchestrators. The default Segment ID range cannot be used for any orchestrator.

- b) In the L3 Partition ID block, click on Add icon, Edit icon or Delete icon to add, edit or delete user-defined orchestrator for L3 partition.

- Orchestrator—Specifies the Orchestrator name.
- Partition ID Range—Specifies the partition ID range for that Orchestrator.

- c) In the VLAN Range block, configure the VLAN range and configure the mobility domains for the fabric.

- System Dynamic VLAN Range
- Core Dynamic VLAN Range
- Translate VLAN Range

Click on Add icon, Edit icon or Delete icon to add, edit or delete mobility domains for the fabric.

- Mobility Name—Species the name for the mobility domain.
- Detectable VLAN Range—Specifies the VLAN IP address range for mobility domain
- Global Mobility Domain— Indicates whether the specified mobility domain is the global mobility domain.

**Step 5** On the Fabric Border tab, configure the border settings for the fabric.

- Enable Partition Extension across Fabric—Enables partition extension across fabric.
- Load Balancing Algorithm—Displays the algorithm applied to Border Leaf/Edge Router pair selection for partition extension.

The algorithm determines whether to choose border leaf based on the least load, fair share, round robin, resource consumption, speed or other criteria.

- **Redundancy Factor**—For each VRF, this specifies the number of Border Leaf/Edge router pairs that the VRF will be instantiated on. The valid range is from 0-100.

This ensures that the VRFs is extended on the specified number sets of border leaf switch. The selected number of Border Leaf/Edge Router pairs for partition (VRF) extension also depends on the Border Leaf/Edge Router pairing topology. Therefore, the number of pairs is equal to or greater than the specified redundancy factor.

- **BGP Route Target ASN**—Specify the autonomous system (AS) number to compose the Route Target using the BGP protocol. This AS number is used for Edge Router and Hub PE.

If you do not specify AS number, Cisco DCNM will disable the partition extension.

**Step 6** Click **Save** to add a LAN Fabric.

---

## Delete LAN Fabric

Perform the following task to delete the LAN fabric.

### Procedure

---

**Step 1** From Cisco DCNM **Web Client** > **Configure** > **LAN Fabric Settings** > **LAN Fabrics**, select the fabric to delete.

**Step 2** Click the Delete icon.

Cisco DCNM will ensure no fabric plan, POAP definition, auto-config data are associated with that LAN fabric before it is deleted.

**Note** The fabric will be deleted without any warning.

---

## Edit LAN Fabric

Perform the following task to edit the LAN fabric.

### Procedure

---

**Step 1** From Cisco DCNM **Web Client** > **Configure** > **LAN Fabric Settings** > **LAN Fabrics**, click on the fabric that you want to edit.

**Step 2** Click the Edit icon..

You can edit all the parameters.

For detailed information, see [Add LAN Fabric](#), on page 191.

**Step 3** Click **Save** to save your changes or click **Cancel** to discard the changes.

---



## Add Fabric Plan

Perform the following task to add a fabric plan for the existing LAN fabric.

### Procedure

- 
- Step 1** From Cisco DCNM **Web Client** > **Configure** > **LAN Fabric Settings** > **LAN Fabrics**, select the fabric to which you want to add a fabric plan.
- Step 2** Click **Add Fabric Plan**.  
The Fabric Plan Wizard screen appears.
- Step 3** In the **Define Switch Type** tab, configure the switch types.
- In the **Switch Type** block, you can add, delete or edit the switch counts available for each switch type and their ports.  
Click on Add icon, Edit icon or Delete icon to add, edit or delete switch types..
    - **Switch Role**—From the dropdown list, choose from Leaf, Spine or BorderLeaf to select the role of the switch.
    - **Switch Count**—Specifies the maximum number of switches allowed in that particular role of the switch.
    - **Fabric Port**—Specifies the port on which the fabric is configured.
    - Click **Save** to apply your configurations.
  - In the Spine Switches block, you can configure leaf switches.  
Click on Add icon, Edit icon or Delete icon to add, edit or delete leaf switches.
    - **Switch Type**—From the drop down list, select from the available Cisco NX-OS switches.
    - **Default POAP Template**—From the drop down list, select the POAP template for the switch.
    - **System Image**—From the drop down list, select the system image for the switch.
    - **Kickstart Image**—From the drop down list, select the kickstart image for the switch.
    - Click **Save** to apply your configurations.
  - In the Spine Switches block, you can configure spine switches.
    - **Switch Type**—From the drop down list, select from the available Cisco NX-OS switches.
    - **Default POAP Template**—From the drop down list, select the POAP template for the switch.
    - **System Image**—From the drop down list, select the system image for the switch.
    - **Kickstart Image**—From the drop down list, select the kickstart image for the switch.
    - Click **Save** to apply your configurations.
  - In the BorderLeaf Switches block, you can configure BorderLeaf switches.
    - **Switch Type**—From the drop down list, select from the available Cisco NX-OS switches.

- **Default POAP Template**—From the drop down list, select the POAP template for the border leaf switch.
- **System Image**—From the drop down list, select the system image for the border leaf switch.
- **Kickstart Image**—From the drop down list, select the kickstart image for the border leaf switch.
- Click **Save** to apply your configurations.

**Step 4** Click **Next**.

**Step 5** In the Define Switch Interface tab, configure the interfaces for the switch.  
You can configure the Management IP, fabric and vPC interfaces for the switch.

a) In the Management IP block:

- **Switch Management IP Range**—Specifies the Management IP Address range for the Switch.

b) In the Fabric Interface block:

**Note** This block is visible only if you are creating a VXLAN-based LAN Fabric.

- **Mask used for derived subnets**—From the drop down list, select the mask for subnets.
- **Base Subnet for Fabric Links**—Specify the base subnet.

**Step 6** Click **Next**.  
The Specify Switch Definition tab appears.

**Step 7** In the Specify Switch Definitions tab, you can configure parameters for the POAP templates.  
For every POAP template chosen while you configured the Leaf, Spine, or BorderLeaf switches, you can configure POAP parameters, which include administrative username and password.

**Step 8** Click **Next**.  
The Publish Fabric Plan tab appears.

**Step 9** You can view, edit the Fabric Plan parameters shown in the table. Click on the cell you want to edit and enter the new parameters.

**Note** Edit the Serial Number entries and assign correct values or "value:VDC" for each device created in the fabric plan. Without a correct serial number, the POAP function will not work.

- Click **Link Table** to see the links. The link table is applicable only for the Numbered Fabric Interfaces.
- Click **Topology** to view the basic Fabric Plan topology.

Use the scroll bar to view table columns to the right.

**Step 10** Click **Finish** to publish the Fabric Plan.

---

## Delete Fabric Plan

Perform the following task to delete a fabric plan for the LAN fabric.

### Procedure

- 
- Step 1** From Cisco DCNM Web Client > **Configure** > **LAN Fabric Settings** > **LAN Fabrics**, select the fabric to which you want to delete a fabric plan.
- Step 2** Click **Delete Fabric Plan**.
- 

## General LAN Fabric Settings

Cisco DCNM allows you to configure the LAN Fabric Settings under **Web Client** > **Configure** > **LAN Fabric Settings** > **General** tab.

### LAN Fabric General Settings

This sections details the fields and their descriptions for the parameters on the Web Client > Configure > LAN Fabric Settings > General > General Settings tab.

### LAN Fabric Border-Leaf Settings

This sections details the fields and their descriptions for the parameters on the Web Client > Configure > LAN Fabric Settings > General > Border-Leaf Settings tab.

### LAN Fabric POAP Settings

This sections details the fields and their descriptions for the parameters on the Web Client > Configure > LAN Fabric Settings > General > POAP Settings tab.

### LAN Fabric Encapsulation Settings

This sections details the fields and their descriptions for the parameters on the Web Client > Configure > LAN Fabric Settings > General > Fabric Encapsulation Settings .

## Mobility Domains

Cisco DCNM allows you to create mobility domains to configure a Mobility Domain Network. The Mobility Domains configured on this page can be used in **Configure** > **LAN Fabric Settings** > **Mobility Domains** page.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

| Field         | Description                                 |
|---------------|---------------------------------------------|
| Mobility Name | Specifies the name for the mobility domain. |

| Field                 | Description                                                                              |
|-----------------------|------------------------------------------------------------------------------------------|
| Detectable VLAN Range | Specifies detectable VLAN range for the particular mobility domain.                      |
| Add                   | Allows you to add a new mobility domain.                                                 |
| Edit                  | Allows you to edit the selected mobility domain and the VLAN range.                      |
| Delete                | Allows you to delete the mobility domain.                                                |
| Refresh               | Refreshes the list of mobility domains.                                                  |
| Show Filter           | Filters list of domains based on the defined value for each column.                      |
| Print                 | Prints the list of mobility domains and VLAN range.                                      |
| Export                | Exports the list of mobility domains and their details to a Microsoft Excel spreadsheet. |

## Add Mobility Domains

### Procedure

- 
- Step 1** From the menu bar, select **Configure > LAN Fabric Settings > Mobility Domains**.
  - Step 2** Click **Add** to add a new mobility domain.
  - Step 3** In the Mobility Domain Name field, specify the name for the Mobility Domain.
  - Step 4** In the Detectable VLAN Range field, specify the VLAN IP Address Range for mobility domain.
  - Step 5** Click **OK** to add a mobility domain.
- 

## Modify Mobility Domains

### Procedure

- 
- Step 1** From the menu bar, select **Configure > LAN Fabric Settings > Mobility Domains**.
  - Step 2** Select the mobility domain from the list and click **Edit**.
  - Step 3** Update and click **OK** to save the settings.
-

## Delete Mobility Domains

### Procedure

- 
- Step 1** From the menu bar, select **Configure > LAN Fabric Settings > Mobility Domains**.
- Step 2** Select the mobility domain from the list and click **Delete**.
- Step 3** Click **Yes** to delete the mobility domain.
- 

## Segment IDs

Cisco DCNM allows you to create a new Segment ID range, and map the orchestrator ID. DCNM will associate the range with the specified orchestrator ID.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

| Field             | Description                                                                                                                                                                         |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Orchestrator Name | Specifies the Orchestrator name.                                                                                                                                                    |
| Section ID Range  | Specifies the segment ID range for that Orchestrator.<br>The Segment ID range is unique for all Orchestrators.<br>The default Segment ID range cannot be used for any orchestrator. |
| Add               | Allows you to add a new Orchestrator.                                                                                                                                               |
| Edit              | Allows you to edit the selected Orchestrator and segment ID range.                                                                                                                  |
| Delete            | Allows you to delete the Orchestrator.                                                                                                                                              |
| Refresh           | Refreshes the list of Orchestrators.                                                                                                                                                |
| Show Filter       | Filters list of switches based on the defined value for each column.                                                                                                                |
| Print             | Prints the list of Orchestrator and their details.                                                                                                                                  |
| Export            | Exports the list of Orchestrators and their details to a Microsoft Excel spreadsheet.                                                                                               |

- [Add Orchestrator, on page 200](#)
- [Modify Orchestrator, on page 200](#)

- [Delete Orchestrator](#) , on page 200

## Add Orchestrator

### Procedure

---

- Step 1** From the menu bar, select **Configure > LAN Fabric Settings > Segment IDs**.
- Step 2** Click **Add** to add a new orchestrator.
- Step 3** In the **Orchestrator Name** field, specify the name for the Orchestrator.
- Step 4** In the **Segment ID Range** field, specify Segment ID range to be associated with the Orchestrator.
- 

## Modify Orchestrator

### Procedure

---

- Step 1** From the menu bar, select **Configure > LAN Fabric Settings > Segment IDs**.
- Step 2** Select the orchestrator from the list and click **Edit**.
- Step 3** Update and click **OK** to save the settings.
- 

## Delete Orchestrator

### Procedure

---

- Step 1** From the menu bar, select **Configure > LAN Fabric Settings > Segment IDs**.
- Step 2** Select the orchestrator from the list and click **Delete**.
- Step 3** Click **Yes** to delete the orchestrator.
- 

# LAN Fabric Provisioning

The LAN Fabric Provisioning menu includes the following submenus:

## LAN Fabric Provisioning

The LAN Fabric Provisioning feature provides a wizard based workflow for overlay provisioning in Cisco Nexus 9000 Series switches based VXLAN BGP EVPN fabrics. At a very high-level, it allows you to create networks and VRFs in a flexible manner that in turn can be deployed to a set of leaf switches or border devices in a few clicks. A list of networks or a list of VRFs can be selected and simultaneously deployed to multiple switches within a fabric at one go. This newly introduced “Multi-to-Multi” functionality is one of the highlights of the top down provisioning that has been significantly enhanced in the DCNM 10.4(2) release. Also, you can view the status and history of each deployment in a granular way. In the case of networks, optionally, interfaces can be selected on a per switch basis on which the associated VLAN needs to be provisioned. Access and trunk switch ports are supported along with all vPC cases.

The following is a high-level set of features newly introduced in DCNM 10.4(2) with LAN Fabric Provisioning:

- 4-byte ASN support for LAN fabrics including Default\_LAN.
- VRF deployment support to leaf switches.
- Auto-selection of vPC port-channel, one on the other vPC peer when a vPC on one peer is selected.
- Support for deployment of multiple networks/VRFs to multiple leaf switches at the same time (maximum 10 selections at one go).
- Multi selection support of switches using a click & drag (box) selection.
- Support for the option of VLAN input at network creation time, which in turn is used as a hint for network deployment to the switches that can be overridden by the user.
- External fabric support for border node deployments:
  - Setup for VRF\_LITE.
  - Setup for EVPN Multi-Site (Overlay & Underlay).
  - Enhanced topology display with External Cloud connections.
- Support for deployment on border leaf switches for the following:
  - VRFs.
  - VRF\_LITE using subinterfaces with auto-pool management of dot1q tags on a per interface basis (IPv4 & IPv6).
  - vPC Support.
  - Network using regular VLAN hand off.
- EVPN Multi-Site support for Border Gateways:
  - Network extension using Multi-Site.
  - VRF extension using Multi-Site.
  - Simultaneous VRF\_LITE & Multi-Site support.
- Resource Manager visibility into the current usage of all the resources employed by the DCNM for LAN fabric provisioning on a per fabric per switch basis:

- VLANs used for Networks.
  - VLANs used for VRFs.
  - Dot1q IDs used for subinterfaces (applicable for border nodes).
- REST API support for each of the LAN fabric provisioning functionality as published on swagger.

**Note**

The LAN Fabric Provisioning > Network Deployment feature requires NX-OS version 7.0(3)I5(2) or later.

The following sections will help you configure a new fabric or update an existing one.

## Creating a New Fabric

### Procedure

- Step 1** From Cisco DCNM Web Client, choose **Configure > LAN Fabric Provisioning > Network Deployment**. The LAN Fabric Provisioning page appears.  
A new fabric can also be created through **Configure > LAN Fabric Settings > LAN Fabrics**.
- Step 2** Click **Continue**. The **Select a Fabric** page comes up.

## Select a Fabric

Choose a fabric with appropriate switches where you want the Top Down functionality to be enabled or create a new fabric.

SITE\_2

 [Fabric Extension Settings](#)

----- OR -----

[+ Create a new fabric](#)

- Step 3** In the **Select a Fabric** page, perform any of the following tasks:
- Choose a fabric with appropriate switches where you want the LAN Fabric Provisioning functionality to be enabled.



b) Create a new fabric.

- Step 4** In the **Select a Fabric** page, click **Create a new fabric**. The **Create Fabric** page comes up.

### Create Fabric

#### ▼ General Settings

|                                         |                             |
|-----------------------------------------|-----------------------------|
| * Fabric Name                           | <input type="text"/>        |
| Description                             | <input type="text"/>        |
| * Fabric Provision Mode                 | DCNMTopDown ▼               |
| * Fabric Encapsulation                  | VXLANFabric ▼               |
| * Allowed Leaf Switches                 | n9k ▼ ?                     |
| * Replication Mode                      | MulticastReplication ▼      |
| * VRF Template                          | Default_VRF ▼               |
| * Network Template                      | Default_Network ▼           |
| * Fabric Autonomous System Number (ASN) | <input type="text"/> ?      |
| * Network Extension Template            | Default_Network_Extension ▼ |
| * VRF Extension Template                | Default_VRF_Extension ▼     |
| Site ID                                 | <input type="text"/>        |

#### ▼ VXLAN Encapsulation Settings

Create Fabric

- Step 5** Under the **General Settings** area, specify the details of the fabric. If you are connecting a VXLAN EVPN fabric to an external fabric, select **External** in the **Fabric Encapsulation** drop down list, fill in the Autonomous System Number (ASN) of the external fabric and go to Step 8. An external fabric is one that can have either managed or unmanaged devices to which the border nodes of the VXLAN fabric connect to.
- Step 6** For a VXLAN fabric, choose the appropriate replication mode in the **Replication Mode** drop-down list, either Multicast Replication or Ingress Replication.
- Step 7** In the **Pool Settings** area, specify the appropriate ranges of L2 Segment ID (Networks), L3 Segment ID (VRFs), Network VLAN, and VRF VLAN. Note that a new range has been introduced called "Subinterface ID Range". This is used for picking the next free dot1q ID in the pool when instantiating subinterfaces for VRFs when extended over VRF\_LITE on a border node. Another optional parameter called Site ID has been introduced. This is applicable for VXLAN EVPN Multi-Site deployments.

## ▼ Pool Settings

|                         |             |
|-------------------------|-------------|
| * L2 Segment ID Range   | 30000-49999 |
| * L3 Partition ID Range | 50000-59999 |
| * Network VLAN Range    | 2400-2999   |
| * VRF VLAN Range        | 2000-2399   |
| * Subinterface ID Range | 2-511       |

**Step 8** Click **Create Fabric**. A fabric is created.

---

### What to Do Next

Select the appropriate VXLAN fabric from the drop down list and then click on the **Continue** button (top right part of the screen) to create Networks and VRFs that make up the fabric. This workflow is applicable for deployment to leaf switches.

If external connectivity and network or VRF extensions need to be provisioned on the border nodes, the first step is to follow the wizard to define and provision the physical connectivity from the border nodes to the external devices. The external devices are typically part of an external fabric. External devices may be other Nexus 9000 Series switches, Nexus 7000 Series switches, or non-Nexus device (including non-Cisco devices). The provisioning of external connectivity is performed only on the border devices. The external device peer for the border node needs to be provisioned independently.

To start provisioning the external connectivity for a given fabric, select that fabric and then click on the **Fabric Extension Settings** option to add the Inter-Fabric interconnect links.

## Creating a Network

After you select a fabric, you can create networks for the VXLAN BGP EVPN fabric. If there are Layer 2 and Layer 3 virtual network traffic that you want to extend to another fabric, then you should add a distinct instance of those networks within the external fabric in DCNM.

### Procedure

---

- Step 1** From Cisco DCNM Web Client, choose **Configure > LAN Fabric Provisioning > Network Deployment**. The LAN Fabric Provisioning page appears.
- Step 2** Select or create a fabric. Select the external fabric name if you want to extend traffic to an external fabric.
- Step 3** Click **Continue** (at the top right part of the screen). The **Networks** page comes up.

Fabric Selected: site1

Networks Selected 0 / Total 7

|                          | Network Name    | Network ID | VRF Name    | IPv4 Gateway/Subnet | IPv6 Gateway/Prefix | Status   | VLAN ID |
|--------------------------|-----------------|------------|-------------|---------------------|---------------------|----------|---------|
| <input type="checkbox"/> | MyNetwork_30001 | 30001      | MyVRF_50001 |                     |                     | DEPLOYED |         |
| <input type="checkbox"/> | MyNetwork_30002 | 30002      | MyVRF_50003 |                     |                     | PENDING  |         |
| <input type="checkbox"/> | MyNetwork_30003 | 30003      | MyVRF_50004 |                     |                     | DEPLOYED |         |
| <input type="checkbox"/> | MyNetwork_30004 | 30004      | MyVRF_50005 |                     |                     | NA       |         |
| <input type="checkbox"/> | MyNetwork_30006 | 30006      | MyVRF_50006 |                     |                     | NA       |         |
| <input type="checkbox"/> | MyNetwork_30007 | 30007      | MyVRF_50007 |                     |                     | DEPLOYED |         |
| <input type="checkbox"/> | MyNetwork_30008 | 30008      | MyVRF_50008 |                     |                     | NA       |         |

**Step 4** In the **Networks** page, click the **Add Network** button. The **Create Network** page comes up.

### Create Network ✕

▼ Network Information

\* Network ID

\* Network Name

\* VRF Name  +

\* Layer 2 Only ☐

\* Network Template

\* Network Extension Template

VLAN ID

▼ Network Profile

General

Advanced

IPv4 Gateway/NetMask  ? example 192.0.2.1/24

IPv6 Gateway/Prefix  ? example 2001:db8::1/64

Interface Description  ?

Create Network

If you are using the VRF view, you can switch to the Network View by clicking the **Network View** button.

**Step 5** Specify the Network Information settings:

- **Network ID**—Specifies the Layer 2 VNI.
- **Network Name**—Specifies the name of the network. The network name should not contain any white spaces or special characters except underscore ( \_ ) and hyphen ( - ).
- **VRF Name**—Allows you to select the Virtual Routing and Forwarding (VRF). If you want to create a new VRF, click the + button. The VRF name should not contain any white spaces or special characters except underscore ( \_ ), hyphen ( - ), and colon ( : ).

Cisco DCNM Web Client Online Help, 10.4(2) Release

205

**Note** You can also create a VRF by clicking the **VRF View** button on the **Networks** page.

- Layer 2 Only—Specifies whether the network is Layer 2 only.
- Network Template—Allows you to select a network template.

The following parameters are relevant for network extension to another fabric.

- Network Extension Template—Allows you to extend this network to another fabric, based on the extension method you have chosen (VRF Lite, Multi Site, etc).
- VLAN ID—Specifies the corresponding tenant VLAN ID for the network.

**Step 6** Specify the general network profile settings:

- IPv4 Gateway/NetMask—Specifies the IPv4 address with subnet.
- IPv6 Gateway/Prefix—Specifies the IPv6 address with subnet.
- Interface Description—Specifies the description for the interface.
- Extension Type—Specifies the type of extension, such as VRF Lite, Multi Site, etc.

**Step 7** Optionally, specify the advanced profile settings by clicking the **Advanced** tab:

- ARP Suppression
- Ingress Replication
- Multicast Group Address
- DHCPv4 Server
- DHCPv4 Server VRF
- MTU for L3 interface

**Step 8** Click **Create Network**.

The network is added to DCNM and an entry appears in the **Networks** page.

Fabric Selection > Network Selection > Network Deployment > VRF View Continue

Fabric Selected: site1

Networks Selected 1 / Total 9 Show All

| <input type="checkbox"/>            | Network Name    | Network ID | VRF Name    | IPv4 Gateway/Subnet | IPv6 Gateway/Prefix | Status   | VLAN ID |
|-------------------------------------|-----------------|------------|-------------|---------------------|---------------------|----------|---------|
| <input type="checkbox"/>            | MyNetwork_30001 | 30001      | MyVRF_50001 |                     |                     | DEPLOYED |         |
| <input type="checkbox"/>            | MyNetwork_30002 | 30002      | MyVRF_50003 |                     |                     | PENDING  |         |
| <input type="checkbox"/>            | MyNetwork_30003 | 30003      | MyVRF_50004 |                     |                     | DEPLOYED |         |
| <input type="checkbox"/>            | MyNetwork_30004 | 30004      | MyVRF_50005 |                     |                     | NA       |         |
| <input type="checkbox"/>            | MyNetwork_30006 | 30006      | MyVRF_50006 |                     |                     | NA       |         |
| <input type="checkbox"/>            | MyNetwork_30007 | 30007      | MyVRF_50007 |                     |                     | DEPLOYED |         |
| <input type="checkbox"/>            | MyNetwork_30008 | 30008      | MyVRF_50008 |                     |                     | NA       |         |
| <input type="checkbox"/>            | MyNetwork_30009 | 30009      | MyVRF_50000 |                     |                     | NA       |         |
| <input checked="" type="checkbox"/> | MyNetwork_30011 | 30011      | MyVRF_50000 |                     |                     | NA       |         |

**Step 9** Repeat the procedure to add relevant networks.

**Step 10** To continue the fabric provisioning process, select the corresponding check boxes next to the network names to add them to specific devices (or add and extend the networks, in case of external fabrics) and click **Continue** (on the top right part of the screen). You can select a maximum of 10 networks on this screen to proceed for network deployment.

## Deploying the Network

### Before You Begin

You can deploy the network after creating or selecting a network.

### Procedure

**Step 1** After you select a fabric, you need to select one or more networks. Based on the fabric settings, network definitions will be available.

Fabric Selection > Network Selection > Network Deployment > VRF View Continue

Fabric Selected: site1

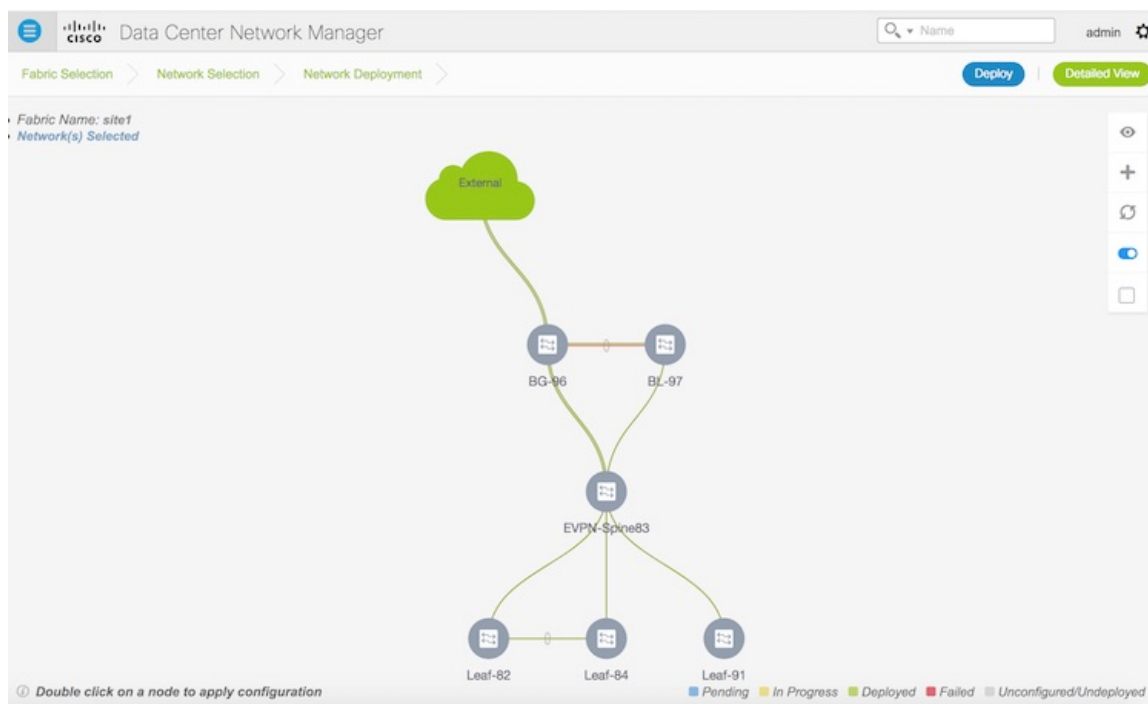
Networks Selected 1 / Total 9

|                                     | Network Name    | Network ID | VRF Name    | IPv4 Gateway/Subnet | IPv6 Gateway/Prefix | Status   | VLAN ID |
|-------------------------------------|-----------------|------------|-------------|---------------------|---------------------|----------|---------|
| <input type="checkbox"/>            | MyNetwork_30001 | 30001      | MyVRF_50001 |                     |                     | DEPLOYED |         |
| <input type="checkbox"/>            | MyNetwork_30002 | 30002      | MyVRF_50003 |                     |                     | PENDING  |         |
| <input type="checkbox"/>            | MyNetwork_30003 | 30003      | MyVRF_50004 |                     |                     | DEPLOYED |         |
| <input type="checkbox"/>            | MyNetwork_30004 | 30004      | MyVRF_50005 |                     |                     | NA       |         |
| <input type="checkbox"/>            | MyNetwork_30006 | 30006      | MyVRF_50006 |                     |                     | NA       |         |
| <input type="checkbox"/>            | MyNetwork_30007 | 30007      | MyVRF_50007 |                     |                     | DEPLOYED |         |
| <input type="checkbox"/>            | MyNetwork_30008 | 30008      | MyVRF_50008 |                     |                     | NA       |         |
| <input type="checkbox"/>            | MyNetwork_30009 | 30009      | MyVRF_50000 |                     |                     | NA       |         |
| <input checked="" type="checkbox"/> | MyNetwork_30011 | 30011      | MyVRF_50000 |                     |                     | NA       |         |

**Step 2** Click **Continue** (on the top right part of the screen) to start deploying the network. If you also want to deploy other undeployed networks, select the appropriate check boxes and then click **Continue**.

**Note** You can deploy one or more networks at any point in time (and not just immediately after creating a network) from the Networks page.

The Network Deployment page (Topology View) appears



There are two views available:

- Detailed View.
- Topology View (default view). This view enables you to click on a node to apply configuration.

In the Topology View, for an existing fabric that already has the devices, DCNM displays the topology for the devices in the fabric. In this page, you can perform the following tasks using the options' panel at the right part of the screen:

- Preview Configuration (eye icon)—Displays the configuration that will be deployed to the device. This only displays data for deployments that are in Pending state. If configurations on a switch are pending, then the switch icon will be blue colored.
- Refresh (refresh icon)—Refreshes the page view.
- Auto Refresh (slide icon)—Click the button to enable/disable automatic refreshing of the page.
- Multi select (check box)—Select the checkbox to deploy multiple networks or VRF instances simultaneously on selected switches in the topology.
  - To select multiple switches, you can either drag the cursor over the switches or you can use the Ctrl key (command key on a Mac keyboard).



When you select multiple switches, the Switches Deploy screen for networks appears.

## Switches Deploy

*Fabric Name:* site1

MyNetwork\_30004

MyNetwork\_30006

*Deploy Options:**① Select the row and click on the cell to edit**② Please save config for the network before switching tabs*

| <input type="checkbox"/> | Switch  | ▲ | VLAN | Interfaces | Status |
|--------------------------|---------|---|------|------------|--------|
| <input type="checkbox"/> | Leaf-82 |   | 6    | ...        | NA     |
| <input type="checkbox"/> | Leaf-84 |   | 6    | ...        | NA     |

Save

The selected devices should have the same role (Border Leaf, Border Gateway, etc).

- A tab is displayed for each network. Click on the tab and the selected switches appear as separate entries/rows.
- Click the checkbox on the corresponding switch. You can update these entries:

**VLAN** – Click the VLAN value. It becomes editable and a **Save | Cancel** box appears in the center of the table.

| <input type="checkbox"/>            | Switch  | ▲ | VLAN | Interfaces    | Status |
|-------------------------------------|---------|---|------|---------------|--------|
| <input checked="" type="checkbox"/> | Leaf-82 |   | 6    | Ethernet1/1   | NA     |
| <input checked="" type="checkbox"/> | Leaf-84 |   | 6    | Save   Cancel | NA     |

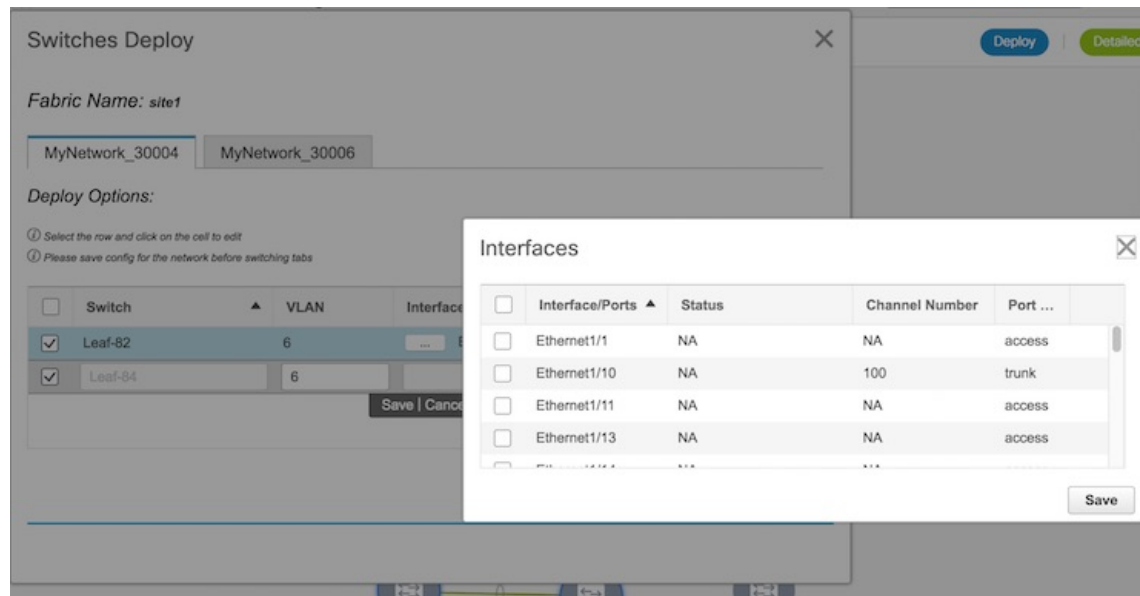
Update the VLAN value and click the Save option.

**Interfaces** – To add interfaces to the selected network, click the ... button in the Interfaces column.

| <input type="checkbox"/>            | Switch  | ▲ | VLAN | Interfaces      |
|-------------------------------------|---------|---|------|-----------------|
| <input checked="" type="checkbox"/> | Leaf-82 |   | 6    | ... Ethernet1/1 |
| <input checked="" type="checkbox"/> | Leaf-84 |   | 6    | ...             |

The available interfaces are displayed in the Interfaces screen





Select the relevant interface checkboxes and click on Save.

Save the added interfaces by clicking on the **Save** button in the **Save | Cancel** box appears in the center of the table.

- Select corresponding tabs to update parameters for other networks.
- Click on the **Save** button at the bottom right part of the Switches Deploy screen to save all network configurations on the selected switches.

**Note** When you select one of a pair of vPC switches, the other automatically gets selected.

The multi select option for deploying networks and for deploying VRF instances contain different fields. The **Interfaces** field is only applicable for network deployment. It has a ... button that should be used to view and add interfaces for deployment.

You cannot zoom in/out the topology view if this option is switched on. Unselect the Multi select checkbox to zoom in/out the topology screen view.

After clicking on Save, the Topology screen appears. The Leaf-82 and Leaf-84 switch icons are displayed in blue color now, indicating a Pending deployment state.

Single switch configuration - To save network configurations onto a single switch, double-click a switch and save configurations in the **Switches Deploy** screen that comes up.

**Step 3** Click on the Preview (eye) icon to preview the configurations. To view network configuration for a specific switch, select the switch and the network from the drop-down boxes at the top of the screen. In this example, the preview displays MyNetwork\_30006 configuration on the Leaf-84 switch.

## Preview Configuration



Select a Switch:

Leaf-84



Select a Network

MyNetwork\_30006



Generated Configuration:

```

configure profile sitel-Default_VRF-50006
vlan 2007
 vn-segment 50006
 interface vlan 2007
 vrf member MyVRF_50006
 ip forward
 ipv6 forward
 no ip redirects
 no ipv6 redirects
 mtu 9192
 no shut

vrf context MyVRF_50006
 vni 50006
 rd auto
 address-family ipv4 unicast
 route-target both auto
 route-target both auto evpn
 address-family ipv6 unicast
 route-target both auto
 route-target both auto evpn
 router bgp 65515
 vrf MyVRF_50006
 address-family ipv4 unicast
 advertise l2vpn evpn
 redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
 maximum-paths ibgp 2
 address-family ipv6 unicast
 advertise l2vpn evpn
 redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
 maximum-paths ibgp 2
 interface nve 1
 member vni 50006 associate-vrf

```

- Step 4** *Deployment* - After you verify the configurations that are generated from the profiles are correct for the selected switches, click the **Deploy** button to deploy the configuration. DCNM will SSH to the switches and deploy the configuration. Then, DCNM shows the deployment status with the topology by highlighting the switches with different colors. You can also select the switch and view the deployment status details.
- Step 5** The other view from which you can deploy configurations is the Detailed View. Click the **Detailed View** button (on the top right part of the screen) to see a tabular form, which has similar functions as the Topology view.

Fabric Name: site1 Network(s) Selected Selected 0 / Total 10

Deploy Preview History Show All

| <input type="checkbox"/> | Name            | Switch  | Ports | Status               |
|--------------------------|-----------------|---------|-------|----------------------|
| <input type="checkbox"/> | MyNetwork_30001 | BG-96   |       | UNDEPLOYED           |
| <input type="checkbox"/> | MyNetwork_30001 | Leaf-82 |       | REDEPLOYMENT PENDING |
| <input type="checkbox"/> | MyNetwork_30001 | Leaf-84 |       | REDEPLOYMENT PENDING |
| <input type="checkbox"/> | MyNetwork_30001 | Leaf-91 |       | REDEPLOYMENT PENDING |
| <input type="checkbox"/> | MyNetwork_30002 | BG-96   |       | UNDEPLOYED           |
| <input type="checkbox"/> | MyNetwork_30002 | Leaf-82 |       | PENDING              |
| <input type="checkbox"/> | MyNetwork_30002 | Leaf-84 |       | PENDING              |
| <input type="checkbox"/> | MyNetwork_30002 | Leaf-91 |       | PENDING              |
| <input type="checkbox"/> | MyNetwork_30003 | Leaf-82 |       | DEPLOYED             |
| <input type="checkbox"/> | MyNetwork_30003 | Leaf-84 |       | DEPLOYED             |

You can perform the following tasks using the button options on the top left part of the table:

- **Preview**—If switches are pending for deployment, click the preview button so that DCNM displays all the configuration yet to be deployed to all the devices.
- **Deploy**—Deploys the configuration to the devices. You can simultaneously deploy multiple networks (or VRF instances) by clicking the Deploy button.
- **History**—Shows the deployment history for the selected network. Click the underlined status to know more deployment details.

#### Network History

Select a Switch: BG-96

| Network Name    | VRF Name    | Ports | Status            | Time of Execution     |
|-----------------|-------------|-------|-------------------|-----------------------|
| NA              | MyVRF_50003 | NA    | <u>UNDEPLOYED</u> | 12/1/2017, 7:37:39 AM |
| MyNetwork_30002 | MyVRF_50003 |       | <u>UNDEPLOYED</u> | 12/1/2017, 7:37:31 AM |
| NA              | MyVRF_50001 | NA    | <u>UNDEPLOYED</u> | 12/1/2017, 7:37:22 AM |
| MyNetwork_30001 | MyVRF_50001 |       | <u>UNDEPLOYED</u> | 12/1/2017, 7:37:13 AM |
| MyNetwork_30002 | MyVRF_50003 |       | <u>DEPLOYED</u>   | 12/1/2017, 7:36:46 AM |
| NA              | MyVRF_50003 | NA    | <u>DEPLOYED</u>   | 12/1/2017, 7:36:35 AM |
| MyNetwork_30001 | MyVRF_50001 |       | <u>DEPLOYED</u>   | 12/1/2017, 7:35:32 AM |
| NA              | MyVRF_50001 | NA    | <u>DEPLOYED</u>   | 12/1/2017, 7:35:12 AM |

- **Edit**—Allows you to edit the selected configurations of network or VRF based on the selection made in the Network or the VRF listing page.

Click the Topology View button (on the top right part of the page) to switch to the topology view.

Once you initiate the deployment process, DCNM displays the deployment status for all the networks in the fabric. You can select a switch and click the **History** button to view the network deployment history for the selected switch.

If the role of the device is *border gateway*, then the network has to be extended on that border leaf switch and cannot be instantiated without extension.

## Editing a Network

### Procedure

- Step 1** From Cisco DCNM Web Client, choose **Configure > LAN Fabric Provisioning > Network Deployment**. The LAN Fabric Provisioning page appears.
- Step 2** Click **Continue**. The **Select a Fabric** page that comes up.
- Step 3** Select the appropriate fabric from the drop-down box and click on the Continue button at the top right part of the screen. The **Networks** page comes up.

Fabric Selected: site1

Selected 0 / Total 7

| Network Name    | Network ID | VRF Name    | IPv4 Gateway/Subnet | IPv6 Gateway/Prefix | Status   | VLAN ID |
|-----------------|------------|-------------|---------------------|---------------------|----------|---------|
| MyNetwork_30001 | 30001      | MyVRF_50001 |                     |                     | DEPLOYED |         |
| MyNetwork_30002 | 30002      | MyVRF_50003 |                     |                     | PENDING  |         |
| MyNetwork_30003 | 30003      | MyVRF_50004 |                     |                     | DEPLOYED |         |
| MyNetwork_30004 | 30004      | MyVRF_50005 |                     |                     | NA       |         |
| MyNetwork_30006 | 30006      | MyVRF_50006 |                     |                     | NA       |         |
| MyNetwork_30007 | 30007      | MyVRF_50007 |                     |                     | DEPLOYED |         |
| MyNetwork_30008 | 30008      | MyVRF_50008 |                     |                     | NA       |         |

- Step 4** Select a network. You can only edit one network at a time.  
If you are using the VRF view, you can switch to the Network View by clicking the **Network View** button.
- Step 5** Click the **Edit** button. The **Edit Network** page appears. You can add/update the Network Profile section by selecting the General and Advanced tabs. You cannot modify the Network Information section.

**Edit Network**

**Network Information**

- \* Network ID: 30004
- \* Network Name: MyNetwork\_30004
- \* VRF Name: MyVRF\_50005
- \* Layer 2 Only: ☐
- \* Network Template: Default\_Network
- \* Network Extension Template: Default\_Network\_Extension
- VLAN ID:

**Network Profile**

**General**

- IPv4 Gateway/NetMask:  ? example 192.0.2.1/24
- IPv6 Gateway/Prefix:  ? example 2001:db8::1/64
- Interface Description:  ?

**Save** **Cancel**

**Step 6** After updating information, click **Save**.

Note that updating a network is not allowed while the network is being deployed. Also, the Save option will only be successful if any values are changed. In this example, the IPv4 gateway address has been updated and displayed in the Networks page.

Networks Selected 1 / Total 9

Show: All

|                                     | Network Name    | Network ID | VRF Name    | IPv4 Gateway/Subnet | IPv6 Gateway/Prefix | Status     | VLAN ID |
|-------------------------------------|-----------------|------------|-------------|---------------------|---------------------|------------|---------|
| <input type="checkbox"/>            | MyNetwork_30001 | 30001      | MyVRF_50001 |                     |                     | UNDEPLOYED |         |
| <input type="checkbox"/>            | MyNetwork_30002 | 30002      | MyVRF_50003 |                     |                     | PENDING    |         |
| <input type="checkbox"/>            | MyNetwork_30003 | 30003      | MyVRF_50004 |                     |                     | DEPLOYED   |         |
| <input checked="" type="checkbox"/> | MyNetwork_30004 | 30004      | MyVRF_50005 | 192.0.2.1/24        |                     | NA         |         |
| <input type="checkbox"/>            | MyNetwork_30006 | 30006      | MyVRF_50006 |                     |                     | NA         |         |
| <input type="checkbox"/>            | MyNetwork_30007 | 30007      | MyVRF_50007 |                     |                     | DEPLOYED   |         |
| <input type="checkbox"/>            | MyNetwork_30008 | 30008      | MyVRF_50008 |                     |                     | NA         |         |
| <input type="checkbox"/>            | MyNetwork_30009 | 30009      | MyVRF_50000 |                     |                     | NA         |         |
| <input type="checkbox"/>            | MyNetwork_30011 | 30011      | MyVRF_50000 |                     |                     | NA         |         |

## Undeploying a Network

### Before You Begin


**Note**

You can only undeploy networks that are deployed.

### Procedure

- Step 1** From Cisco DCNM Web Client, choose **Configure > LAN Fabric Provisioning > Network Deployment**. The LAN Fabric Provisioning page appears.
- Step 2** Click **Continue**. The **Select a Fabric** page comes up.
- Step 3** Select the appropriate fabric from the drop-down box and click on the **Continue** button at the top right part of the screen. The **Networks** page comes up. You can only undeploy networks whose status is **DEPLOYED**. For example, you can undeploy the networks MyNetwork\_30003 and MyNetwork\_30003.

Fabric Selected: site1

Networks Selected 0 / Total 7

|                          | Network Name    | Network ID | VRF Name    | IPv4 Gateway/Subnet | IPv6 Gateway/Prefix | Status   | VLAN ID |
|--------------------------|-----------------|------------|-------------|---------------------|---------------------|----------|---------|
| <input type="checkbox"/> | MyNetwork_30001 | 30001      | MyVRF_50001 |                     |                     | DEPLOYED |         |
| <input type="checkbox"/> | MyNetwork_30002 | 30002      | MyVRF_50003 |                     |                     | PENDING  |         |
| <input type="checkbox"/> | MyNetwork_30003 | 30003      | MyVRF_50004 |                     |                     | DEPLOYED |         |
| <input type="checkbox"/> | MyNetwork_30004 | 30004      | MyVRF_50005 |                     |                     | NA       |         |
| <input type="checkbox"/> | MyNetwork_30006 | 30006      | MyVRF_50006 |                     |                     | NA       |         |
| <input type="checkbox"/> | MyNetwork_30007 | 30007      | MyVRF_50007 |                     |                     | DEPLOYED |         |
| <input type="checkbox"/> | MyNetwork_30008 | 30008      | MyVRF_50008 |                     |                     | NA       |         |

- Step 4** Select the networks you want to undeploy and click on the **Continue** button, at the top right part of the screen. The Topology screen comes up. This screen displays the fabric, the devices it is comprised of, and the connections between the devices.



Different colors denote different statuses for the selected networks, as noted in the status panel. The deployed devices Leaf-82 and Leaf-84 are displayed in green color because MyNetwork\_30003 and MyNetwork\_30003 are deployed on these devices.

**Note** The color code is subjective to network selection in the Networks page. In the explained example, deployed networks were selected. From the Networks page, if you select a network that is yet to be deployed, or in the process of being deployed (MyNetwork\_30002) and proceed to the Topology screen, then Leaf-82 and Leaf-84 are displayed in blue color, because the network is still in Pending state.

**Step 5** Double-click on the Leaf-82 or Leaf-84 device icon (for the deployed networks). The **Switches Deploy** screen appears.

Switches Deploy

Fabric Name: site1

MyNetwork\_30003

MyNetwork\_30007

Deploy Options:

Select the row and click on the cell to edit

Please save config for the network before switching tabs

| <input type="checkbox"/>            | Switch  | VLAN | Interfaces | Status   |
|-------------------------------------|---------|------|------------|----------|
| <input checked="" type="checkbox"/> | Leaf-82 | 2001 | ...        | DEPLOYED |
| <input checked="" type="checkbox"/> | Leaf-84 | 2001 | ...        | DEPLOYED |

Save

Each tab represents a network that you have chosen to undeploy (from the Networks page). The tab contains a table. Each row in the table represents a switch on which the network has presence.

- Step 6** Unselect the check box in each row, as appropriate and click on the Save button, at the bottom right part of the screen.
- For example, in the **MyNetwork\_30003** tab, if you unselect the Leaf-82 and Leaf-84 check boxes and click on Save, the network will be undeployed from those devices.
- Step 7** Select the other tab and delete the selected network on appropriate switches, as explained above. Leaf-82 and Leaf-84 make up a vPC switch pair. If you click on one of the vPC switches, then the Switches Deploy screen will contain both the vPC switches since the configuration (or removal of configuration) is similar for a pair of vPC switches.
- Step 8** Alternatively, you can click on the **Detailed View** button to undeploy networks. The network-switch combination displayed in the **Switches Deploy** screen appears in a tabular form.

Fabric Name: site1    Network(s) Selected    Selected 0 / Total 4

| <input type="checkbox"/> | Name            | Switch  | Ports | Status   |
|--------------------------|-----------------|---------|-------|----------|
| <input type="checkbox"/> | MyNetwork_30003 | Leaf-82 |       | DEPLOYED |
| <input type="checkbox"/> | MyNetwork_30003 | Leaf-84 |       | DEPLOYED |
| <input type="checkbox"/> | MyNetwork_30007 | Leaf-82 |       | DEPLOYED |
| <input type="checkbox"/> | MyNetwork_30007 | Leaf-84 |       | DEPLOYED |



Select the appropriate network-switch combination and click the **Edit** button. The **Switches Deploy** screen will come up. Undeploy networks as per the process explained in the previous step.

## Deleting a Network

### Before You Begin

You should undeploy a network before deleting it.

### Procedure

- Step 1** From Cisco DCNM Web Client, choose **Configure > LAN Fabric Provisioning > Network Deployment**. The LAN Fabric Provisioning page appears.
- Step 2** Click **Continue**. The **Select a Fabric** page comes up.
- Step 3** Select the appropriate fabric from the drop-down box and click on the **Continue** button at the top right part of the screen. The **Networks** page comes up.

Fabric Selected: site1

Selected 0 / Total 7

|                          | Network Name    | Network ID | VRF Name    | IPv4 Gateway/Subnet | IPv6 Gateway/Prefix | Status   | VLAN ID |
|--------------------------|-----------------|------------|-------------|---------------------|---------------------|----------|---------|
| <input type="checkbox"/> | MyNetwork_30001 | 30001      | MyVRF_50001 |                     |                     | DEPLOYED |         |
| <input type="checkbox"/> | MyNetwork_30002 | 30002      | MyVRF_50003 |                     |                     | PENDING  |         |
| <input type="checkbox"/> | MyNetwork_30003 | 30003      | MyVRF_50004 |                     |                     | DEPLOYED |         |
| <input type="checkbox"/> | MyNetwork_30004 | 30004      | MyVRF_50005 |                     |                     | NA       |         |
| <input type="checkbox"/> | MyNetwork_30006 | 30006      | MyVRF_50006 |                     |                     | NA       |         |
| <input type="checkbox"/> | MyNetwork_30007 | 30007      | MyVRF_50007 |                     |                     | DEPLOYED |         |
| <input type="checkbox"/> | MyNetwork_30008 | 30008      | MyVRF_50008 |                     |                     | NA       |         |

- Step 4** The delete button (X) is disabled by default. Select one or more networks you want to delete (by selecting appropriate check boxes). The delete button will be enabled. Click the delete button, and then click the Yes button that comes up to confirm network deletion.

## Creating a VRF

### Procedure

- Step 1** From Cisco DCNM Web Client, choose **Configure > LAN Fabric Provisioning > Network Deployment**. The LAN Fabric Provisioning page appears.
- Step 2** Click **Continue**. The **Select a Fabric** page comes up.
- Step 3** Select the appropriate fabric from the drop-down box and click on the **Continue** button at the top right part of the screen. The **Networks** page comes up.
- Step 4** Click on the **VRF View** button, at the top right part of the screen. The **VRFs** page comes up.

Fabric Selected: site1

Selected 0 / Total 9

| <input type="checkbox"/> | VRF Name    | VRF ID | Status     |
|--------------------------|-------------|--------|------------|
| <input type="checkbox"/> | MyVRF_50000 | 50000  | UNDEPLOYED |
| <input type="checkbox"/> | MyVRF_50001 | 50001  | DEPLOYED   |
| <input type="checkbox"/> | MyVRF_50002 | 50002  | UNDEPLOYED |
| <input type="checkbox"/> | MyVRF_50003 | 50003  | PENDING    |
| <input type="checkbox"/> | MyVRF_50004 | 50004  | DEPLOYED   |
| <input type="checkbox"/> | MyVRF_50005 | 50005  | NA         |
| <input type="checkbox"/> | MyVRF_50006 | 50006  | NA         |
| <input type="checkbox"/> | MyVRF_50007 | 50007  | DEPLOYED   |
| <input type="checkbox"/> | MyVRF_50008 | 50008  | NA         |

This contains a list of VRF instances created for the *site1* fabric.

**Note** You can also create a VRF while creating a new network (See Creating a Network section).

- Step 5** Click the Create VRF (+) button. The **Create VRF** screen appears. The following fields are auto-populated.
- VRF ID—This is the Layer 3 VNI.
  - VRF Name—The VRF name should not contain any white spaces or special characters except underscore (\_), hyphen (-), and colon (:).
  - VRF Template—Two templates, Default\_VRF and Default\_VRF\_asn, are available.
  - VRF Extension Template—Two templates are available for a network extension use case, Default\_VRF\_Extension and Default\_VRF\_Extension\_asn.
- Step 6** Click the **Create VRF** button. The VRF instance is added and an entry appears in the VRFs page, at the bottom.
- Step 7** Repeat the procedure to add relevant VRF instances.

## What to Do Next

Similar to deploying networks, you can deploy VRF instances after creating them, by selecting check boxes next to corresponding VRF instances and then associating them with specific devices. You can select a maximum of 10 VRF instances on this screen to proceed for deployment.

## Deploying VRF Instances

When you create a VRF in the **VRFs** page, it gets added to the list of VRFs at the bottom of the page (MyVRF\_50011 in this example). Also, the check box next to the newly created VRF is automatically selected for deployment.

Fabric Selection > Network Selection > Network Deployment > Network View Continue

Fabric Selected: site1

VRFs Selected 1 / Total 11 Show All

| <input type="checkbox"/>            | VRF Name    | VRF ID | Status     |
|-------------------------------------|-------------|--------|------------|
| <input type="checkbox"/>            | MyVRF_50000 | 50000  | UNDEPLOYED |
| <input type="checkbox"/>            | MyVRF_50001 | 50001  | DEPLOYED   |
| <input type="checkbox"/>            | MyVRF_50002 | 50002  | UNDEPLOYED |
| <input type="checkbox"/>            | MyVRF_50003 | 50003  | PENDING    |
| <input type="checkbox"/>            | MyVRF_50004 | 50004  | DEPLOYED   |
| <input type="checkbox"/>            | MyVRF_50005 | 50005  | NA         |
| <input type="checkbox"/>            | MyVRF_50006 | 50006  | NA         |
| <input type="checkbox"/>            | MyVRF_50007 | 50007  | DEPLOYED   |
| <input type="checkbox"/>            | MyVRF_50008 | 50008  | NA         |
| <input type="checkbox"/>            | MyVRF_50010 | 50010  | NA         |
| <input checked="" type="checkbox"/> | MyVRF_50011 | 50011  | NA         |

## Procedure

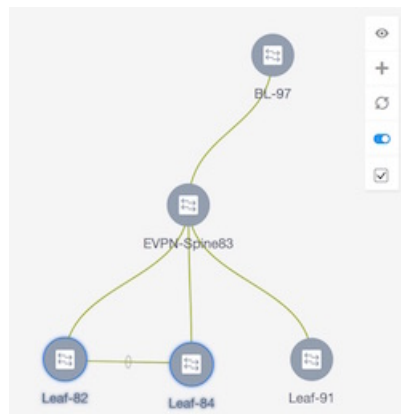
- Step 1** Click **Continue** (on the top right part of the screen) to start deploying the VRF. If you also want to deploy other undeployed VRF instances, select the appropriate check boxes and then click **Continue**. You can deploy one or more VRF instances at any point in time (and not just immediately after creating a VRF) from the **VRFs** page. After clicking **Continue**, the VRF Deployment page (Topology View) appears. There are two views available:



- Detailed View.
- Topology View (default view). This view enables you to click on a node to apply configuration. In the Topology View, for an existing fabric that already has the devices, DCNM displays the topology for the devices in the fabric.

**Step 2** In the topology view, you can perform the following tasks using the options' panel at the right part of the screen:

- Preview Configuration (eye icon)—Displays the configuration that will be deployed to the device. This only displays data for deployments that are in Pending state. If configurations on a switch are pending, then the switch icon will be blue colored.
  - Refresh (refresh icon)—Refreshes the page view.
  - Auto Refresh (slide icon)—Click the button to enable or disable automatic refreshing of the page.
  - Multi select (checkbox icon)—Select the checkbox to deploy multiple VRF instances simultaneously on selected switches in the topology.
- 1 To select multiple switches, you can either drag the cursor over the switches or you can use the Ctrl key (command key on a Mac keyboard).



When you select multiple switches (Leaf-82 and Leaf-84 icons are highlighted in the example), the **Switches Deploy** screen for VRFs appears.

Switches Deploy

Fabric Name: site1

MyVRF\_50005

MyVRF\_50006

Deploy Options:

Select the row and click on the cell to edit

Please save config for the vrf before switching tabs

| <input type="checkbox"/> | Switch  | VLAN | Status |
|--------------------------|---------|------|--------|
| <input type="checkbox"/> | Leaf-82 | 2006 | NA     |
| <input type="checkbox"/> | Leaf-84 | 2006 | NA     |

Save

**Note** The selected devices should have the same role (Border Leaf, Border Gateway, etc).

- A tab is displayed for each VRF instance. Click on the tab and the selected switches appear as separate entries/rows.
- Click the checkbox on the corresponding switches.
- Click other tabs for deploying other VRF instances.
- Click the **Save** button at the bottom right part of the Switches Deploy screen to save all VRF configurations on the selected switches.
  - When you select one of a pair of vPC switches, the other automatically gets selected.
  - The multi select option for deploying networks and for deploying VRF instances contain different fields. The **Interfaces** field is only applicable for network deployment.
  - You cannot zoom in/out the topology view if this option is switched on. Unselect the Multi select checkbox to zoom in/out the topology screen view.

**Note** After clicking on Save, the Topology screen appears. The Leaf-82 and Leaf-84 switch icons are displayed in blue color now, indicating a *Pending* deployment state.

- Single switch configuration - To save VRF configurations onto a single switch, double-click a switch and save configurations in the **Switches Deploy** screen that comes up.
- Preview – Click on the Preview (*eye*) icon to preview the configurations. To view the VRF configuration for a specific switch, select the switch and the VRF instance from the drop-down boxes at the top of the screen. In this example, the preview displays MyVRF\_50005 configuration on the Leaf-84 switch.



- Deployment - After you verify the configurations that are generated from the profiles are correct for the selected switches, click the **Deploy** button to deploy the configuration. DCNM will SSH to the switches and deploy the configuration. Then, DCNM shows the deployment status with the topology by highlighting the switches with different colors. You can also select the switch and view the deployment status details.

**Detailed View** - Apart from topology view, the other view from which you can deploy configurations is the Detailed View. Click the **Detailed View** button (on the top right part of the topology screen) to see a tabular form, which has similar functions as the Topology view.

| Fabric Name: site1                                                                                |             | VRF(s) Selected |       | Selected 0 / Total 4 |  |
|---------------------------------------------------------------------------------------------------|-------------|-----------------|-------|----------------------|--|
| <input type="checkbox"/> Deploy <input type="checkbox"/> Preview <input type="checkbox"/> History |             | Show            |       | All                  |  |
| <input type="checkbox"/>                                                                          | Name        | Switch          | Ports | Status               |  |
| <input type="checkbox"/>                                                                          | MyVRF_50005 | Leaf-82         |       | PENDING              |  |
| <input type="checkbox"/>                                                                          | MyVRF_50005 | Leaf-84         |       | PENDING              |  |
| <input type="checkbox"/>                                                                          | MyVRF_50006 | Leaf-82         |       | PENDING              |  |
| <input type="checkbox"/>                                                                          | MyVRF_50006 | Leaf-84         |       | PENDING              |  |

**Step 3** You can perform the following tasks using the button options on the top left part of the table:

- **Preview**—If switches are pending for deployment, click the preview button so that DCNM displays all the configuration yet to be deployed to all the devices (colored in blue in the topology view, for pending deployment).
- **Deploy**—Deploys the configuration to the devices. You can simultaneously deploy multiple VRF instances by clicking the Deploy button.
- **History**—Shows the deployment history for the selected VRF. You can click the Status to know more deployment details.

VRF History

Select a Switch: Leaf-91

| VRF Name    | Ports | Status     | Time of Execution      |
|-------------|-------|------------|------------------------|
| MyVRF_50001 | NA    | DEPLOYED   | 12/13/2017, 7:15:16 AM |
| MyVRF_50003 | NA    | UNDEPLOYED | 12/1/2017, 6:18:01 AM  |
| MyVRF_50001 | NA    | UNDEPLOYED | 12/1/2017, 6:16:19 AM  |
| MyVRF_50003 | NA    | DEPLOYED   | 12/1/2017, 6:11:12 AM  |
| MyVRF_50001 | NA    | DEPLOYED   | 12/1/2017, 6:09:03 AM  |
| MyVRF_50002 | NA    | UNDEPLOYED | 12/1/2017, 6:06:42 AM  |
| MyVRF_50001 | NA    | UNDEPLOYED | 12/1/2017, 6:06:28 AM  |
| MyVRF_50002 | NA    | DEPLOYED   | 12/1/2017, 6:03:58 AM  |
| MyVRF_50001 | NA    | DEPLOYED   | 12/1/2017, 6:03:37 AM  |
| MyVRF_50000 | NA    | UNDEPLOYED | 12/1/2017, 6:02:12 AM  |
| MyVRF_50000 | NA    | DEPLOYED   | 12/1/2017, 6:01:39 AM  |
| MyVRF_50000 | NA    | DEPLOYED   | 12/1/2017, 5:59:25 AM  |

- **Edit**—Allows you to edit the selected configurations of network or VRF based on the selection made in the Networks or VRFs page.

Click the **Topology View** button (on the top right part of the page) to switch to the topology view.

- Step 4** Once you initiate the deployment process, DCNM displays the deployment status for all the VRF instances in the fabric. You can select a switch and click the **History** button to view the VRF deployment history for the selected switch.

If the role of the device is *border gateway*, then the VRF has to be extended on that border leaf switch and cannot be instantiated without extension.

## Editing a VRF

### Procedure

- Step 1** From Cisco DCNM Web Client, choose **Configure > LAN Fabric Provisioning > Network Deployment**. The LAN Fabric Provisioning page appears.
- Step 2** Click **Continue**. The **Select a Fabric** page comes up.
- Step 3** Select the appropriate fabric from the drop-down box and click on the **Continue** button at the top right part of the screen. The **Networks** page comes up.
- Step 4** Click on the **VRF View** button to go to the VRFs page.

Fabric Selected: site1

Selected 0 / Total 9

VRFs

| <input type="checkbox"/> | VRF Name    | VRF ID | Status     |
|--------------------------|-------------|--------|------------|
| <input type="checkbox"/> | MyVRF_50000 | 50000  | UNDEPLOYED |
| <input type="checkbox"/> | MyVRF_50001 | 50001  | DEPLOYED   |
| <input type="checkbox"/> | MyVRF_50002 | 50002  | UNDEPLOYED |
| <input type="checkbox"/> | MyVRF_50003 | 50003  | PENDING    |
| <input type="checkbox"/> | MyVRF_50004 | 50004  | DEPLOYED   |
| <input type="checkbox"/> | MyVRF_50005 | 50005  | NA         |
| <input type="checkbox"/> | MyVRF_50006 | 50006  | NA         |
| <input type="checkbox"/> | MyVRF_50007 | 50007  | DEPLOYED   |
| <input type="checkbox"/> | MyVRF_50008 | 50008  | NA         |

**Step 5** Select a VRF. You can only edit one VRF at a time.

**Step 6** Click the **Edit** button. The **Edit VRF** screen appears. You cannot modify the VRF Information section.

**Step 7** Click **Save** after updating information.  
updating a VRF is not allowed while the VRF is being deployed. Also, the **Save** option will only be successful if any values are changed.

## Undeploying a VRF

### Before You Begin



**Note** You can only undeploy VRF instances that are deployed.

### Procedure

- Step 1** From Cisco DCNM Web Client, choose **Configure > LAN Fabric Provisioning > Network Deployment**. The LAN Fabric Provisioning page appears.
- Step 2** Click **Continue**. The **Select a Fabric** page comes up.
- Step 3** Select the appropriate fabric from the drop-down box and click on the **Continue** button at the top right part of the screen.  
The **Networks** page comes up.
- Step 4** Click the **VRF View** button to see the list of VRF instances.



VRFs

Selected 0 / Total 11

Show All

| <input type="checkbox"/> | VRF Name    | VRF ID | Status     |
|--------------------------|-------------|--------|------------|
| <input type="checkbox"/> | MyVRF_50000 | 50000  | UNDEPLOYED |
| <input type="checkbox"/> | MyVRF_50001 | 50001  | DEPLOYED   |
| <input type="checkbox"/> | MyVRF_50002 | 50002  | UNDEPLOYED |
| <input type="checkbox"/> | MyVRF_50003 | 50003  | PENDING    |
| <input type="checkbox"/> | MyVRF_50004 | 50004  | DEPLOYED   |

You can only undeploy VRF instances whose status is DEPLOYED. For example, you can undeploy MyVRF\_50001 and MyVRF\_50004.

- Step 5** Select the VRFs you want to undeploy and click on the **Continue** button, at the top right part of the screen.
- The Topology screen comes up. This screen displays the fabric, the devices it is comprised of, and the connections between the devices.



Different colors denote different statuses for the selected networks, as noted in the status panel at the bottom part of your screen. The deployed devices Leaf-82 and Leaf-84 are displayed in green color because the selected VRF instances are deployed on these devices.

**Note** The color code is subjective to network selection in the VRFs page. In the explained example, deployed VRF instances were selected. From the VRFs page, if you select a VRF that is yet to be deployed, or in the process of being deployed (MyVRF\_50003) and proceed to the Topology screen, then Leaf-82 and Leaf-84 will be displayed in blue color, because the VRF is still in *Pending* state on these switches.

- Step 6** Double-click on the Leaf-82 or Leaf-84 device icon (for the deployed networks). The **Switches Deploy** screen appears.

## Switches Deploy

Fabric Name: *site1*

MyVRF\_50001

MyVRF\_50004

## Deploy Options:

Select the row and click on the cell to edit

Please save config for the vrf before switching tabs

| <input type="checkbox"/>            | Switch ▲ | VLAN | Status   |
|-------------------------------------|----------|------|----------|
| <input checked="" type="checkbox"/> | Leaf-82  | 2004 | DEPLOYED |
| <input checked="" type="checkbox"/> | Leaf-84  | 2004 | DEPLOYED |

Save

Each tab represents a VRF that you have chosen to undeploy (from the VRFs page). The tab contains a table. Each row in the table represents a switch on which the VRF has presence.

Unselect the check box in each row, as appropriate and click on the Save button, at the bottom right part of the screen. For example, in the MyVRF\_50001 tab, if you unselect the Leaf-82 and Leaf-84 check boxes and click on Save, the VRF instance will be undeployed from those devices.

Select the other tab and delete the selected VRF on appropriate switches, as explained above.

**Note** Leaf-82 and Leaf-84 make up a vPC switch pair. If you click on one of the vPC switches, then the Switches Deploy screen will contain both the vPC switches since the configuration (or removal of configuration) is similar for a pair of vPC switches.

Alternatively, you can click on the **Detailed View** button to undeploy networks. The network-switch combination displayed in the **Switches Deploy** screen appears in a tabular form.

Fabric Name: *site1* VRF(s) Selected Selected 0 / Total 7

|                          | Deploy      | Preview | History | Show       | All |  |
|--------------------------|-------------|---------|---------|------------|-----|--|
| <input type="checkbox"/> | Name        | Switch  | Ports   | Status     |     |  |
| <input type="checkbox"/> | MyVRF_50001 | BG-96   |         | UNDEPLOYED |     |  |
| <input type="checkbox"/> | MyVRF_50001 | BL-97   |         | UNDEPLOYED |     |  |
| <input type="checkbox"/> | MyVRF_50001 | Leaf-82 |         | DEPLOYED   |     |  |
| <input type="checkbox"/> | MyVRF_50001 | Leaf-84 |         | DEPLOYED   |     |  |
| <input type="checkbox"/> | MyVRF_50001 | Leaf-91 |         | DEPLOYED   |     |  |
| <input type="checkbox"/> | MyVRF_50004 | Leaf-82 |         | DEPLOYED   |     |  |
| <input type="checkbox"/> | MyVRF_50004 | Leaf-84 |         | DEPLOYED   |     |  |

Select the appropriate network-switch combination and click the **Edit** button. The **Switches Deploy** screen comes up. Delete networks as per the process explained in the previous step.

## Deleting a VRF

### Before You Begin

You should undeploy a VRF before deleting it. The VRF must also be undeployed from all devices. You cannot delete a VRF when a device is under a deployment process on the same VRF. Also, a VRF can only be deleted after all the networks that use the VRF are deleted.

### Procedure

- 
- Step 1** From Cisco DCNM Web Client, choose **Configure > LAN Fabric Provisioning > Network Deployment**. The LAN Fabric Provisioning page appears.
  - Step 2** Click **Continue**. The **Select a Fabric** page that comes up.
  - Step 3** Select the appropriate fabric from the drop-down box and click on the **Continue** button at the top right part of the screen.  
The **Networks** page comes up.
  - Step 4** Click on the **VRF View** button to see the list of VRFs.
  - Step 5** The delete button (X) is disabled by default. Select one or more VRF instances you want to delete (by selecting appropriate check boxes). The delete button will be enabled.
  - Step 6** Click the delete button and then click the **Yes** button that comes up to confirm network deletion.
- 

## Adding Fabric Extensions

### Before You Begin

On the main topology, the border switches should be set with an appropriate role (e.g. Border Leaf or Border Gateway). The subsequent procedure describes how the inter-fabric connections between the border devices in the selected fabric and the external devices are defined.

### Procedure

- 
- Step 1** From the Cisco DCNM Web Client, choose **Configure > LAN Fabric Provisioning > Network Deployment**. The LAN Fabric Provisioning page appears.  
A new fabric can also be created through **Configure > LAN Fabric Settings > LAN Fabrics**.
  - Step 2** Click **Continue**.  
The **Select a Fabric** page comes up.

# Select a Fabric

Choose a fabric with appropriate switches where you want the Top Down functionality to be enabled or create a new fabric.

SITE\_2


 [Fabric Extension Settings](#)

OR

[+ Create a new fabric](#)

**Step 3** In the **Select a Fabric** page, click **Fabric Extension Settings**. The **Fabric Extension** screen comes up.

Fabric Extension ✕

Inter-Fabric Connect Selected 0 / Total 1 

| Type                                     | Source Fabric | Source Switch | Source Port  | Destination Fa... | Destination Sw... | Destination Port | Configuration               | Status   |
|------------------------------------------|---------------|---------------|--------------|-------------------|-------------------|------------------|-----------------------------|----------|
| <input type="radio"/> MULTISITE_UNDERLAY | site1         | BG-96         | Ethernet1/32 | External          | RS1               | Ethernet1/32     | <a href="#">View Config</a> | DEPLOYED |

The **Inter-Fabric Connections** section lists previously created external connections. Each line represents a physical or logical connection between a border node in the selected fabric and an external device in some other fabric. For each connection, the source fabric, source device, source interface, destination fabric, destination device, and destination interface are listed along with the type of external connectivity. This section will be empty the first time you add an external connection. Two primary types of external connectivity are supported.

- **VRF Lite (VRF\_LITE)** - For each VRF, an external BGP (eBGP) peering session needs to be set up between the border node and the external device. As part of the connection setup, the eBGP peering session is established from the border node in the default VRF along with additional global configuration of route-maps for IPv4/IPv6 cases.
- **EVPN Multi-Site**: This requires setting up the Border Gateway base configuration for enabling the Multi-Site feature and the underlay peering to the external devices (**MULTISITE\_UNDERLAY**). This is followed by establishing overlay peering from the border gateway to appropriate external devices,

either Border Gateways in other fabrics or Route Servers (**MULTISITE\_OVERLAY**). Both the underlay and overlay peering are established over eBGP. Recall that Border Gateways are special devices that allow clear control and data plane segregation from one site to another while allowing for policy enforcement points for any inter-fabric traffic. They allow the same data plane (VXLAN) and control plane (BGP EVPN) to be employed both for inter-fabric and intra-fabric traffic.

**Note** If you extend the fabric through EVPN Multi-Site, you should first create an underlay extension (select **MULTISITE\_UNDERLAY** in the **Extension Type** field) on the border gateway and then create overlay extensions (select **MULTISITE\_OVERLAY** in the **Extension Type** field).

#### Prerequisite configuration for Multi-Site Top Down extension

There are three loopback interfaces configured on the border gateway that must be reachable by fabric internal neighbors as well as fabric external neighbors. The fabric internal neighbors will learn these through the fabric IGP. For fabric external neighbors, these are redistributed into the IPv4 eBGP session. In order to achieve that, the loopback IP addresses must be tagged as shown below:

| Loopback configuration                                                                                                                                            | Description                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>interface loopback0 description RID AND BGP PEERING ip address 10.100.100.21/32 tag 54321 ip router ospf UNDERLAY area 0.0.0.0 ip pim sparse-mode</pre>      | <ul style="list-style-type: none"> <li>• This is the address used for BGP peering with external and internal neighbors.</li> <li>• In this example, OSPF is shown as the fabric underlay routing protocol used for fabric neighbors.</li> <li>• The <b>ip pim sparse-mode</b> setting is needed only for intra-site multicast-based BUM replication.</li> </ul> |
| <pre>interface loopback1 description NVE INTERFACE (PIP VTEP) ip address 10.200.200.21/32 tag 54321 ip router ospf UNDERLAY area 0.0.0.0 ip pim sparse-mode</pre> | This is the interface used for local NVE peer address.                                                                                                                                                                                                                                                                                                          |
| <pre>Interface loopback100 description MULTI-SITE INTERFACE (VIP VTEP) ip address 10.111.111.1/32 tag 54321 ip router ospf UNDERLAY area 0.0.0.0</pre>            | This is the multisite loopback address. This is provisioned as part of TOP DOWN auto-configuration of the underlay/overlay, and only shown here for the sake of completeness. This does not need to be pre-provisioned.                                                                                                                                         |

**Step 4** Click on the **Add** icon to add a new external connection. The **Add Inter-Fabric Connection** screen appears.

**Add Inter-Fabric Connect**

1 Fabric Interconnect → 2 Define Variables → 3 Preview & Deploy

\* Extension Type: VRF\_LITE

\* Base Template: BorderBase\_v1

\* Extension Template: FabricSetup

\* Source Fabric: site1

\* Destination Fabric:

\* Source Device:

\* Source Interface:

\* Destination Device:

\* Destination Interface:

① VRF\_LITE: Set switch role - Border; MULTISITE: Set switch role - Border Gateway

Previous Next Save & Deploy Cancel

**Step 5** Fill up the fields in this page. The Source Fabric field is pre-populated in the **Fabric Interconnect** section. By default, the Extension Type is set to VRF\_LITE. The Base template references the template that contains a one-time configuration pushed to border devices. The Extension template references the setup template that contains the configuration that will be generated and pushed to the border device to setup the corresponding inter-fabric connection. These templates are auto-populated with corresponding pre-packaged default templates based on user selections. The destination fabric that contains the external device peer must be selected. Note that based on the selection of the source device and source interface, the destination information will be auto-populated based on CDP information if available. There is extra validation performed to ensure that the destination external device is indeed part of the destination fabric.

**Step 6** Click **Next** to go to the **Define Variables** section.

The dialog box titled "Add Inter-Fabric Connect" has a close button (X) in the top right corner. It features a progress bar with three steps: "1 Fabric Interconnect", "2 Define Variables" (highlighted with a blue border), and "3 Preview & Deploy". Below the progress bar, there is a section titled "Network Profile" with a dropdown arrow. Under "Network Profile", there is a "General" tab. The "General" tab contains five input fields, each with a red asterisk indicating it is mandatory: "IF\_NAME" (pre-filled with "Ethernet1/1"), "IP\_MASK", "NEIGHBOR\_IP", "NEIGHBOR\_ASN" (pre-filled with "50002"), and "Extension Type" (pre-filled with "VRF\_LITE"). Each input field has a question mark icon to its right. At the bottom of the dialog, there are four buttons: "Previous", "Next", "Save & Deploy", and "Cancel".

Here, the IP address details of the source and destination port are pre populated from the previous step. The template variables are parsed from the templates selected in the previous step and displayed for user input. All mandatory parameters must be entered.

**Step 7** Click **Next** to go to the **Preview and Deploy** section.

### Add Inter-Fabric Connect

1 Fabric Interconnect
→
2 Define Variables
→
3 Preview & Deploy

Switch: BG-96

Generated Configuration:

```

ip prefix-list default-route seq 5 permit 0.0.0.0/0 le 1
ip prefix-list host-route seq 5 permit 0.0.0.0/0 eq 32
route-map EXTCON-RMAP-FILTER deny 10
 match ip address prefix-list default-route
route-map EXTCON-RMAP-FILTER deny 20
 match ip address prefix-list host-route
route-map EXTCON-RMAP-FILTER permit 1000

ipv6 prefix-list default-route-v6 seq 5 permit 0::/0
ipv6 prefix-list host-route-v6 seq 5 permit 0::/0 eq 128
route-map EXTCON-RMAP-FILTER-V6 deny 10
 match ipv6 address prefix-list default-route-v6
route-map EXTCON-RMAP-FILTER-V6 deny 20
 match ip address prefix-list host-route-v6
route-map EXTCON-RMAP-FILTER-V6 permit 1000

```

Previous
Next
Save & Deploy
Cancel

Here, you can preview the configuration that will be deployed to the selected border device. Note that no configuration will be pushed to the external device itself.

**Step 8** Click **Save and Deploy** to complete the task.

This results in the configuration getting pushed to the appropriate border node. The external connection will appear in the Fabric Extension screen.

Fabric Extension

Inter-Fabric Connect

Selected 0 / Total 2

| Type                                     | Source Fa... | Sour... | Source Port  | Destination Fa... | Destination Sw... | Destination Port | Configur...                 | Status            |
|------------------------------------------|--------------|---------|--------------|-------------------|-------------------|------------------|-----------------------------|-------------------|
| <input type="radio"/> MULTISITE_UNDERLAY | site1        | BG-96   | Ethernet1/32 | External          | RS1               | Ethernet1/32     | <a href="#">View Config</a> | DEPLOYED          |
| <input type="radio"/> VRF_LITE           | site1        | BG-96   | Ethernet1/1  | External          | N9K-9348GC-F...   | Ethernet1/1      | <a href="#">View Config</a> | DEPLOYMENT PEN... |

The view doesn't auto-refresh, hence the refresh button on the top right needs to be clicked to trigger refresh. You can check the status of the deployment (Pending, Deployed, Failed etc.) in the **Status** column. In case of FAILED or UNDEPLOYMENT FAILED status, use the hyperlink in the **Status** column to check the error messages for failure.

**Step 9** For additional inter-fabric connections, a similar set of steps is repeated. Note however, the base configuration to the border node is only pushed once, when the first inter-fabric connection is deployed for a given type. The connections can either be added or deleted, they cannot be updated/edited. On successful deployment of the inter-fabric connections, in the LAN Fabric provisioning topology view, each inter-fabric connection will be displayed as an edge (solid for physical or dotted for logical) between the appropriate border node and the



external fabric. Note that individual devices in the external fabric are not shown and only a fabric/cloud icon with the fabric name is displayed.



## Viewing the Status of the LAN Fabric Provisioning

Cisco DCNM allows you to view the status of the LAN Fabric Provisioning and also to view which VLANs have been used on the devices within a scope.

- 1 You can view the status through **Configure > LAN Fabric Provisioning > Status**.
  - The **Status** column displays the status of the provisioning (Failed, Pending, or NA).
  - The **VLAN Visibility** button (on the top left part of the table) opens the VLAN Visibility screen. It displays the used and unused VLAN ID details for each switch. Select a switch from the list of switches to view corresponding VLAN details for the switch.
- 2 To view which VLANs have been used on the devices within a scope, use **Configure > LAN Fabric Provisioning > Resource**.

## Migrating Cisco NFM Overlay Networks to Cisco DCNM

Cisco Nexus Fabric Manager (NFM) provides a simple point-and-click approach to build and manage both the underlay spine-leaf topology and the VXLAN overlay. Since it is fully fabric aware, it understands how the fabric should operate and can autonomously configure and maintain fabric health throughout its lifecycle. You can migrate your existing Cisco NFM deployments to Cisco DCNM to gain additional capabilities.

## Prerequisites

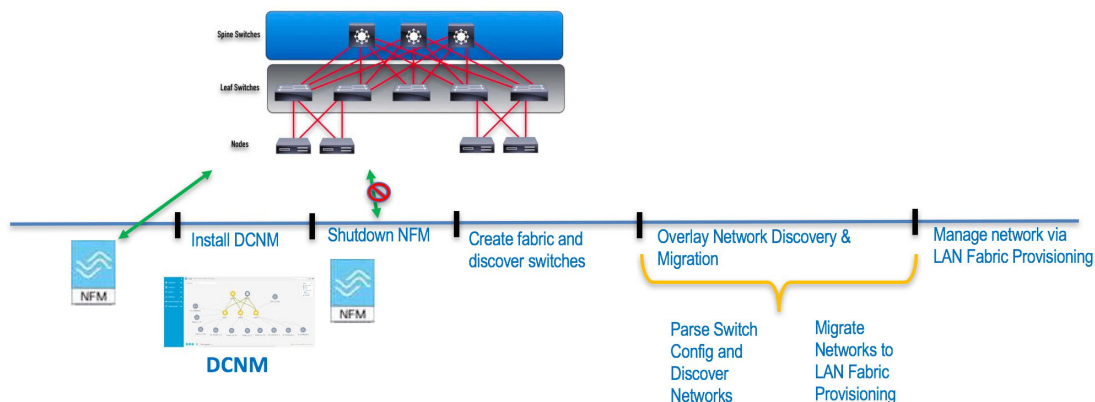
- Install Cisco DCNM if you have not done so already. For more information about installing Cisco DCNM, see the [Cisco DCNM Installation Guide](#).
- The NFM-managed switch nodes should be in steady and stable condition (for example, there should be no configuration updates in progress or further changes from NFM)
- Cisco DCNM 10.4(2) enables you to migrate Cisco NFM Overlay Networks to Cisco DCNM using a migration wizard. During the migration process, you need to disable Cisco NFM so that it does not overwrite the new configuration profiles and settings deployed by Cisco DCNM.
- No configuration changes must be made to the switches while migration is in progress.
- You must upgrade the switch software to Cisco NX-OS version 7.0(3)I5(2) or later. For more information, see [LAN Fabric Provisioning](#).
- We recommend that you take a backup of the switch configurations and save them before the migration. These configurations can be used to restore the network if required.

## Guidelines and Limitations

- Cisco DCNM 10.4(2) supports only one migration to be active at a time.
- Cisco NFM to Cisco DCNM Migration is supported for Cisco Nexus 9000 switches only.
- When an overlay network that was deployed by NFM is migrated to DCNM, only the default templates “Default\_Network” and “Default\_VRF” are supported while creating the overlay network and VRF within DCNM.

## Migration Workflow for Overlay Network

Cisco DCNM 10.4(2) provides a migration assistant to read and migrate the NFM-generated configurations of a switch into the LAN Fabric Provisioning functions of Cisco DCNM.



Using the migration assistant, you can perform the following steps to migrate from Cisco NFM to Cisco DCNM:

## Procedure

- Step 1** Ensure that all the prerequisites have been met and Cisco DCNM is ready.
- Step 2** Install or upgrade Cisco DCNM to version 10.4(2).
- Step 3** Add your switch user credentials from the **Configure > Credentials Management > LAN Credentials**.
- Step 4** Shut down the Cisco NFM server to prevent NFM from undoing changes made by Cisco DCNM. From this point forward you do not use NFM for administering the switches.
- Step 5** Create a new LAN Fabric in Cisco DCNM or use an existing LAN Fabric that have matching settings listed below.

a) Choose **Configure > LAN Fabric Provisioning > Network Deployment > Create a new fabric**.

- 1 Select Replication mode as “Ingress Replication”
- 2 Enter the Fabric Autonomous System Number (ASN) from the NFM fabric

**Create Fabric**

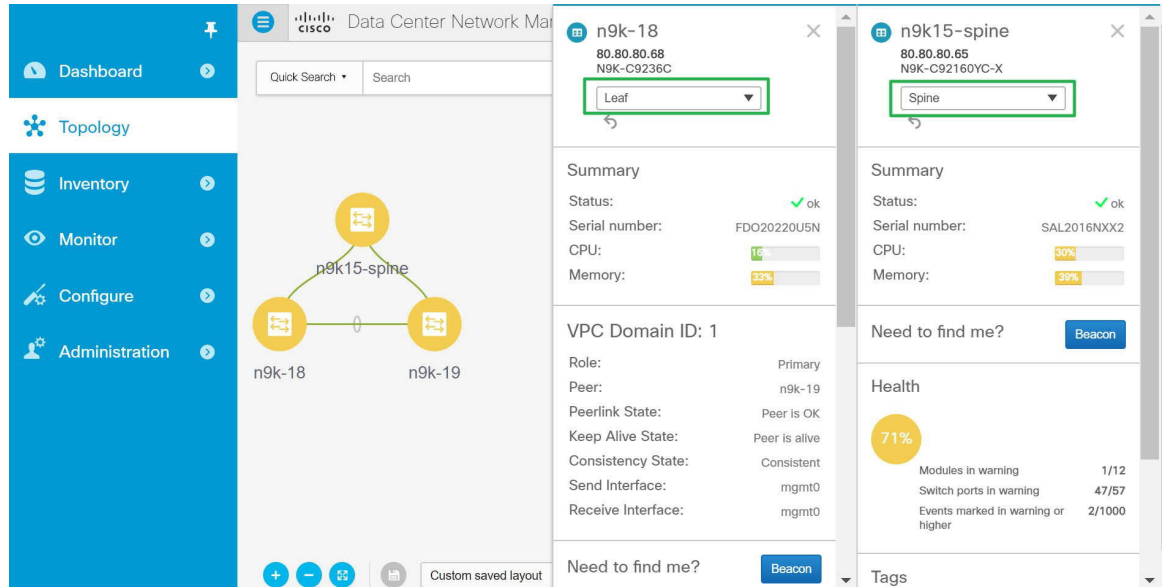
▼ General Settings

- \* **Fabric Name** nfmFabric
- Description
- \* **Fabric Provision Mode** DCNMTopDown
- \* **Fabric Encapsulation** VXLANFabric
- \* **Allowed Leaf Switches** n9k
- \* **Replication Mode** IngressReplication
- \* **VRF Template** Default\_VRF
- \* **Network Template** Default\_Network
- \* **Fabric Autonomous System Number (ASN)** 65535
- \* **Network Extension Template** Default\_Network\_Extension
- \* **VRF Extension Template** Default\_VRF\_Extension
- Site ID

**Create Fabric**

b) Choose **Inventory > Discover > LAN Switches** to discover existing switches and add them to the new LAN Fabric.

- c) Set the role of the switches to Leaf or Spine as appropriate. To do so, access the Topology Display and for each switch double-click the switch-icon to show the pop-out and select the Role as Leaf or Spine.



- Step 6** Run the Cisco DCNM NFM Migration from **Configure > LAN Fabric Provisioning > Migration** menu.. This re-entrant function will automatically create equivalent overlay network entries in the Cisco DCNM **Configuration > LAN Fabric Provisioning > Network Deployment** entries and remove the NFM-generated CLI to migrate the switch to the DCNM mode of operation. For more information about using the Migration wizard, see the [Using the Migration Wizard, on page 241](#) section.
- Step 7** Once the migration is complete (all networks are migrated), the Overlay networks can be managed from **Configuration > LAN Fabric Provisioning > Network Deployment**.

## Migration Workflow Status Definitions

The following table describes the various states for the discovery or migration workflow.

### Discovery-related Status Definitions:

| Status                    | Definition                                                           |
|---------------------------|----------------------------------------------------------------------|
| DISCOVERY INITIATED       | A discovery has been triggered and waiting to start                  |
| DISCOVERY IN PROGRESS     | The discovery is active                                              |
| DISCOVERY FAILED          | The previous discovery failed                                        |
| DISCOVERY ABORT INITIATED | An attempt to abort or cancel an active discovery has been initiated |
| DISCOVERY ABORTED         | The previous discovery has been aborted                              |

| Status              | Definition                                    |
|---------------------|-----------------------------------------------|
| DISCOVERY COMPLETED | The discovery has been completed successfully |

**Migration-related Status Definitions:**

| Status                     | Definition                                                           |
|----------------------------|----------------------------------------------------------------------|
| MIGRATION INITIATED        | Migration has been initiated for a set of network(s)                 |
| MIGRATION IN PROGRESS      | Migration is in progress for a set of network(s)                     |
| MIGRATION FAILED           | The previous migration failed                                        |
| MIGRATION ABORT INITIATED- | An attempt to abort or cancel an active migration has been initiated |
| MIGRATION ABORTED          | Migration has been aborted                                           |
| MIGRATION PENDING          | There are more networks waiting to be migrated                       |
| MIGRATION COMPLETED        | All the networks have been migrated                                  |

**Network Migration Status Definitions**

The following table describes the various states of the network migration workflow:

| Status                                    | Definition                                                     |
|-------------------------------------------|----------------------------------------------------------------|
| DISCOVERED                                | The network has been discovered from the switch configurations |
| SWITCH MIGRATION PREPARATION IN PROGRESS  | The switch where the network is present is being prepared      |
| SWITCH MIGRATION PREPARATION FAILED       | The switch preparation step failed                             |
| NETWORK MIGRATION PREPARATION IN PROGRESS | The L3 network is being prepared for migration                 |
| NETWORK MIGRATION PREPARATION FAILED      | The L3 network preparation step failed                         |
| NETWORK CREATION IN PROGRESS              | The LAN Fabric Provisioning Network entry is being created     |
| NETWORK CREATION FAILED                   | The LAN Fabric Provisioning Network entry creation failed      |
| NETWORK DEPLOYMENT IN PROGRESS            | The LAN Fabric Provisioning Network deployment is in progress  |

| Status                                             | Definition                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NETWORK DEPLOYMENT FAILED                          | The LAN Fabric Provisioning Network deployment failed                                                                                                                                                                                                                                                                    |
| ORIGINAL CONFIGURATION REMOVAL PENDING             | The LAN Fabric Provisioning Network deployment is successful and waiting to remove the original NFM configured CLIs                                                                                                                                                                                                      |
| ORIGINAL CONFIGURATION REMOVAL IN PROGRESS         | The removal of the original NFM configured CLIs is in progress                                                                                                                                                                                                                                                           |
| ORIGINAL CONFIGURATION REMOVAL RECOVERABLE FAILURE | The removal of the original NFM configured CLIs failed, but, can be retried on a future attempt after fixing any underlying issues                                                                                                                                                                                       |
| ORIGINAL CONFIGURATION REMOVAL FAILED              | The removal of the original NFM configured CLIs failed. The failure reason must be reviewed and manual corrective action must be taken. Please review the nature of the failure(s). If some of the configuration CLIs were partially applied, please reapply the failed and rest of the CLIs manually on the switch(es). |
| COMPLETED                                          | The network was migrated successfully                                                                                                                                                                                                                                                                                    |

#### Network Migration History Definitions:

A network migration history will contain the following items and can be used to review detailed information.

| Status                        | Definition                                                                                                                                                                               |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch Migration Preparation  | Provides status of preparing the switch for the migration. This action is performed only once per switch, but, will show up in all network histories                                     |
| Network Migration Preparation | Provides status of the network migration preparations. This entry will be present for L3 network only                                                                                    |
| Deploy Network                | Provides status of the LAN Fabric Network provisioning                                                                                                                                   |
| Unapply Manual Configurations | Provides status of removing the network overlay CLIs configured by NFM. Note: This does not lead to any loss of configuration since LAN Fabric Provisioning uses configuration profiles. |

## Using the Migration Wizard

The Migration wizard will help you migrate over the NFM Overlay networks (or “broadcast domains” as known in the NFM). The migration has two phases—“Discovery” and “Migration”. The Discovery phase is where the configurations that are on the switches are parsed and presented in the GUI for review. The networks, interfaces, and switches where the networks exist is shown to the user. Once you verify the information to be accurate, you can move to the Migration phase by selecting the network(s) that need to be migrated and then proceeding to deploy those networks. The GUI workflow tracks the status of the migrations for audit purposes. The migration is considered completed when all the networks are migrated.

**Note**

It is important that the discovered networks and data are verified before a migration is attempted. Once the first network is migrated (Migration Phase) it is not possible to go back to the Discovery Phase to make changes.

Cisco NFM supports single fabric, whereas Cisco DCNM supports multiple fabrics, so the original NFM-deployed fabric becomes one fabric among all the Cisco DCNM-managed fabrics.

**Note**

It is important that no configuration or network changes are made to the switches until the migration is completed. Any out-of-band configuration changes can interfere with the migrations and can cause significant network issues.

The migration consists two steps:

- Preparing the switch for migration to DCNM Top-Down managed networks.
- Removing the original configuration that existed on the switch prior to the deployment

**Note**

The migration status will be presented to you for review.

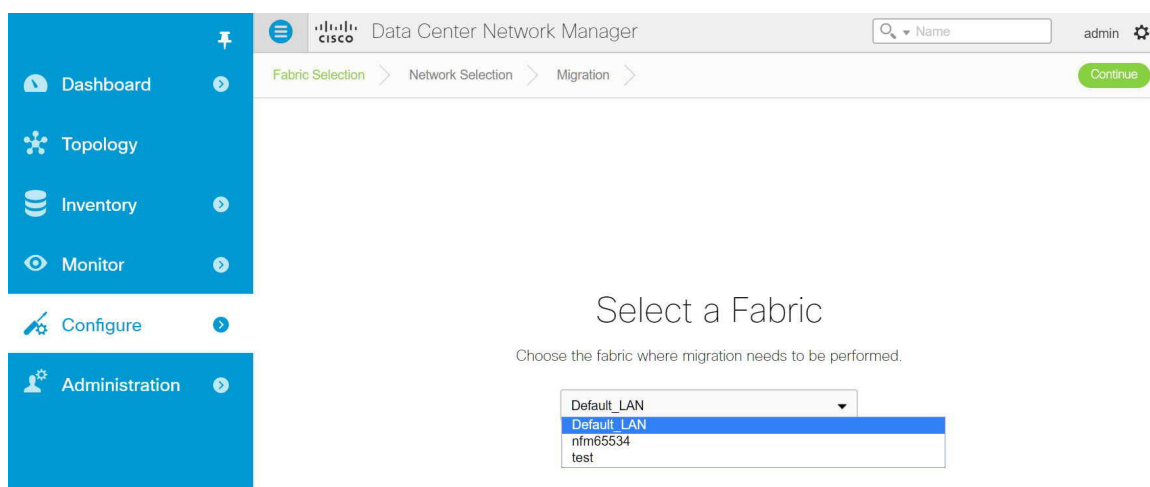
To use the Migration wizard perform the following steps:

### Procedure

- Step 1** Launch Cisco DCNM Web Client.
- Step 2** From the menu bar, choose **Configure > LAN Fabric Provisioning > Migration**.
- Step 3** Select the fabric that have the NFM fabric switches, and then click **Continue**.
  - a) After the discovery phase is complete, review the list of networks and ensure its accuracy.
  - b) Make necessary changes if required, and then click **Rediscover** to restart the discovery process again.The discovery process auto-generates the network name of the form as Auto\_Net\_VLANxxx\_VNIyyyyy . Cisco DCNM will retrieve the running configuration from the switch(es), parse the configurations to discover the VXLAN overlay data. At this point, the migration is considered to be in progress. The parsing occurs in the background and the page refreshed with the discovered networks. One cannot proceed further till the discovery process is completed. The ‘Continue’ button and check boxes will be disabled while discovery is in progress.

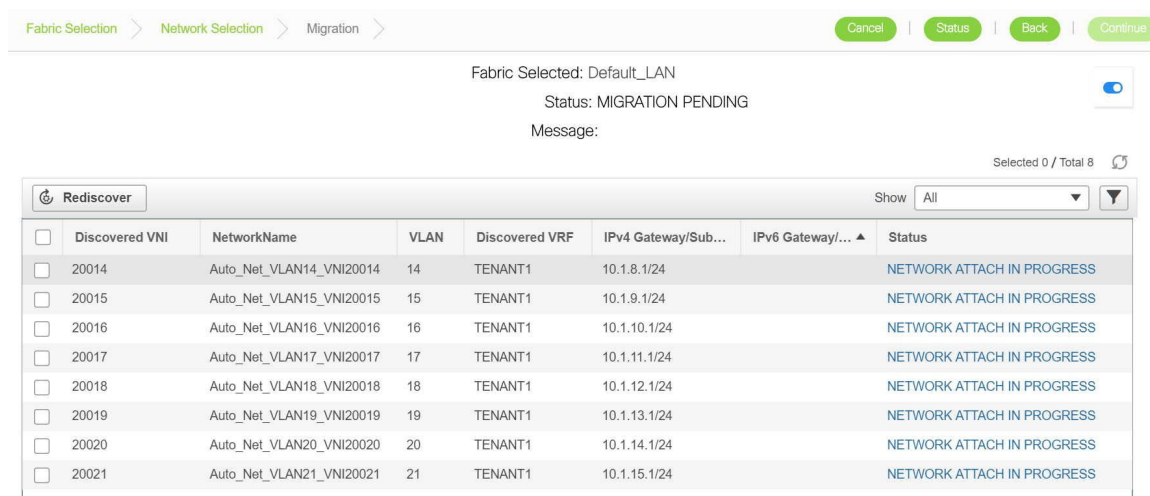
The discovered networks are persisted till one of the following event occurs:

- Migration is completed (network is deployed and the original configuration CLIs are removed).
- Until you click the **Rediscover** button upon which the current list is discarded and configuration is parsed again. The Rediscover button will throw an error once the migration status is changed to MIGRATION IN PROGRESS. The only time a Rediscovery can be performed is when the status is DISCOVERY COMPLETED. The other states where the Rediscover can be triggered are DISCOVERY FAILED and DISCOVERY ABORTED.
- Until you cancel the migration.



**Step 4** Select the network(s) that you wish to migrate by clicking the **Continue** button. The Network Selection page displays the following buttons:

- Cancel—Click the **Cancel** button to abort the discovery process that is in progress.
- Status—Click the **Status** button to the spreadsheet view.
- Continue—This button will be enabled only when you select one or more switches.



**Step 5** Select the network(s) that need to be migrated and click the **Continue** button.



The following page that appears has some additional options that allow you to perform the following functions:

- Preview the configurations on the switch and configurations that are going to be deployed to switch.

The screenshot shows the 'Migration' tab in the Cisco DCNM web client. At the top, it says 'Fabric Selected: Default\_LAN' and 'Status: MIGRATION PENDING'. Below this is a table with columns: Switch Na..., IP Address, Serial No, and Preview. Two switches are listed: n9k-18 (80.80.80.68, FDO20220U5N) and n9k-19 (80.80.80.69, FDO20220U77). A 'Preview Configuration' window is open, showing the configuration for the selected switch. It displays the configuration on the switch and the configurations to be deployed.

| Switch Na...                               | IP Address  | Serial No   | Preview |
|--------------------------------------------|-------------|-------------|---------|
| <input checked="" type="checkbox"/> n9k-18 | 80.80.80.68 | FDO20220U5N |         |
| <input checked="" type="checkbox"/> n9k-19 | 80.80.80.69 | FDO20220U77 |         |

**Preview Configuration**

Configurations on Switch:

```

#####
Network:Auto_Net_VLAN14_VNI20014
#####
vlan 3964
 vn-segment 16777213
 interface Vlan3964
 no shutdown
 vrf member TENANT1
 no ip redirects
 ip forward
 ipv6 address use-link-local-only
 no ipv6 redirects
 vrf context TENANT1
 vni 16777213
 rd auto

```

Configurations to be Deployed:

```

#####
Network:Auto_Net_VLAN14_VNI20014
#####
interface vlan 14
 ip address 10.1.8.1/24 tag 12345
 configure profile Default_LAN-Default_VRF-
 vlan 3964
 vn-segment 16777213
 interface vlan 3964

```

- You can select the switch(es) where the networks needs to be migrated. It is however recommended to select all the switches for the migration. If only a subset of switches is selected, ensure that both the switches in the VPC pair are present.

## Viewing Migration Status

### Procedure

- Step 1** In the Migration page, click the **Status** button. This status page appears when you click the Status button. This reports the cumulative status of all migrations performed so far.

The screenshot shows the 'Migration Status' page. At the top, it says 'Fabric Selected: Default\_LAN' and 'Status: MIGRATION PENDING'. Below this is a table with columns: Network, n9k-18 (FDO20220U5N), and n9k-19 (FDO20220U77). The table lists the status of various networks. The status for most networks is 'COMPLETED', while for others it is 'NETWORK ATTACH IN PROGRESS'.

| Network                  | n9k-18 (FDO20220U5N)       | n9k-19 (FDO20220U77)       |
|--------------------------|----------------------------|----------------------------|
| Auto_Net_VLAN10_VNI20010 | COMPLETED                  | COMPLETED                  |
| Auto_Net_VLAN11_VNI20011 | COMPLETED                  | COMPLETED                  |
| Auto_Net_VLAN12_VNI20012 | COMPLETED                  | COMPLETED                  |
| Auto_Net_VLAN13_VNI20013 | COMPLETED                  | COMPLETED                  |
| Auto_Net_VLAN14_VNI20014 | NETWORK ATTACH IN PROGR... | NETWORK ATTACH IN PROGRESS |
| Auto_Net_VLAN15_VNI20015 | NETWORK ATTACH IN PROGR... | NETWORK ATTACH IN PROGRESS |
| Auto_Net_VLAN16_VNI20016 | NETWORK ATTACH IN PROGR... | NETWORK ATTACH IN PROGRESS |

- Step 2** You can click the hyperlinks to view migration history and status.

## Migration History for Network 'Auto\_Net\_VLAN13\_VNI20013'

| Operation                     | Status   | Time of Execution          |
|-------------------------------|----------|----------------------------|
| Switch Migration Preparation  | SUCCESS  | 2017-12-07 12:43:02.86209  |
| Network Migration Preparation | SUCCESS  | 2017-12-07 12:44:19.80374  |
| Deploy Network                | DEPLOYED | 2017-12-11 01:17:46.973854 |
| Unapply Manual Configurati... | SUCCESS  | 2017-12-11 01:18:13.652946 |

## Troubleshooting Cisco NFM to Cisco DCNM Migration

The Migration workflow involves multiple steps and some unexpected issues that might be encountered while migrating Cisco NFM to Cisco DCNM.

Issues (if any) will be indicated with an appropriate "FAILED" status for the individual network(s) or the entire workflow.



## Network Migration Failures

- 1 Go to the Migration page.
- 2 Identify the network and switch that has encountered the failure and click on the Status hyperlink. The resulting popup will show the status of each migration step.  
Further details can be obtained by clicking the appropriate hyperlinks.  
Additional details can be obtained by reviewing the log files.

## Migration Workflow Failures

The migration status will indicate a FAILURE. Additional details can be obtained by reviewing the log files.

## Detailed Logs

The migration workflow logs are maintained on DCNM. You can review them using this procedure.

- 1 SSH into DCNM
- 2 `cd /usr/local/cisco/dcm/fm/logs`
- 3 `ls -ltr migrate.log*`

Multiple logs files can exist (because of rollover) with the most recent one being 'migrate.log'

Example log file:

```
[root@dcnm84 logs]# pwd
/usr/local/cisco/dcm/fm/logs
[root@dcnm84 logs]# ls -ltr migrate.log*
-rw-r--r-- 1 root root 10485678 Nov 20 22:01 migrate.log.3
-rw-r--r-- 1 root root 10484761 Nov 20 23:36 migrate.log.2
-rw-r--r-- 1 root root 10485721 Nov 21 03:03 migrate.log.1
-rw-r--r-- 1 root root 7414428 Nov 21 05:36 migrate.log
```


**Note**

The logs are for review purpose only. Do not attempt to delete or make changes to them.

Contact Cisco TAC if further assistance is needed.

## LAN Fabric Auto-Configuration

The LAN Fabric Auto-Configuration menu includes the following submenus:

### LAN Fabric Auto-Configuration

This feature automates network provisioning and provides a new layer of automation integration in which the data center fabric-switching infrastructure is automatically provisioned for the physical or virtual workload that is being instantiated.


**Note**

These features appear on your Cisco DCNM Web Client application only if you have deployed the DCNM installer in the Unified Fabric mode.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

| Field/Icons                  | Description                                                     |
|------------------------------|-----------------------------------------------------------------|
| <b>Organizations Section</b> |                                                                 |
| Organization/Partition Name  | Specifies the organization or the partition name.               |
| Description                  | Specifies the description for the organization.                 |
| Partition ID                 | Specifies the partition ID to be associated with the partition. |
| Orchestration Engine         | Specifies the Orchestrator name for the organization.           |
| Service Node IP Address      | Specifies the IP address for the service node for a partition   |

| Field/Icons             |                    | Description                                                          |
|-------------------------|--------------------|----------------------------------------------------------------------|
| Edge Router ID          |                    | Specifies the Edge Router ID.                                        |
| Extension Status        |                    | Specifies if the extension is enabled or disabled.                   |
| Profile                 |                    | Specifies the default profile used.                                  |
| <b>Networks Section</b> |                    |                                                                      |
| Network Name            |                    | Specifies the name to identify the network.                          |
| Partition Name          |                    | Allows you to select the partition to be applied for the network.    |
| Segment ID              |                    | Specifies the segment ID to be used for partition extension.         |
| Mobility Domain         | VLAN ID            | Specifies the VLAN ID for the mobility domain.                       |
|                         | Mobility Domain ID | Allows you to select the mobility domain ID from the drop-down list. |
| Profile Name            |                    | Specifies the default profile used.                                  |
| DHCP Scope              | Subnet             | Specifies the subnet for the network.                                |
|                         | Gateway            | Specifies the gateway for the network.                               |
|                         | IP Range           | Specifies the IP address range available for the network.            |
| Add                     |                    | Allows you to add Organization, Partition, or Network.               |
| Edit                    |                    | Allows you to edit Organization, Partition, or Network.              |
| Delete                  |                    | Allows you to delete Organization, Partition, or Network.            |
| Enable Extension        |                    | Allows you to enable the extension for the selected Organization.    |
| Disable Extension       |                    | Allows you to disable the selected extension.                        |
| Deploy Configuration    |                    | Allows you to deploy the network for the selected partition.         |
| Undeploy Configuration  |                    | Allows you to undeploy the network configuration.                    |
| Refresh                 |                    | Refreshes the list of items in the view.                             |
| Show Filter             |                    | Filters list of items based on the defined value for each column.    |

| Field/Icons | Description                                                                   |
|-------------|-------------------------------------------------------------------------------|
| Print       | Prints the list of Organizations or Networks along with their details.        |
| Export      | Exports the list of items and their details to a Microsoft Excel spreadsheet. |
| Maximize    | Allows you to maximize the view for Organizations or Networks.                |

Fabric provides the following configuration options:

- Organizations
  - [Adding an Organization, on page 248](#)
  - [Editing an Organization, on page 248](#)
  - [Deleting an Organization, on page 248](#)
  - [Adding a Partition, on page 249](#)
  - [Editing a Partition, on page 249](#)
  - [Deleting a Partition, on page 249](#)
- Networks
  - [Adding a Network, on page 250](#)
  - [Editing a Network, on page 251](#)
  - [Deleting a Network, on page 251](#)

## Organizations

You can create profiles from the Cisco DCNM **Web Client > Configure > LAN Fabric Auto-Configuration > Organizations**.

## Adding an Organization

### Procedure

- 
- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > Organizations > Add > Organization**.
  - Step 2** In the Add Organization window, specify the Name and Description of the organization.
  - Step 3** Specify the Orchestration Engine.
  - Step 4** Click **Add**.
- 

## Editing an Organization

### Procedure

- 
- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > Organizations**.
  - Step 2** Select an organization from the List and click the Edit icon.
  - Step 3** In the Edit Organization window, change the configuration.
  - Step 4** Click **Edit** to save the changes.
- 

## Deleting an Organization



---

**Note** You must delete all partitions under an organization before deleting the organization.

---

### Procedure

- 
- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > Organizations**.
  - Step 2** Select an organization from the List and click the **Delete** icon.
  - Step 3** Click **Yes** to confirm.
- 

## Partitions

You can create profiles from the Cisco DCNM Web Client > **Configure > LAN Fabric Auto-Configuration > Partitions**.

## Adding a Partition

### Procedure

- 
- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > Partitions**.
  - Step 2** Specify the Name for the partition.  
Ensure that you have selected an organization from the **Organizations** drop-down list before adding partitions.
  - Step 3** Specify the VRF name and provide description for the partition.
  - Step 4** Specify the Edge Router ID for the partition.  
Select the checkbox if you choose to extend the partition across the fabric. If you do not select the checkbox, this partition will not be extended across the Fabric.
  - Step 5** Specify the DNS Server and the Secondary DNS server for the partition.
  - Step 6** From the drop-down list, select the default Profile Name.  
The values for the Profile Parameters are auto-populated based on the default Profile Name.
  - Step 7** Click **OK** to configure the partition.
- 

## Editing a Partition

### Procedure

- 
- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > Partitions**.
  - Step 2** Click an organization from the List and select the Partition.
  - Step 3** Click the Edit icon
  - Step 4** In the Edit Partition window, change the configuration.
  - Step 5** Click **Edit** to save the changes.
- 

## Deleting a Partition

**Note**

---

You must delete all networks under the partition before deleting the partition.

---

### Procedure

- 
- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > Partitions**.
- Step 2** Click an organization from the List and select the Partition.
- Step 3** Click the **Delete** icon
- Step 4** Click **Yes** to confirm.
- 

## Networks

You can create profiles from the Cisco DCNM Web Client > **Configure > LAN Fabric Auto-Configuration > Networks**.

### Adding a Network

#### Procedure

- 
- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > Networks**.
- Step 2** Specify the VRF Name for the partition.  
**Note** Ensure that you have selected appropriate organization and partition from the respective **Organizations** and **Partitions** drop-down lists before adding a network.  
The VRF Name must be of the format *organizationName.partitionName*.
- Step 3** Specify the Network Name to identify the network.
- Step 4** Specify the Multicast Group Address.  
**Note** The Multicast Group Address is used to Enable VXLAN Encapsulation on the Admin > Fabric Encapsulation Settings page.
- Step 5** Select the Network Role from the drop-down list based on the type of the network.
- Step 6** In the Network ID section, choose one of the following:
- Segment ID Only
    - Specify the **Segment ID** for the network.
  - Mobility Domain and VLAN
    - Specify the **Segment ID** for your network.
    - Select **Generate Seg ID** to generate segment ID automatically.
    - Specify the **VLAN ID** and **Mobility Domain ID** if you need to create a VLAN + Mobility Domain network.



- Step 7** In the DHCP Scope section, specify the **IP Range**.
  - Step 8** Use the drop-down to select the **Profile**.
  - Step 9** Specify the **Profile** parameters.
  - Step 10** Specify the **Service Configuration** parameters.
  - Step 11** Click **Add**.
- 

## Editing a Network

### Procedure

---

- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > Networks**.
  - Step 2** Select a network from the List and click the Edit icon
  - Step 3** In the Edit Partition window, change the configuration.
  - Step 4** Click **Edit** to save the changes.
- 

## Deleting a Network

### Procedure

---

- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > Networks**.
  - Step 2** Select a network from the list and click the Delete icon.
  - Step 3** Click **Yes** to confirm.
- Note** Cisco DCNM will send **clear fabric database host** command to the switches when the network is deleted from Cisco DCNM Web Client.
- 

## Profiles

You can create profiles from the Cisco DCNM **Web Client > Configure > LAN Fabric Auto-Configuration > Profiles**.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

**Table 33: Profiles**

| Field | Description                        |
|-------|------------------------------------|
| Name  | Specifies the name of the profile. |

| Field              | Description                                                          |
|--------------------|----------------------------------------------------------------------|
| Type               | Specifies the type of the profile.                                   |
| Sub Type           | Specifies the sub type of profiles differentiate profile categories. |
| Description        | Displays the description for the profile.                            |
| Forwarding Mode    | Specifies the mode for forwarding.                                   |
| Editable           | Specifies if the profile parameters are editable or not.             |
| Last Modified Time | Displays the last time when the profile was modified.                |

**Table 34: Profile instances**

| Field             | Description                                                     |
|-------------------|-----------------------------------------------------------------|
| Organization Name | Displays the name of the Organization.                          |
| Partition Name    | Displays the name of the partition created in the organization. |
| VRF Name          | Species the VRF name for the profile.                           |
| Segment ID        | Specifies the Segment ID for the profile instance               |
| VLAN ID           | Specifies the VLAN ID for the profile                           |
| Network Name      | Specifies the network name for the profile.                     |

Profiles provide the following configuration options:

- Profiles
  - [Adding a profile, on page 253](#)
  - [Editing a Profile, on page 254](#)
  - [Delete a Profile, on page 254](#)
- Profile Instance
  - [Editing a Profile Instance, on page 254](#)

## Adding a profile

### Procedure

- 
- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > Profiles**.
- Step 2** In the Add Profile window, specify the **Name** and **Description** of the profile.
- Note** A global VLAN is a FabricPath-enabled VLAN which is not mapped to a Segment ID. Before Cisco DCNM 7.2(2), the user-defined Global VLAN profile names must end with “GblVlanProfile” (case-insensitive), for the network to auto-refresh.
- Step 3** Use the drop-down, select the **Type** of the Profile.
- Note** Devices with different platforms may use profiles of different profile types. For this release, **FPVLAN, FPBD, IPVLAN, IPBD** are supported.
- Step 4** From the drop down, select **Sub Type**. Sub Type of profiles differentiate profile categories, such as :
- individual profile
  - universal profile
  - network profile
  - partition profile
  - DCI profile and so on.

The following subtypes are supported:

- network:universal - Universal profile for a network
- network:universal,gblvlan
- network:universal,ir
- network:individual—Individual profile for a network
- partition:universal—Universal profile for a partition
- partition:universal,bl
- partition:universal,er
- partition:universal,pe
- partition:individual—Individual profile for a partition
- bl-er:universal,bl—Universal profile for a Border Leaf
- bl-er:universal,er—Universal profile for a Edge Router
- bl-er:universal,pe
- bl-er:individual,bl
- bl-er:individual,er
- bl-er:individual,pe
- none

- Step 5** Use the drop-down to select the Forwarding Mode. The following values are supported:
- anycast-gateway
  - proxy-gateway
  - none
- Step 6** Enter the Profile Content from collection of CLI commands to discover a specific configuration.
- Step 7** Click **Add**.
- 

## Editing a Profile

### Procedure

- 
- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > Profiles**.
- Step 2** Select a profile from the list and click the Edit icon.
- Step 3** In the Edit profile window, change the configuration.
- Step 4** Click **Edit** to save the changes.
- 

## Delete a Profile

### Procedure

- 
- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > Profiles**.
- Step 2** Select a profile from the list and click the Delete icon.
- Step 3** Click **Yes** to confirm.
- 

## Editing a Profile Instance

### Procedure

- 
- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > Profiles**.
- Step 2** Select a profile from the list and click the Edit icon.
- Step 3** In the Edit Profile Instance window, change the configuration.
- Step 4** Click **Edit** to save the changes.
-

## Border Leaf Device Pairing

This feature allows you to pair Border Leaf with the Edge Router and specify device associated configurations such as interface between Border Leaf and Edge Router. DCNM selects appropriate Border Leaf/Edge Router pairs during partition (VRF) extension.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

| Field                       | Description                                                                                                                                       |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Edge Router/Border Leaf     | Specifies the Name of the Edge Router or the connected Border Leaf.                                                                               |
| IP Address                  | Specifies the IP address of the Border Leaf/Edge Router.                                                                                          |
| Interface Name/Port Channel | Specify the interface name or port channel between Border Leaf and Edge Router.                                                                   |
| Profile Name                | Specifies the default profile name.                                                                                                               |
| Type                        | Specifies if the device is an Edge Router configuration or a Border Leaf configuration.                                                           |
| Partition Utilization       | Specifies the partitions utilized and the maximum partitions available for the device.                                                            |
| Add                         | Allows you to add a Border Leaf/Edge Router. For more information, see <a href="#">Creating an Edge Router</a> , on page 256.                     |
| Edit                        | Allows you to edit a Border Leaf/Edge Router.                                                                                                     |
| Delete                      | Allows you to delete a Border Leaf/Edge Router. For more information, see <a href="#">Deleting Edge Router/Border leaf devices</a> , on page 257. |
| View Profile                | Allows you to view the profile created                                                                                                            |
| Refresh                     | Refreshes the list of switches.                                                                                                                   |
| Show Filter                 | Filters list of switches based on the defined value for each column.                                                                              |
| Print                       | Prints the list of devices and their details.                                                                                                     |
| Export                      | Exports the list of devices and their details to a Microsoft Excel spreadsheet.                                                                   |

## Creating an Edge Router

### Procedure

---

- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > Border Leaf Pairing**.
- Step 2** Click **Add**. Select Edge Router.
- Step 3** To configure the Edge Router, perform the following steps.
- On the Add Edge Router screen, select a Device from the drop-down list.
  - In the **IP Address** field, enter the IP address of the device.
  - In the Maximum Number of Partitions, enter an appropriate number for the Partitions required for the Edge Router.
  - Select Notify Edge Router when relevant partitions are changed to notify the Edge Router.
  - Click **OK** to add an edge router.
- Step 4** To configure a Border PE, perform the following steps
- On the Add Border PE screen, select a device from the **Device Name** drop-down list.
  - Specify the IP Address for the Edge Router.
  - Specify the Maximum Number of Partitions required for the Edge Router.
  - Select Notify Edge Router when relevant partitions are changed to notify the Edge Router.
  - Define the Profile Parameters.
    - asn—specifies the autonomous system (AS) number for the Border PE
    - vrfSegmentId—specifies the VRF segment ID.
    - rsvdGlobalAsn—specifies the reserved global autonomous system number.
    - dcId—specifies the Edge Router ID for the Border PE
    - vrfName—Specifies the vrf name
- Note** The value for vrfName must be of the format 'organizationName:partitionName'.
- Step 5** Click OK to save the configuration.
- 

## Connect New Border leaf to the Edge Router

### Procedure

---

- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > Border Leaf Pairing**.
- Step 2** Click **Add**. Select Border Leaf.
- Step 3** Define the parameters for the Border leaf configuration and edge router configuration for pairing.

| Field                                       | Description                                                                       |
|---------------------------------------------|-----------------------------------------------------------------------------------|
| Name                                        | Select the name from the drop-down list for the Border leaf.                      |
| IP Address                                  | The IP address is auto-populated based on the selected Border Leaf.               |
| Port Channel or the Interface Name          | Specify the interface name or port channel between Border Leaf and Edge Router.   |
| Maximum Number of Partitions                | Specifies the number of partitions required for the configuration                 |
| Default Profile Name                        | Select the default profile name from the drop-down list to apply for the profile. |
| Notify Border Leaf when relevant partitions | Select to notify the Border Leaf when relevant partitions are created.            |

**Step 4** Click **OK** to connect the new border leaf device to the Edge router.

## Deleting Edge Router/Border leaf devices

### Procedure

- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > Border Leaf Pairing**.
- Step 2** Select the Edge Router/Border leaf device definitions from the list and click **Delete**.
- Step 3** Click **Yes** to confirm and delete the profile.

## Extended Partitions

This screen lists the extended partitions, selected Border Leaf/Edge Router pairs, and their corresponding profiles and configurations. From the menu bar, select **Configure > LAN Fabric Auto-Configuration > Extended Partitions**.

The following icons are listed at the menu bar of the window to customize the view of the information in the window:

| Field | Description                                        |
|-------|----------------------------------------------------|
| VRF   | Specifies the VRF name for the extended partition. |

| Field                  | Description                                                                 |
|------------------------|-----------------------------------------------------------------------------|
| Organization           | Specifies the name of organization which the extended partition belongs to. |
| Partition              | Specifies the name of the partition that is extended.                       |
| Redundancy Factor      | Specifies the run-time redundancy factor for that partition extension.      |
| Edge Router            | Specifies the name of the Edge Router.                                      |
| Edge Router IP Address | Specifies the IP address of the Edge Router device.                         |
| Edge Router Profile    | Specifies the default profile for the edge router.                          |
| Border Leaf (BL)       | Specifies the name of the Border Leaf device                                |
| BL IP Address          | Specifies the IP address of the Border Leaf device.                         |
| BL Profile             | Specifies the default profile for the border leaf device.                   |

## End Hosts

Cisco DCNM provides repository for end host MAC address to segment ID mapping, which can be used for end hosts such as auto-configuration of the bare-metal server.

The following table describes the fields that appear on **Configure > LAN Fabric Auto-Configuration > End Host**.

| Field                | Description                                                                                                                                                         |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| End Host ID          | Specifies the ID for this end host.<br>The value is a MAC address if End Host Type is <b>MAC Address</b> .                                                          |
| End Host Type        | Specifies the type for this end host.<br>The default type is MAC Address.                                                                                           |
| End Host Name        | Specifies a name for this end host.                                                                                                                                 |
| Connection Port Mode | Select the connection port mode from the drop down list.<br>The options available are: <ul style="list-style-type: none"> <li>• Native</li> <li>• Tagged</li> </ul> |



| Field      | Description                                 |
|------------|---------------------------------------------|
| Segment ID | Specifies the segment ID for this end host. |

This section contains the following:

## Adding End Hosts

Perform the following task to add end hosts.

### Procedure

- 
- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > End Host**.
  - Step 2** Click **Add** icon.
  - Step 3** In the Add End Host window, specify the required parameters.
  - Step 4** Click **OK** to add the End Host.
- 

## Editing End Hosts

Perform the following task to edit end hosts.

### Procedure

- 
- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > End Host**.
  - Step 2** Click **Edit** icon.
  - Step 3** In the Edit End Host window, update the required parameters.
  - Step 4** Click **OK** to save your changes.
- 

## Deleting End Hosts

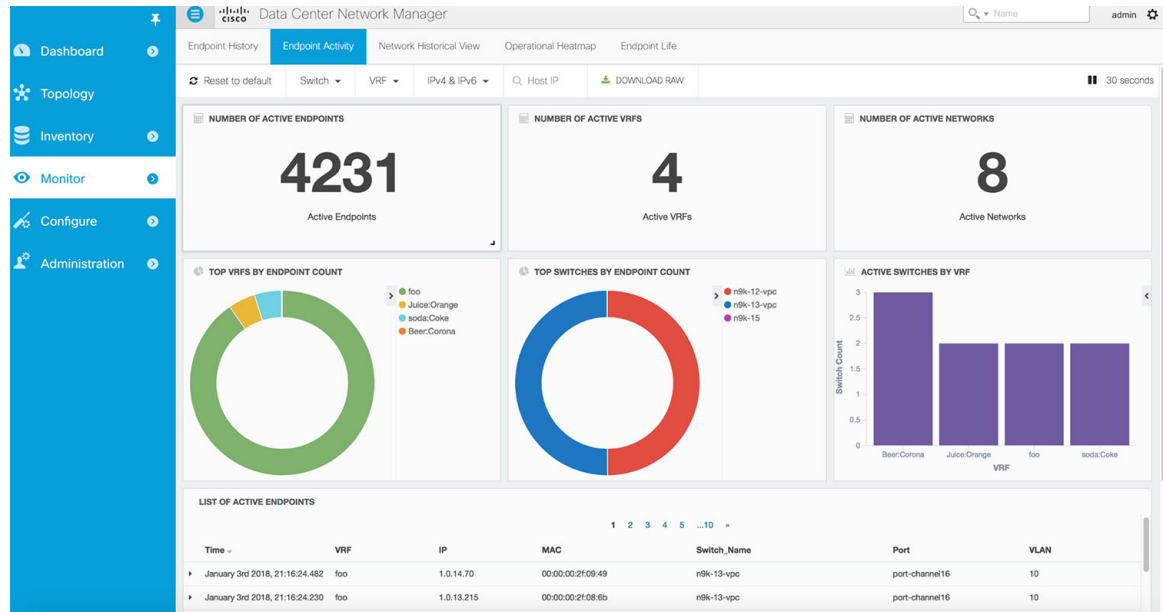
Perform the following task to delete end hosts.

### Procedure

- 
- Step 1** From the menu bar, select **Configure > LAN Fabric Auto-Configuration > End Host**.
  - Step 2** Select the End Host ID you want to delete, and click **Delete** icon.
  - Step 3** Click **OK** to confirm and delete the End Host.
-

# Endpoint Locator

The Endpoint Locator (EPL) feature allows real-time tracking of endpoints within a data center. This includes tracing the network life history of an endpoint as well as getting insights into the trends associated with endpoint additions, removals, moves etc. An endpoint is anything with a IP and MAC address. In that sense, an endpoint can be a virtual machine (VM), container, bare-metal server, service appliance etc.



## Note

**Endpoint Locator is currently only supported for VXLAN BGP EVPN fabric deployments and DFA (BGP L3VPN) based fabric deployments. It is not supported for access aggregation based deployments.**

EPL relies on BGP updates to track endpoint information. Hence, the DCNM needs to peer with the BGP Route-Reflector (RR) to get these updates. For this purpose, IP reachability from the DCNM to the RR is required.

Some key highlights of the Endpoint Locator are:

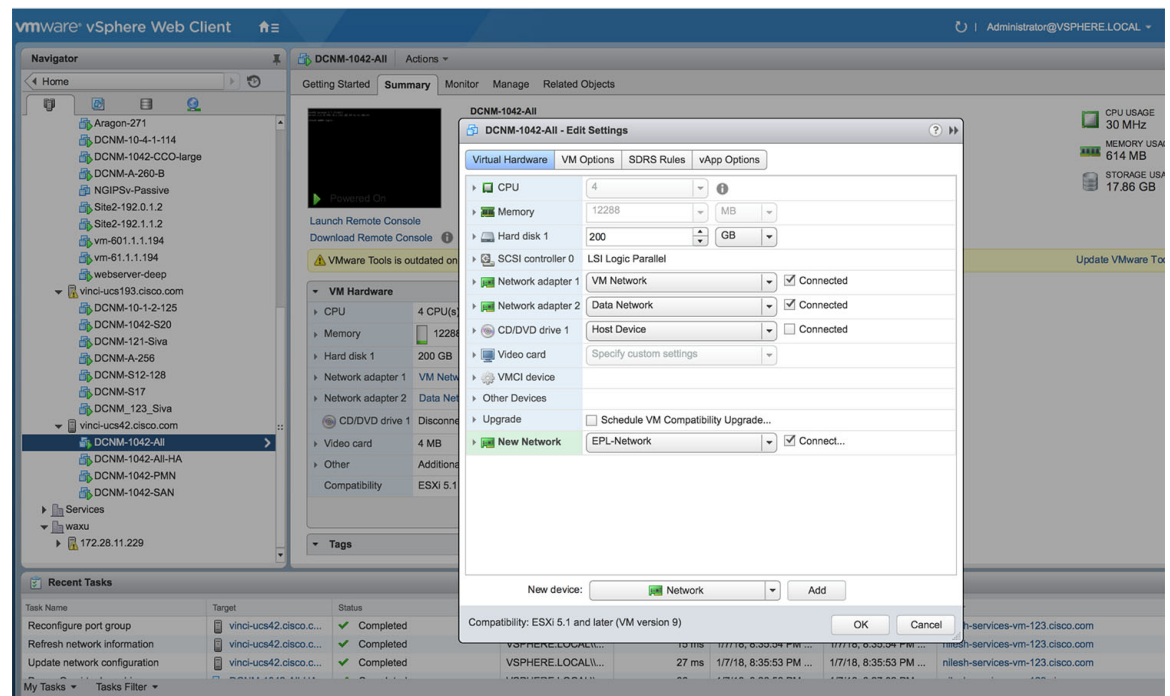
- Support for dual-homed and dual-stacked (IPv4 + IPv6) endpoints
- Support for up to 2 BGP route reflectors
- Support for real-time and historical dashboards for insights such as endpoint lifetime, network, endpoint, VRF daily views, and operational heat map
- Support for high availability
- Support for endpoint data stored for up to 180 days, amounting to a maximum of 5 G storage space
- Support for optional flush of the endpoint data to start afresh
- Supported scale: 10K endpoints

For more information about EPL, refer to the following sections:

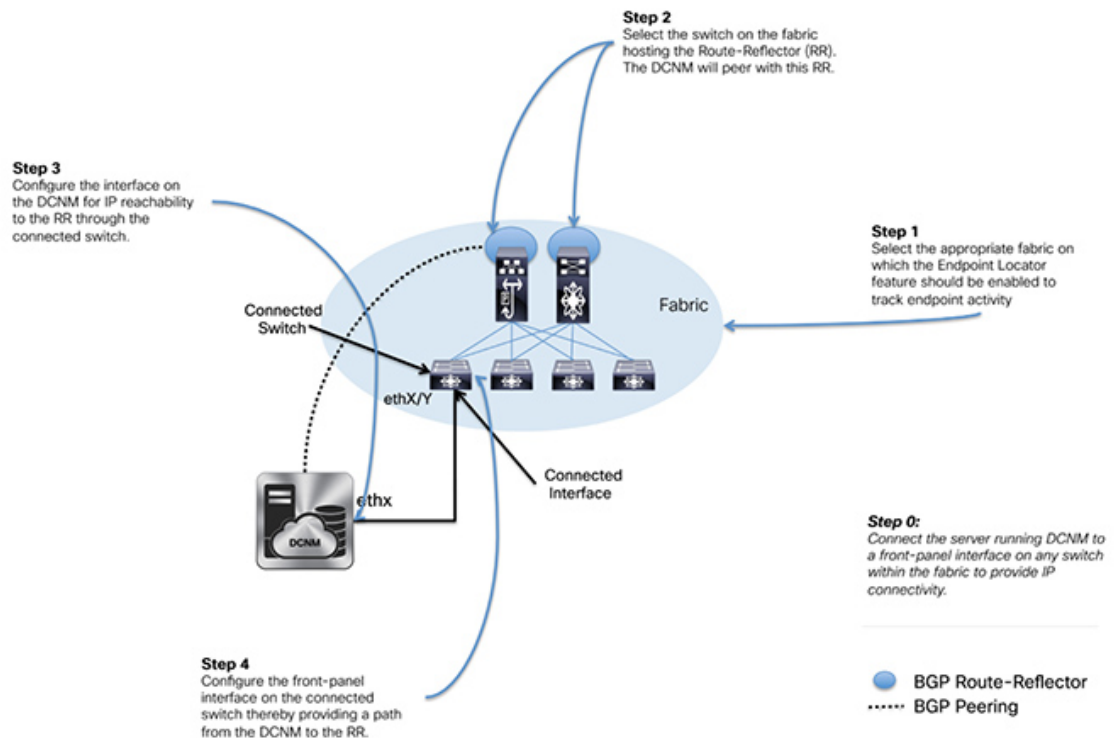
## Configuring Endpoint Locator

With the DCNM OVA or ISO form factor, the default installation occurs with 2 interfaces—eth0 interface for external access to the DCNM and eth1 interface that is used primarily for fabric management. In most deployments, the eth1 interface is part of the same network on which the mgmt0 interfaces of the Nexus switches reside (Out-of-band or OOB network). This allows DCNM to perform out-of-band management of these devices including POAP.

For EPL, BGP peering from the DCNM to the BGP Route-Reflector is required. Since the BGP process on Nexus devices typically runs on the non-management VRF, specifically default VRF, there is a requirement to have in-band IP connectivity from the DCNM to the fabric. For this purpose, a third interface, ethx, is required. This is a pre-requisite for enabling the EPL feature. For the OVA deployment, addition of a new interface does not require a restart of the DCNM VM. Once the vnic is added to the DCNM VM, the corresponding veth interface gets created and shows up in the VM as the appropriate *ethx* interface.



Once in-band connectivity is established between server (physical or virtual) on which DCNM is running and the fabric, BGP peering can be established. There is a simple 4-step wizard for enabling EPL. The 4 steps are highlighted below:

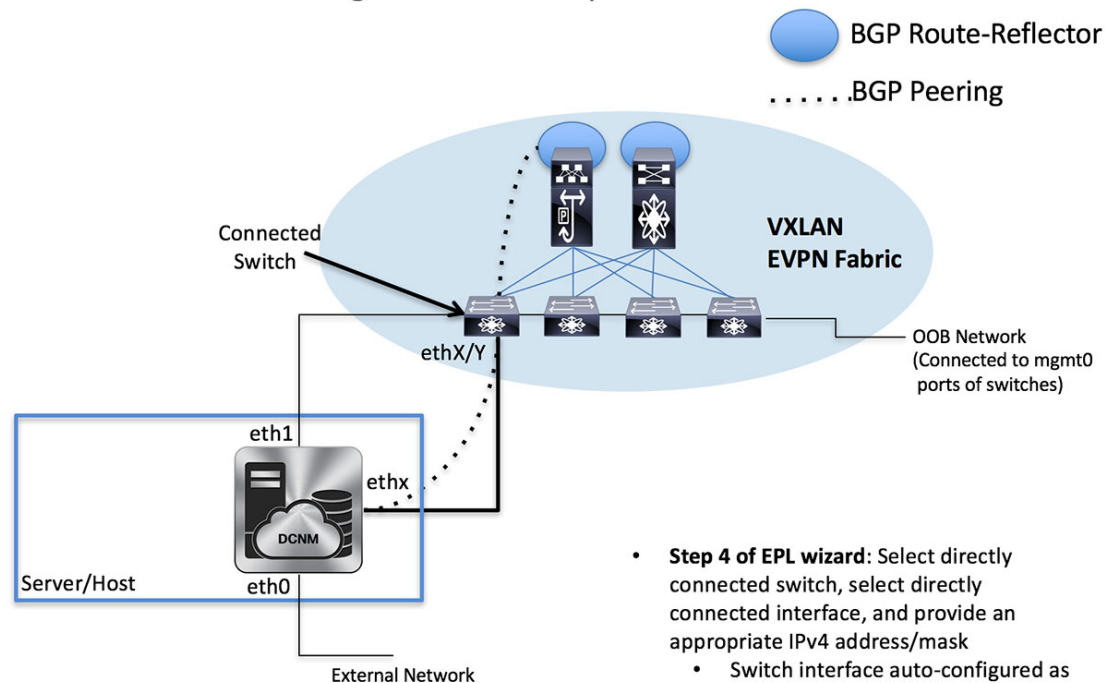


There are 2 sub-modes for configuring EPL which differ in how the network fabric will be configured to do BGP peering from the RR to the DCNM. These specifically differ in the options selected and entered in step 4. These sub-modes are:

- Fully-automated**—In this option, as the name suggests, all the configuration on the network fabric and the DCNM is done as part of EPL enablement. Here, the assumption is that the server on which DCNM is running is directly attached to a ToR/leaf that in turn provides reachability to the RR. In this option, when EPL is enabled, the interface on the ToR/leaf is automatically configured as a routed interface and the corresponding subnet prefix reachability is redistributed into the fabric via the appropriately configured IGP within the fabric. In addition, the RR(s) are configured to accept DCNM as a BGP peer for distributing endpoint information.

## Option 1: Fully Automated

The Server Hosting DCNM is directly connected to a leaf

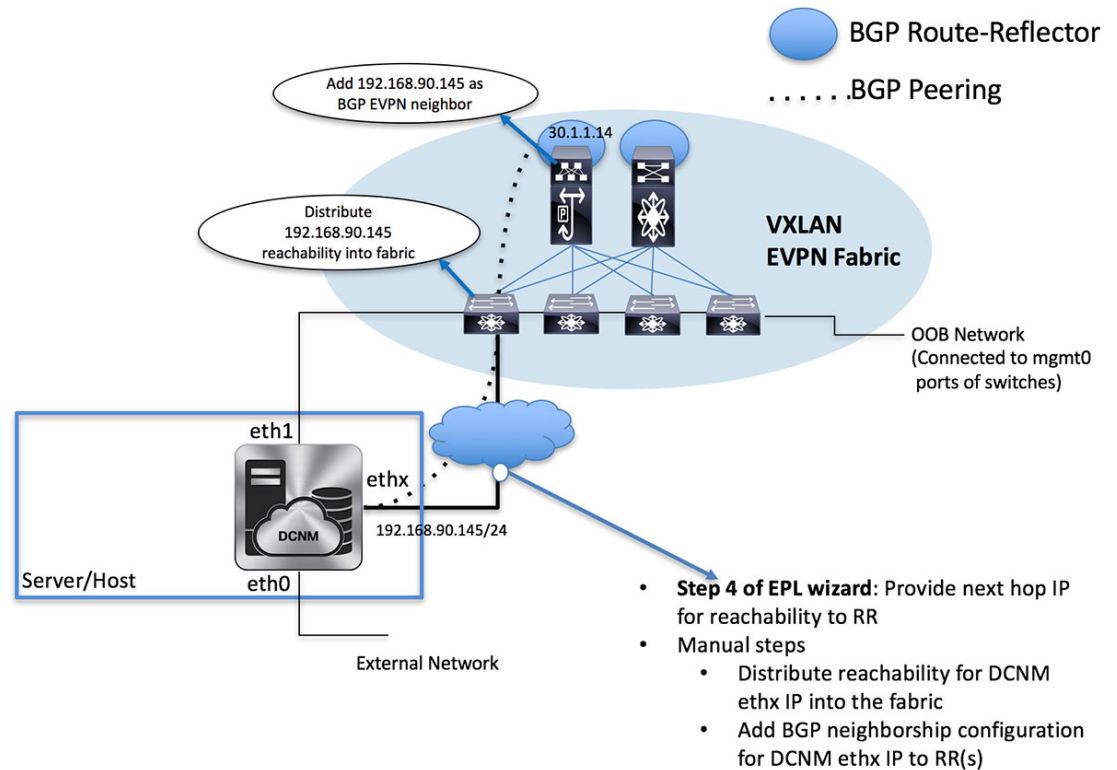


- **Step 4 of EPL wizard:** Select directly connected switch, select directly connected interface, and provide an appropriate IPv4 address/mask
  - Switch interface auto-configured as routed port
  - BGP neighborhood configuration for DCNM auto-added to RR(s)

- **Semi-automated**—In this option, only the DCNM is configured appropriately for EPL. The assumption is that there is IP reachability already pre-established from the DCNM to the RR, hence an appropriate next-hop IP address should be provided in step 4 for this purpose. In addition, appropriate BGP neighborhood configuration must be added to the RRs to accept DCNM as a peer. Note that, DCNM queries the BGP RR to glean information for establishment of the peering (e.g. ASN, RR IP etc.).

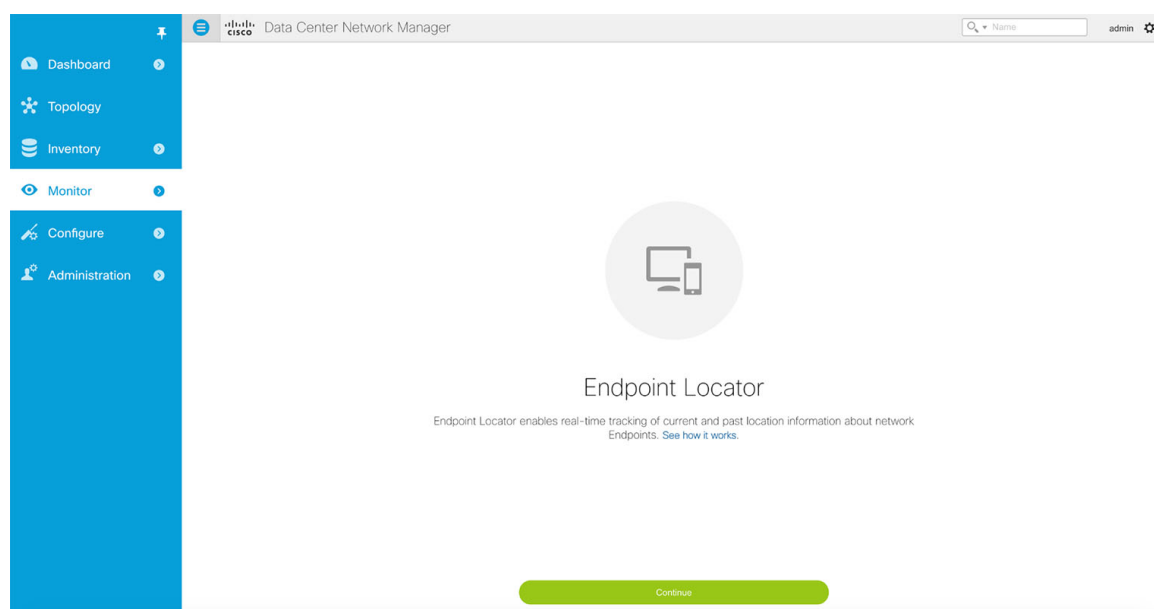
## Option 2: Semi Automated

The Server Hosting DCNM has IP connectivity to BGP RR(s)



### Procedure

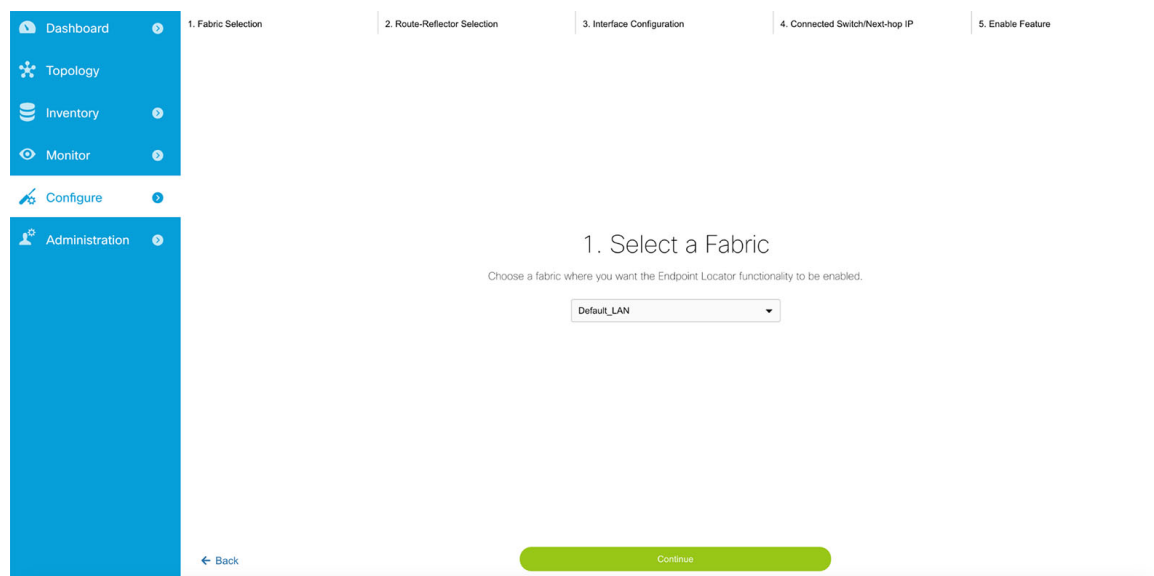
- Step 1** From the menu bar, choose **Configure > Endpoint Locator > Configure**. The Endpoint Locator page appears with a **See how it works** help link.



**Step 2** Click **Continue**.

**Step 3** Select the appropriate fabric on which the Endpoint Locator feature should be enabled to track endpoint activity.

EPL can only be enabled for one fabric (this can be DFA or EVPN).



**Step 4** Select the switch(es) on the fabric hosting the Route-Reflector (RRs). DCNM will peer with the RR(s).

1. Fabric Selection | 2. Route-Reflector Selection | 3. Interface Configuration | 4. Connected Switch/Next-hop IP | 5. Enable Feature

## 2. Select Route-Reflector (RR)

Choose the switch(es) on which the BGP Route-Reflector(s) has been configured.

n9k-14-spine

BGP Route-Reflector 2 (optional)

← Back Continue

**Step 5** Configure the interface on DCNM for IP reachability to the RR. Select the appropriate interface ethx and provide the IP address and subnet mask for that interface. Through this interface, the in-band connectivity is established from the DCNM to the RR.

1. Fabric Selection | 2. Route-Reflector Selection | 3. Interface Configuration | 4. Connected Switch/Next-hop IP | 5. Enable Feature

## 3. Configure DCNM Interface

Choose the Ethernet interface on the DCNM that will provide reachability to the BGP Route-Reflector(s) within the fabric.

eth2

Interface IP

192.168.90.145 / 24

← Back Continue

**Step 6** In the next step, a selection must be made by checking (fully-automated mode) or unchecking the “Configure my fabric” (semi-automated mode) option. First, we will look at the semi-automated mode which is likely the preferred option in scenarios where there is no direct connectivity between the DCNM server and the ToR. In the semi-automated mode, the “Configure my fabric” option is un-checked. Hence, only the next-hop IP address for reachability to the RR must be specified. Recall that any configuration on the network fabric for reachability between the RR and the DCNM must be done separately in this case.



1. Fabric Selection | 2. Route-Reflector Selection | 3. Interface Configuration | 4. Connected Switch/Next-hop IP | 5. Enable Feature

### 4. Connected Switch/Next-hop IP

Provide the next-hop IP that provides reachability to the BGP Route-Reflector (RR).

☐ Configure my fabric

Next-hop IP

192.168.90.18

← Back Continue

**Step 7** The last step provides a summary of the information entered in the previous steps. The wizard view allows navigation to any particular step whereby one can make necessary changes/edits. In this step, one must specify whether additional information such as PORT, VLAN, VRF etc. is required when enabling the EPL feature. If the No option is selected, then this information will not be collected and reported by EPL.

1. Fabric Selection | 2. Route-Reflector Selection | 3. Interface Configuration | 4. Connected Switch/Next-hop IP | 5. Enable Feature

### 5. Review and Enable Endpoint Locator

|                           |                          |                                                     |
|---------------------------|--------------------------|-----------------------------------------------------|
| Fabric:                   | DCNM Interface:          | Fabric configuration                                |
| Default_LAN               | eth2 (192.168.90.145/24) | Skip configuring my fabric                          |
| Route-Reflector 1:        | Next-hop IP:             | * Collect additional information (Port, VLAN, etc.) |
| n9k-14-spine (24.21.0.14) | 192.168.90.18            | No                                                  |
| Route-Reflector 2:        |                          |                                                     |

← Back Continue

However, if the Yes option is selected in the drop down, a warning pop-up appears that feature NX-API must be supported and enabled on the switches/ToRs/leafs to gather this information. Otherwise this additional information cannot be fetched or reported.

This option requires NX-API feature to be enabled on the switches. Please ensure this step is done for the Endpoint Locator feature to fetch additional information. Are you sure you want to continue?

Yes No

### 5. Review and Enable Endpoint Locator

Fabric: Default\_LAN DCNM Interface: eth2 (192.168.90.145/24) Fabric configuration: Skip configuring my fabric

Route-Reflector 1: n9k-14-spine (24.21.0.14) Next-hop IP: 192.168.90.18 \* Collect additional information (Port, VLAN, etc.): Yes

Router-Reflector 2:

Back Continue

**Step 8** Once the appropriate selections are made and various inputs have been reviewed, click on the Continue button to enable EPL. A progress bar will appear indicating the status of the EPL feature enable process.

### 5. Review and Enable Endpoint Locator

Fabric: Default\_LAN DCNM Interface: eth2 (192.168.90.145/24) Fabric configuration: Skip configuring my fabric

Route-Reflector 1: n9k-14-spine (24.21.0.14) Next-hop IP: 192.168.90.18 \* Collect additional information (Port, VLAN, etc.): No

Router-Reflector 2:

Back Continue

If there are any errors during the enablement, the enable process will abort and the appropriate error message will be displayed. Otherwise, EPL will be successfully enabled and on clicking the Ok, the screen will be automatically redirected to the EPL dashboard.

**Step 9** In case in Step 4, the “Configure my fabric” option is selected/checked, then the user has opted for the fully-automated mode for enabling EPL. Recall that in this case the DCNM server must be directly attached to a ToR/leaf switch. The appropriate connected switch and port on the other side of the DCNM *ethx* interface must be selected. The specified IP address will be configured on the selected interface on the connected switch.

In this case, the review step will look as follows:

When the Endpoint Locator feature is enabled, there are a number of steps that occur in the background. DCNM will contact the selected RR(s) and determine the ASN, determine whether the fabric is L3VPN or EVPN enabled, and also determine the interface IP that is bound to the BGP process. Also, appropriate BGP neighbor statements are added on the RR(s), to get it ready to accept the BGP connection that will be initiated from the DCNM. The neighbor address will be the same as that of the ethx interface specified in step 2. DCNM will configure the ethx interface that provides in-band connectivity to the fabric with the appropriate IP address provided in step 2. In order to provide reachability to the RR, a static route will be added to DCNM. If the “Configure my fabric” option is selected during enabling EPL, the connected switch and associated interface specified in step 2 will be configured as a routed interface. This ensures that DCNM has connectivity to the RR. Once EPL is successfully enabled, the user is automatically redirected to the EPL dashboard that depicts operational and exploratory insights into the endpoints that are present in the fabric. For more information, please refer to the Section “Exploring Endpoint Locator Details”.

## Flushing the Endpoint Database

To flush the all the Endpoint information, perform the following steps:

### Procedure

- Step 1** Choose **Configure > Endpoint Locator > Configure**, and then click the **clean up** link.

The screenshot shows the Cisco Data Center Network Manager web interface. On the left is a blue sidebar with navigation links: Dashboard, Topology, Inventory, Monitor, Configure (highlighted), and Administration. The main content area is titled "Endpoint Locator". It contains several input fields and a dropdown menu:

- Fabric:** Default\_LAN
- DCNM Interface:** eth2 (192.168.91.58/24)
- Fabric configuration:** Configure my fabric (dropdown menu)
- Route-Reflector 1:** n9k-14-spine (24.21.0.14)
- Connected Switch:** n9k-15 (24.21.0.15)
- \* Collect additional information (Port, VLAN, etc.):** Yes (dropdown menu)
- Router-Reflector 2:** (empty field)
- Connected Switch Interface:** Ethernet1/3 - 192.168.91.1

At the bottom of the configuration area, there is a red button labeled "Disable Feature" and a "clean up" link with a trash icon.

This shows a warning message indicating that all the endpoint information from the database will be flushed.

This screenshot shows the same "Endpoint Locator" configuration page as the previous one, but with a confirmation dialog box overlaid in the center. The dialog box has a red "X" icon and the title "Delete Endpoint Locator Data". The text inside the dialog asks: "Are you sure you want to permanently delete the existing Endpoint Locator?". There are two buttons at the bottom of the dialog: "Delete" (in blue) and "Cancel" (in gray). The background configuration fields are dimmed.

**Step 2** Click **Delete** to continue or *Cancel* in case the user wants to abort.

## Adding High Availability Node to Endpoint Locator Configuration

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Endpoint Locator > Configure**. The Endpoint Locator page appears and the fabric configuration details are displayed.
  - Step 2** Click the **Add HA node** link.
  - Step 3** In the Configure Standby DCNM Interface page, choose the Ethernet interface on DCNM that will provide reachability to the BGP Route-Reflector(s) within the fabric.
  - Step 4** Click **Continue**.
  - Step 5** In the Connected Switch on Standby DCNM screen, select the physical switch's front-panel interface to which the DCNM is connected.
  - Step 6** Click **Configure HA Node**. The configuration details are displayed on the Endpoint Locator page.
- 

## Configuring Endpoint Locator in DCNM High Availability Mode

### Procedure

---

- Step 1** From the menu bar, choose **Monitor > Endpoint Locator > Configure**. The Endpoint Locator page appears and the fabric configuration details are displayed.
  - Step 2** In the Select a fabric to configure endpoint locator in DCNM HA mode.
  - Step 3** Click **Continue**.
  - Step 4** Select a Route-Reflector (RR).
  - Step 5** Click **Continue**.
  - Step 6** Configure Ethernet interfaces on both primary and standby DCNM nodes.
  - Step 7** Click **Continue**.
  - Step 8** Select switch interface connected to both primary and standby DCNM.
  - Step 9** Click **Continue**.
  - Step 10** Configure the Connect Switch or Next-hop IP.
  - Step 11** Click **Continue**.  
After you configure the Endpoint Locator in HA mode, you can view details such as Endpoint Activity and Endpoint History in the Endpoint dashboard. To view these details, navigate to **Monitor > Endpoint Locator > Explore**.
-

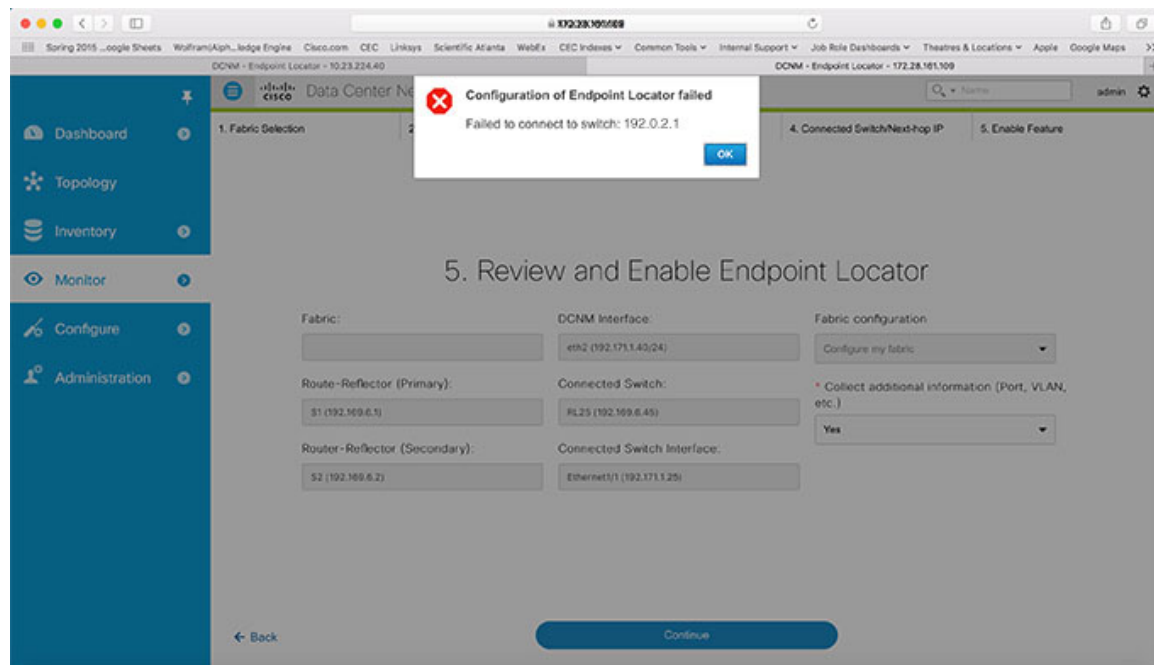
## Disabling Endpoint Locator

### Procedure

- Step 1** From the menu bar, choose **Configure > Endpoint Locator > Configure**. The Endpoint Locator page appears and the fabric configuration details are displayed.
- Step 2** Click the **Disable Feature** button.

## Troubleshooting Endpoint Locator

There may be multiple reasons why enabling the Endpoint Locator feature may fail. Typically, if the appropriate devices are selected and the IP addresses to be used are correctly specified, the connectivity of the DCNM to the BGP RR may not be present due to which the feature cannot be enabled. This is a sanity check that is present to ensure that basic IP connectivity is available. The following image shows an example error scenario that was encountered during an attempt to enable the EPL feature.



The logs for EPL are located at the following location: `/usr/local/cisco/dcm/fm/logs`. The log that provides further details on what all occurred when the EPL feature is enabled or disabled, are present in the file `epl.log`. The following example provides a snapshot of the log that will provide the user further information on when EPL enablement failed.

The following example helps you to understand why Endpoint Locator is unable to Connect to a switch.

```
#tail -f epl.log
2017.04.08 07:47:05 INFO [epl] Running script: [/sbin/appmgr, status, epls]
2017.04.08 07:47:05 INFO [epl] Received response:
```

```

2017.04.08 07:47:05 INFO [epl]
2017.04.08 07:47:05 INFO [epl] >>> Sat Apr 8 07:47:05 PDT 2017
2017.04.08 07:47:05 INFO [epl] appmgr status epls
2017.04.08 07:47:05 INFO [epl]
2017.04.08 07:47:05 INFO [epl] EPLS is stopped...
2017.04.08 07:47:08 INFO [epl] Running command: ifdown eth2
2017.04.08 07:47:08 INFO [epl] Received response:
2017.04.08 07:47:08 INFO [epl] EPL disabled succesfully
2017.04.08 08:00:06 INFO [epl] Enable End Point Locator
2017.04.08 08:00:13 ERROR [epl] Failed to connect to switch 192.169.6.2:java.lang.Exception:
 Authentication failed : Ssh/Telnet failed to connect with the switch
2017.04.08 08:00:13 INFO [epl] Failed to Enabled End Point Locator. Trying to removing
 configuration
2017.04.08 08:00:13 INFO [epl] Disable EPL
2017.04.08 08:00:19 ERROR [epl] Failed to connect to switch 192.169.6.2:java.lang.Exception:
 Authentication failed : Ssh/Telnet failed to connect with the switch
2017.04.08 08:00:19 ERROR [epl] Failed to connect to switch: 192.169.6.2
2017.04.08 08:00:21 ERROR [epl] Failed to unconfigure BGP neighbor or failed to connect to
 switch or fabric information not provided.
2017.04.08 08:00:21 ERROR [epl] Failed to unconfigure BGP neighbor or failed to connect to
 switch or fabric information not provided.
2017.04.08 08:00:21 INFO [epl] Received response: configure terminal
Interface Ethernet1/1
no ip address
switchport
end
Enter configuration commands, one per line. End with CNTL/Z.
(config)# Interface Ethernet1/1
(config-if)# no ip address
(config-if)# switchport
(config-if)# end
from 192.169.6.45
2017.04.08 08:00:21 ERROR [epl] Failed to disable EndPoint locator:
java.lang.NullPointerException
2017.04.08 08:00:21 INFO [epl] EPL disabled succesfully

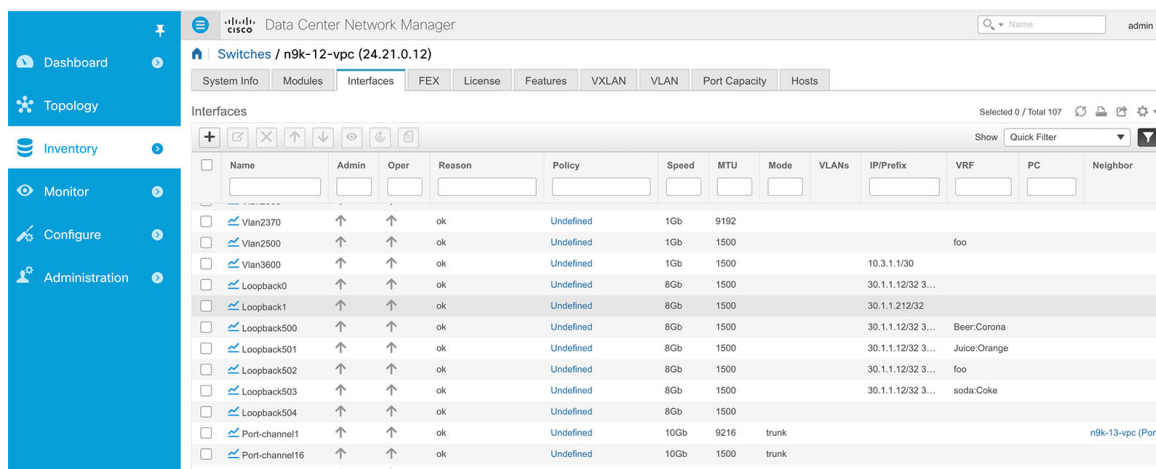
```

In this example, the LAN credentials set in DCNM for accessing the switch were incorrect. There may be other reasons for which enablement of the EPL feature may fail. In all scenarios, an appropriate error message will be depicted to the user and additional context information can be obtained from epl.log.

Once EPL is successfully enabled, all the debug/error/info logs associated with endpoint information are stored in bgp.log. Depending on the scale of the network and the number of endpoint events, the file size may grow. Hence, there is a restriction on the maximum number and size of bgp.log. Up to 10 such files will be stored with each file having a maximum size of 10MB.

As mentioned earlier, the Endpoint Locator relies on BGP updates to get endpoint information. In order for this to work, the switch loopback or VTEP interface IPs must be discovered on the DCNM for all switches that have endpoints. This can be validated by navigating to the Cisco DCNM Switch Dashboard Interfaces tab, and verifying if the IP/Prefix associated with the corresponding L3 interfaces (typically loopbacks) are correctly displayed.





In a large-scale setup, it may take more than 30 seconds (default timer set in Cisco DCNM) to get this information from the switch. If this occurs, the `ssh.read-wait-timeout` property (in the Administration > DCNM Server > Server Properties page) should be changed from 30000(default) to 60000 or a higher value.

## SAN

The SAN menu includes the following submenus:

## SAN Zoning

Zoning enables you to set up access control between storage devices or user groups. If you have administrator privileges in your fabric, you can create zones to increase network security and to prevent data loss or corruption. Zoning is enforced by examining the source-destination ID field.

The following table describes the fields and icons that appear on Cisco DCNM **Configure > SAN > Zoning** tab.

| Field          | Description                                                                                                                               |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Fabric         | From the Fabric drop-down list, you can choose the fabric for which you are configuring or viewing the SAN Zoning.                        |
| VSAN           | From the VSAN drop-down list, you can choose the VSAN for which you are configuring zoning.                                               |
| Switches       | From the Switch drop-down list, select the switch to which you want to configure.                                                         |
| Commit Changes | Commits the Zoning configuration changes to all the switches. This field is only applicable when a zone is in the enhanced or smart mode. |

| Field                   | Description                                                                                                               |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Distribute              | Distributes the Zoning configuration to all the switches. This field is only applicable when a zone is in the basic mode. |
| Export All              | You can export the Zoning configurations to a .csv file, and save it on your local directory.                             |
| Zonesets                | Lists all the Zoneset configured for the selected Fabric, VSAN and the Switch.                                            |
| Zones                   | Lists all the Zones configured under the selected Zoneset.                                                                |
| Zone Members            | Lists the members present in the selected Zone.                                                                           |
| Available to Add        | Lists the available devices to add to the Zones.                                                                          |
| Clear Server Cache      | Clears the cache on the Cisco DCNM server.                                                                                |
| Discard Pending Changes | Discards the changes in progress.                                                                                         |

This section contains the following:

## Zonesets

Based on the selected Fabric, VSAN and Switch, the Zoneset area displays the configured zonesets and their status. You can create, copy, delete or edit the zonesets. Further, the zonesets can be activated or deactivated.

### Procedure

- 
- Step 1** To create zonesets, from Cisco DCNM **Web Client > Configure > SAN Zoning > Zonesets**, click Create Zoneset icon.
- a) In the Create Zoneset window, enter a valid name for the zoneset, and click **Create**.  
A zoneset is created and is listed in the **Zoneset** area.
- Step 2** To clone or copy zonesets, from Cisco DCNM **Web Client > Configure > SAN Zoning > Zonesets**, select the zone radio button and click Clone/Copy Zoneset icon.  
The Clone or Copy Zoneset window shows two options.
- a) Click the appropriate Action radio button.  
You can choose of the of the following:
- **Copy**—Creates a new zoneset that consists copies of the zones in the initial zoneset.  
You can prepend or append a string to identify the copied zoneset. Enter a valid string in the **Tag** field, and select the **Prepend** or **Append** radio button.
  - **Clone**—To create a new zoneset with a new name consisting of the same zones as the source zoneset.

In the Name field, enter a valid name for the new zoneset.

- b) Click **OK** to clone or copy the zoneset.  
The cloned or the copied zoneset appears in the Zoneset area.

- Step 3** To delete the zoneset, from Cisco DCNM Web Client > **Configure** > **SAN Zoning** > **Zones**, select the zoneset radio button and click delete zoneset icon.  
A confirmation window appears.  
Click **Yes** to delete the zoneset.
- Step 4** To edit the zone name, from Cisco DCNM Web Client > **Configure** > **SAN Zoning** > **Zoneset**, select the zone radio button and click Rename Zoneset icon.  
In the Name field, enter the new name for the zoneset.  
Click **Rename**.
- Step 5** To Activate Zoneset, from Cisco DCNM Web Client > **Configure** > **SAN Zoning** > **Zonesets**, select the zoneset radio button and click **Activate**.  
The Zoneset Differences window shows the changes made to the zoneset since it was activated previously.  
Click **Activate**.
- Step 6** To Deactivate Zoneset, from Cisco DCNM Web Client > **Configure** > **SAN Zoning** > **Zonesets**, select the zoneset radio button and click **Deactivate**.  
A confirmation window appears.  
Click **Yes** to deactivate the zoneset.

## Zones

Based on the Zoneset selected, the zones configured under that zoneset are displayed in the **Zones** area. It will also display true or false only when the VSAN has smart zone enabled. You can create, copy, delete or edit the zones. Furthermore, the zones can be added to or removed from the selected Zoneset. You can also enable or disable smart zone on the zone table.



### Note

You must select the Zoneset for which you need to alter the zones.

Select **Zoneset** radio button in the Zonesets area. The zones configured on the selected Zoneset and zones on the switch are displayed. The zones that are a part of the Zone are marked with a green check mark.

The Zones area has the following fields and their descriptions.

| Field      | Description                                                                                                                                    |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| In Zoneset | Specifies whether a zone is part of a zoneset.<br>Displays <b>true</b> if the zone is part of a zoneset.<br>Otherwise, displays <b>false</b> . |

| Field      | Description                                                                                                                                                                                                                                                                                                      |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | You can search by choosing true or false from the <b>In Zoneset</b> drop-down list.                                                                                                                                                                                                                              |
| Zone Name  | Displays the name of the zone.<br>You can search by specifying the zone name.                                                                                                                                                                                                                                    |
| Smart Zone | Specifies whether a zone is a smart zone.<br>Displays <b>true</b> if the zone is a smart zone. Otherwise, displays <b>false</b> .<br>You can search this field by choosing <b>true</b> or <b>false</b> from the <b>Smart Zone</b> drop-down list. This field only shows up when the VSAN has smart zone enabled. |

## Procedure

- Step 1** To create zones, from Cisco DCNM Web Client > **Configure** > **SAN** > **Zoning** > **Zones**, click Create icon.
- In the Create Zoneset window, enter a valid name for the zoneset, and click **Create**.  
A zone is created and is listed in the **Zones** area.
- Step 2** To Clone Zones, from Cisco DCNM Web Client > **Configure** > **SAN** > **Zoning** > **Zones**, select the zone radio button and click Clone Zone icon.  
The Clone Zone screen appears.
- In the Name field, enter a valid name for the new zoneset.
  - Click **Clone** to clone the zone.  
The cloned zones appear in the **Zones** area.
- Step 3** To add zone to a zoneset, from Cisco DCNM Web Client > **Configure** > **SAN Zoning** > **Zones**, select the zone that is not a part of the zoneset and click Add Zone icon. You can select more than one zone to be added to the Zoneset.  
The zone will be added to the selected Zoneset. A green tick mark appears next to the Zone name to indicate that the zone is added to the zoneset.
- Step 4** To remove zone from a zoneset, from Cisco DCNM Web Client > **Configure** > **SAN Zoning** > **Zones**, check the zone check box and click Remove Zone icon. You can select more than one Zone to be deleted from the Zoneset.  
The zone will be removed from the selected Zoneset. A green tick mark disappears next to the Zone name to indicate that the zone is removed from the zoneset.
- Step 5** To Delete Zones, from Cisco DCNM Web Client > **Configure** > **SAN Zoning** > **Zones**, check zone check box and click Delete Zone icon.  
A confirmation window appears.  
Click **Yes** to delete the selected zones.
- Note** You cannot delete a zone that is a member of the selected zoneset. You must remove the zone from the zoneset to delete it.

- Step 6** To edit the zone name, from Cisco DCNM Web Client > **Configure** > **SAN Zoning** > **Zones**, select the zone radio button and click **Rename Zone** icon.  
In the **Name** field, enter the new name for the zone.  
Click **Rename**.
- Step 7** To enable smart zone, from Cisco DCNM Web Client > **Configure** > **SAN Zoning** > **Zones**, select the zone radio button and click **Enable Smart Zone** icon.  
Under the **Smart Zone** column, it will display **True**.
- Step 8** To disable smart zone, from Cisco DCNM Web Client > **Configure** > **SAN Zoning** > **Zones**, select the zone radio button and click **Disable Smart Zone** icon.  
Under the **Smart Zone** column, it will display **false**.

## Zone Members

Based on the selected Zoneset and the Zone, the Zone Members area displays the zone members and their status. You can create, or remove members from the Zoneset.

The Zone Members area has the following fields and their descriptions.

| Field            | Description                                                                                                                                                                                                                                                                                                         |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Zone             | Displays the Zone under which this member is present.<br>You can search by zone name in this field.                                                                                                                                                                                                                 |
| Zoned By         | Displays the type of zoning.<br>You can search by type of zoning such as WWN, FCID, fcAlias, or iSCSI.                                                                                                                                                                                                              |
| Device Type      | Displays the smart zoning device type.<br>The applicable values are <b>Host</b> , <b>Storage</b> , or <b>Both</b> .<br>You can search this field by choosing <b>Host</b> , <b>Storage</b> or <b>Both</b> from the <b>Device Type</b> drop-down list. This field only shows up when the VSAN has smart zone enabled. |
| Name             | Displays the name of the zone member.<br>You can search by specifying the zone name.                                                                                                                                                                                                                                |
| Switch Interface | Specifies the switch interface that the zone member is attached to.<br>You can search by specifying the switch interface.                                                                                                                                                                                           |
| FcId             | Specifies the FcID associated with the zone member.<br>You can search by specifying the FcID associated with the zone member.                                                                                                                                                                                       |

| Field | Description                                                                             |
|-------|-----------------------------------------------------------------------------------------|
| WWN   | Specifies the WWN of the switch.<br>You can search by specifying the WWN of the switch. |

## Procedure

- Step 1** To create zone members, from Cisco DCNM Web Client > **Configure** > **SAN Zoning** > **Zone Members**, click Create icon.
- In the Create and Add Member window, enter the WWN name for the zone member.
  - Click **Create and Add**.  
**Add Members to Zones** window pops out, you can specify the smart zoning device type as **Host**, **Storage** or **Both(Host and Storage)**. A zone member is created and is listed in the **Zone Member** area.
- The Create and Add feature allows you to add a member to a zone that does not exist in the fabric, currently. This feature can also be utilized when the device discovery did not discover all the devices. With the Available to add feature, you can add a discovered device to the zone.
- Step 2** To Remove Zone Member, from Cisco DCNM Web Client > **Configure** > **SAN Zoning** > **Zone Members**, check the zone member check box and click Remove Member icon.  
You can more than one zone member at a time, for deletion.

## Available to Add

Perform the following task to add discovered devices to the zone(s).

The Available to Add area has the following fields and their descriptions.

| Field            | Description                                                                                                                                                                                                     |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type             | Displays the smart zoning device type.<br>The applicable values are <b>Host</b> or <b>Storage</b> .<br>You can search this field by choosing <b>Host</b> or <b>Storage</b> from the <b>Type</b> drop-down list. |
| Name             | Displays the name of the zone.<br>You can search by specifying the zone name.                                                                                                                                   |
| Switch Interface | Specifies the switch interface that the zone member is attached to.<br>You can search by specifying the switch interface.                                                                                       |
| FcId             | Specifies the FcID associated with the zone member.                                                                                                                                                             |

| Field | Description                                                                             |
|-------|-----------------------------------------------------------------------------------------|
|       | You can search by specifying the FcID associated with the zone member.                  |
| WWN   | Specifies the WWN of the switch.<br>You can search by specifying the WWN of the switch. |

### Procedure

- Step 1** From Cisco DCNM **Web Client** > **Configure** > **SAN** > **Zoning** > **Available to Add**, in the Zone by area select the Ports or Device radio buttons.  
The Zone by feature determines if the device must be added to the zone using the device WWN or Device alias.  
A window appears showing the list of End Ports or Devices available to add.  
If you choose **Zone By: End Port**, the devices are added to the zones by WWN. If you choose **Zone By: Device Alias**, the devices are added to the zones by Device Alias. Based on the zone by option you choose, the devices are displayed.
- Step 2** Select the devices to add to a zone.
- Step 3** Click **Add** to add the selected devices to the zone.
- Note** You can select more than one zone. When this occurs, a dialog appears that shows a list of all the zones that are currently selected on the zone table.

## Configuring FCIP

Cisco DCNM allows you to create FCIP links between Gigabit Ethernet ports, enables Fibre Channel write acceleration and IP compression. You can configure FCIP from **Cisco DCNM Web Client** > **SAN** > **FCIP**.

### Procedure

- Step 1** From the menu bar, select **Configure** > **SAN** > **FCIP**.  
The Welcome page displays the tasks to configure FCIP using the FCIP Wizard.
- Step 2** Click **Next** to select the switch pair.
- Step 3** Select two MDS switches to be connected via FCIP for **Between Switch** and **and Switch** from the drop-down list.  
Each switch must have an ethernet port connected to an IP network to function correctly.
- Note** In the case of a federation setup, both switches must belong to fabrics that are discovered or managed by the same server.
- Step 4** Click **Next** to select the Ethernet ports.
- Step 5** Select the Ethernet ports to be used in FCIP ISL between the selected switches.

Down ports should be enabled to function correctly. Security can be enforced for unconfigured 14+2, 18+4, 9250i and SSN16 Ethernet ports.

**Step 6** Click **Next** to specify the IP addresses and add IP route.

**Step 7** Enter the Ethernet ports IP addresses and specify the IP Routes if the port addresses are in a different subnet.

**Note** The changes to IP Address and IP Route will be applied on pressing the **Next** button.

**Step 8** Click **Next** to specify Tunnel properties.

**Step 9** Specify the following parameters to tunnel the TCP connections.  
Enter the parameters

- **Max Bandwidth**—Enter the number between 1 to 5000. The unit is **Mb**.
- **Min Bandwidth**—Enter the minimum bandwidth value. The unit is **Mb**.
- **Estimated RTT(RoundTrip Time)**—Enter the number between 0 to 300000. The unit is **us**. Click **Measure** to measure the roundtrip time.
- **Write Acceleration**—Check the check box to enable the write acceleration.  
**Note** If Write Acceleration is enabled, ensure that flows will not load balance across multiple ISLs.
- **Enable Optimum Compression**—Check the check box to enable the optimum compression.
- **Enable XRC Emulator**—Check the check box to enable XRC emulator.
- **Connections**—Enter the number of connections from 0 to 100.

**Step 10** Click **Next** to create FCIP ISL.

**Step 11** Enter the **Profile ID** and **Tunnel ID** for the switch pair, and select the **FICON Port Address** from the drop-down list. Click **View Configured** to display the **Profiles** and **Tunnels** information. Select the **Trunk Mode** from **nonTrunk**, **trunk** and **auto**. Specify the **Port VSAN** for **nonTrunk** and **auto**, and allowed **VSAN List** for Trunk tunnel.

**Step 12** Click **Next** to the last summary page.  
The **Summary** view displays what you have selected in the previous steps.

**Step 13** Click **Deploy** to configure FCIP or click **Finish** complete the configuration and deploy later.

## Device Alias

A device alias is a user-friendly name for a port WWN. Device alias name can be specified when configuring features such as zoning, QoS and port security. The device alias application uses the Cisco Fabric Services (CFS) infrastructure to enable efficient database management and fabric-wide distribution.

This section contains context sensitive online help content under **Configure > SAN > Device Alias**.

The following table describes the fields that appear on Cisco DCNM Web Client **Configure > SAN > Device Alias**.



| Field        | Description                                        |
|--------------|----------------------------------------------------|
| Seed Switch  | Displays the device alias seed switch name.        |
| Device Alias | Displays the alias retrieved from the seed switch. |
| pWWN         | Displays the port WWN.                             |

This section contains the following:

## Configuration

Select the Fabric from the Fabric drop-down list. The list of device aliases existing on the fabric will be retrieved and displayed.

Before performing any Device Alias configuration, check the status on the **CFS** tab, to ensure that the status is "success".



### Note

To perform Device Alias configuration from the Cisco DCNM Web client, the fabric must be configured as Device Alias enhanced mode.

## Procedure

- Step 1** To delete the device alias, Cisco DCNM Web Client > **Configure** > **SAN** > **Device Alias** > **Configuration** tab, check the device alias you need to delete.
- Click **Delete**.  
A confirmation message appears.  
**Note** Deleting the device alias may cause traffic interruption.
  - Click **Yes** to delete the topic alias.
- Step 2** To create the device alias, from Cisco DCNM Web Client > **Configure** > **SAN** > **Device Alias** > **Configuration** tab, click **Create**.  
The Add Device Alias windows appears.  
All the provisioned port WWNs are populated in the table.
- Enter a device alias name in the **Device Alias** field to indicate to create a device alias for the selected pWWN.
  - Click **Save** to exit the inline editor mode.
  - Click **Apply** to assign the device alias to the switches.  
You can also create a device alias with a non-provisioned port WWN.
  - Click **New Alias** to create a new table row in inline editor mode.
  - In the **pWWN** field, enter the non-provisioned port WWN for the new alias.
  - Click **Save** to exit the inline editor mode.
  - Click **Apply** to assign the device alias and the associated pWWN to the switches.

**Note** If you close the Add Device Alias window before applying the device alias to the switches, the changes will be discarded and the device alias will not be created.

**Step 3** For end devices with an attached service profile, the service profile name is populated to the **Device Alias** field. This allows the service profile name as device alias name for those devices.

---

Device Alias creation is CFS auto-committed after clicking Apply. Click **CFS** tab to check if CFS is properly performed after the device alias was created. In case of failure, you must troubleshoot and fix the problem.

## CFS

Select the Fabric from the Fabric drop-down list. The list of device aliases existing on the fabric will be retrieved and displayed.

CFS information is listed for all the eligible switches in the fabric. Before performing any Device Alias configuration, check the status on the CFS tab, to ensure that the status is "success". If the CFS is locked by another user, or if the previous operation failed, ensure that the CFS session is unlocked.

The Cisco DCNM Web Client Configure > SAN > Device Alias > CFS tab shows the following fields.

### Procedure

---

**Step 1** To commit the CFS configuration, from Cisco DCNM **Web Client** > **Configure** > **SAN** > **Device Alias** > **CFS** tab, click the **Switch** radio button.

Click **Commit**.

The CFS configuration for this switch is committed.

**Step 2** To abort the CFS configuration, from Cisco DCNM **Web Client** > **Configure** > **SAN** > **Device Alias** > **CFS** tab, click the **Switch** radio button.

Click **Abort**.

The CFS configuration for this switch will be aborted.

**Step 3** To clear the lock on the CFS configuration of the switch, from Cisco DCNM **Web Client** > **Configure** > **SAN** > **Device Alias** > **CFS** tab, click the **Switch** radio button.

Click **Clear Lock**.

If the CFS is locked by another user, or if the previous operation failed, ensure that the CFS session is unlocked.

---

## Port Monitoring

This feature allows you to save custom Port Monitoring policies in the Cisco DCNM database. It allows you to push the selected custom policy to one or more fabrics or Cisco MDS 9000 Series Switches. The policy is designated as active Port-Monitor policy in the switch.

This feature is supported only on the Cisco MDS 9000 SAN Switches and therefore the Cisco DCNM user is allowed to select the MDS switch to push the policy.

Cisco DCNM provides five templates to customize the policy. The user-defined policies are saved in the Cisco DCNM database. You can select any template or customized policy to push to the selected fabric or switch with the desired port type.



**Note** You can edit only user-defined policies.

The following table describes the fields that appear on Cisco DCNM **Web Client > Configure > SAN > Port Monitoring**.

| Field            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Templates        | <p>This drop-down list shows the following templates for policies:</p> <ul style="list-style-type: none"> <li>• Normal_accessPort</li> <li>• Normal_allPort</li> <li>• Normal_trunksPort</li> <li>• Aggressive_accessPort</li> <li>• Aggressive_allPort</li> <li>• Aggressive_trunksPort</li> <li>• Most-Aggressive_accessPort</li> <li>• Most-Aggressive_allPort</li> <li>• Most-Aggressive_trunksPort</li> <li>• default</li> <li>• slowdrain</li> </ul> |
| Save             | Allows you to save your changes for the user-defined policies.                                                                                                                                                                                                                                                                                                                                                                                             |
| Save As          | <p>Allows you to save an existing policy as a new policy with a different name.</p> <p>This creates another item in the templates as Custom Policy. The customized policy will be saved under this category.</p> <p>If you click <b>Save As</b> while the policy is edited, the customized policy will be saved.</p> <p><b>Note</b> The port type of the customized policy will not be saved when Save As is selected.</p>                                 |
| Delete           | Allows you to delete any user-defined policies.                                                                                                                                                                                                                                                                                                                                                                                                            |
| Push to switches | Allows you to select a fabric or switch and push the selected policies with a desired port type.                                                                                                                                                                                                                                                                                                                                                           |

| Field               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | <p>The available port types are:</p> <ul style="list-style-type: none"> <li>• trunks/Core</li> <li>• access-port/Edge</li> <li>• all</li> </ul> <p><b>Note</b> If you choose trunks or all, the port guard will be disabled.</p> <p>The following policies select the trunks/Core policy type:</p> <ul style="list-style-type: none"> <li>• Normal_trunksPort</li> <li>• Aggressive_trunksPort</li> <li>• Most-Aggressive_trunksPort</li> </ul> <p>The following policies select the access-port/Edge policy type:</p> <ul style="list-style-type: none"> <li>• Normal_accessPort</li> <li>• Aggressive_accessPort</li> <li>• Most-Aggressive_accessPort</li> <li>• slowdrain</li> </ul> <p>The following policies select the all policy type:</p> <ul style="list-style-type: none"> <li>• Normal_allPort</li> <li>• Aggressive_allPort</li> <li>• Most-Aggressive_allPort</li> <li>• default</li> </ul> <p>Select the parameters and click <b>Push</b> to push the policies to the switches in the fabric.</p> <p>If there is any active policy with the same or common port type, the push command will configure the same policy on the selected devices. This policy will replace the existing active policy with the same or common port type.</p> <p>If you click <b>Push to Switches</b> while the policy is edited, the customized policy will not be saved.</p> |
| Counter Description | <p>Specifies the counter type.</p> <p>Move the pointer to the "i" icon next to the counter description to view detailed information.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Field             | Description                                                                                                                                                                              |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rising Threshold  | Specifies the upper threshold limit for the counter type.                                                                                                                                |
| Rising Event      | Specifies the type of event to be generated when rising threshold is reached or crossed.                                                                                                 |
| Falling Threshold | Specifies the lower threshold limit for the counter type.                                                                                                                                |
| Falling Event     | Specifies the type of event to be generated when falling threshold is reached or crossed.                                                                                                |
| Poll Interval     | Specifies the time interval to poll for the counter value.                                                                                                                               |
| Warning Threshold | Allows you to set an optional threshold value lower than the rising threshold value and higher than the falling threshold value to generate syslogs. The range is 0–9223372036854775807. |
| Port Guard        | Specifies if the port guard is enabled or disabled. The value can be false, flap, or errordisable.<br>The default value is "false".                                                      |
| Monitor ?         | The default value is "true".                                                                                                                                                             |





## Administration

---

This section contains context-sensitive Online Help content for the **Web Client > Administration** tab.

- [DCNM Server, page 289](#)
- [Management Users, page 300](#)
- [Performance Setup, page 304](#)
- [Event Setup, page 307](#)

## DCNM Server

The DCNM Server menu includes the following submenus:

### Starting, Restarting, and Stopping Services

#### Procedure

---

- Step 1** From the menu bar, choose **Administration > DCNM Server > Server Status**.  
You see a table of services per server and the status of each as shown in the below image.
- Step 2** In the **Actions** column, use the **Start**, **Stop** or **Delete** icons to start, stop or delete any of the services. You can see the latest status in the **Status** column.
- 

### Viewing Log Information

This feature enables you to view the Cisco DCNM Web Client log. These processes have no corresponding GUI that allows you to view information about these log files. If you see errors, preserve these two files for viewing.

**Note**

Logs cannot be viewed from a remote server in a federation.

**Procedure**

- 
- Step 1** From the menu bar, choose **Administration > DCNM Server > Logs**.  
You see a tree-based list of logs in the left-hand column. Under the tree, there is a node for every server in the federation. The log files are under the corresponding server node.
- Step 2** Click a log file under each node of the tree to view it in the right-hand column.
- Step 3** Double-click the tree node for each server to download a zip file containing those log files from that server.
- Step 4** Click the **Print** icon on the upper right corner of the right-hand column to print the logs page.
- 

## Server Properties

This page allows you to set common parameters which will be populated as default values in DCNM server. Specify the parameters in the following fields according to the corresponding description.

**Procedure**

|               | Command or Action                                                                                | Purpose |
|---------------|--------------------------------------------------------------------------------------------------|---------|
| <b>Step 1</b> | From the menu bar, select <b>Administration &gt; DCNM Server &gt; Server Properties</b> .        |         |
| <b>Step 2</b> | After finishing all the property fields, click <b>Apply Changes</b> to save the server settings. |         |

## Configuring SFTP/TFTP Credentials

You can configure the SFTP/TFTP credentials for the file store.

A file server is required to collect device configuration and restoring configurations to the device.

**Procedure**

- 
- Step 1** From the menu bar, choose **Administration > DCNM Server > SFTP/TFTP Credentials**.  
You see the SFTP/TFTP credentials page.
- Step 2** In the **Server Type** field, use the radio button to select **SFTP**.
- Note** You must have a SFTP server on the DCNM server to perform backup operation. The SFTP directory must be an absolute Linux/SSH path format and must have read/write access to the SFTP User.
- a) Enter the **SFTP Username** and **SFTP Password**.



- b) Enter the **SFTP Directory path**.  
The path must be in absolute Linux path format.  
If SFTP is unavailable on your device, use external SFTP applications, such as, miniSFTP, Solarwinds, and so on. When you use an external SFTP, the you must provide the relative path in the SFTP Directory Path. For example, consider the use cases at the end of this procedure.
- c) From the **Verification Switch(es)** drop-down, select the switch.
- d) Click **Apply** to apply the configuration.
- e) Click **Verify and Apply** to verify and apply the configuration. If there are any failures during the verification, the new changes will not be stored.
- f) Click **Clear SSH Hosts** to clear SSH hosts for all switches or selected switches. If there is a failure in any of the switches, an error message is displayed. Go to **Configure > Archive > Device Configuration > Archive Jobs > Job Execution Details** page to view the number of successful and unsuccessful switches.

**Step 3** In the **Server Type** field, use the radio button to select **TFTP**.

Cisco DCNM uses an internal TFTP server for data transfer. Ensure that there is no external TFTP server running on the DCNM server.

**Note** Ensure that your switch user role includes the copy command. Operator roles will receive a *permission denied* error. You can change your credentials from the **Inventory > Discovery** page.

- a) From the **Verification Switch** drop-down, select the switch.
- b) Click **Apply** to apply the configuration.
- c) Click **Verify and Apply** to verify and apply the configuration. If there are any failures during the verification, the new changes will not be stored.

**Step 4** From the menu bar, choose **Configuration > Templates > Jobs** to view individual device verification status. The configurations that are backed up are removed from the file server and are stored in the database.

---

### Examples for SFTP Directory Path

#### Use Case 1:

If Cisco DCNM is installed on Linux platforms (OVA/ISO/Linux), and the test folder is located at `/test/sftp/`, you must provide the entire path of the SFTP directory. In the SFTP Directory field, enter `/test/sftp`.

#### Use Case 2:

If Cisco DCNM is installed on Windows platform, and the test folder is located at `C://Users/test/sftp/`, you must provide the relative path of the SFTP directory. In the SFTP Directory field, enter `/`.

For Example:

- If the path in the external SFTP is `C://Users/test/sftp/`, then the Cisco DCNM SFTP Directory path must be `/`.
- If the path in the external SFTP is `C://Users/test`, then the Cisco DCNM SFTP Directory path must be `/sftp/`.

## Modular Device Support

In order to support any new hardware which doesn't require many major changes, a patch can be delivered instead of waiting for the next DCNM release. **Modular Device Support** helps to deliver and apply the DCNM patch releases. An authorized DCNM administrator can apply the patch to the production setup. Patch releases are applicable for the following scenarios:

- Support any new hardware (Chassis or Line cards).
- Support latest NX-OS versions.
- Support critical fixes as patches.

### Procedure

- 
- Step 1** From the menu bar, choose **Administration > DCNM Server > Modular Device Support** to view the patch details.  
You see the **DCNM Servers** column on the left-hand side of the window and **Modular Device support information** window on the right-hand side.
- Step 2** You can view all the DCNM servers under the **DCNM Servers** window, as well as the list of patch installed along with the version number, corresponding platforms supported, chassis supported, NX-OS version supported, PID supported, backup directory and the last patch deployment time in the **Modular Device support information** table.
- Step 3** For more details about how to apply and rollback a patch, please go to [WWW.cisco.com/go/dcnm](http://WWW.cisco.com/go/dcnm) for more information.
- 

## Managing Switch Groups

Beginning with Cisco NX-OS Release 6.x, you can configure switch groups by using Cisco DCNM Web Client. You can add, delete, rename or move a switch to a group or move a group of switches to another group.

This section contains the following:

### Adding Switch Groups

You can add a switch group from the Cisco DCNM Web Client.

### Procedure

- 
- Step 1** From the menu bar, choose **Administration > DCNM Server > Switch Groups**.
- Step 2** Click the **Add** icon, and the **Add Group** window appears that allows you to enter the name for the switch group.
- Step 3** Enter the name of the switch group and click **Add** to complete adding the switch group.

The switch group name validation and the maximum tree depth is 10. If you do not choose a parent group before adding a new switch group, the new group is added on the top of the hierarchy

---

## Deleting a Group or a Member of a Group

You can delete group(s) and/or member(s) of a group from the Cisco DCNM Web Client. When you delete a group, the associated group(s) are deleted and the fabrics or Ethernet switches of the deleted group(s) are moved back to the default SAN or LAN.

### Procedure

---

- Step 1** Choose the switch group or member(s) of a group that you want to remove.
  - Step 2** Click the **Remove** icon or press the Delete key on your keyboard.  
A dialog box prompts you to confirm the deletion of the switch group or the member of the group.
  - Step 3** Click **Yes** to delete or **No** to cancel the action.
- 

## Moving a Switch Group to Another Group

### Procedure

---

- Step 1** Click on the switch or switch group and drag the highlighted switch or switch group to another group. To move multi devices or switches across different switch groups, you can select multiple devices using **CTRL** key or **SHIFT** key.
  - Step 2** You can see the switch or switch group Users are not allowed to move multiple items on the group level under the new group now.  
**Note** It is not allowed to move multiple items on the group level. You may not mix group with devices.
- 

## Managing Custom Port Groups

Custom port groups aids you to test the performance of the interfaces in the group. You can view the defined custom ports and their configurations from **Administration > DCNM Server > Custom Port Groups** on the Cisco DCNM Web Client.

This section includes the following topics:

### Adding Custom Port Groups

You can add a custom port group from the Cisco DCNM Web Client.

### Procedure

- 
- Step 1** From the menu bar, choose **Administration > DCNM Server > Custom Port Groups**.
  - Step 2** In the **User Defined Groups** block, click the **Add** icon.
  - Step 3** Enter the name for the custom port group in the **Add Group Dialog** window.  
Click **Add**, and a custom port group is created in the **User Defined Groups** block.
- 

## Configuring Switch and Interface to the Port Group

You can configure the custom port group to include switches and their interfaces.

### Procedure

- 
- Step 1** From the menu bar, choose **Administration > DCNM Server > Custom Port Groups**.
  - Step 2** In the **User Defined Groups** block, select the port group for which you need to add the switch and interfaces.
  - Step 3** In the **Configurations** block, click the **Add Member** icon.  
The **Port Configuration** window appears for the selected custom port group.
  - Step 4** In the **Switches** tab, select the switch that you need to include in custom port group.  
The list of available **Interfaces** appears.
  - Step 5** Select all the interfaces for which you need to check the performance.
  - Step 6** Click **Submit**.  
The list of interfaces is added to the custom port group.
- 

## Removing Port Group Member

You can remove or delete the port group member from the Custom Port group.

### Procedure

- 
- Step 1** From the menu bar, choose **Administration > DCNM Server > Custom Port Groups**.
  - Step 2** In the **User Defined Groups** block, select the port group for which you need to add the switch and interfaces.
  - Step 3** In the **Configuration** block, select the switch name and interface that must be deleted.
  - Step 4** In the **User Defined Groups** block, select the group for which you which must be deleted. Click **Remove Member** icon.  
A confirmation window appears.
  - Step 5** Click **Yes** to delete the member from the custom port group .
-

## Removing Port Group

You can remove or delete the port group from the Cisco DCNM Web Client.

### Procedure

- Step 1** From the menu bar, choose **Administration > DCNM Server > Custom Port Groups**.
- Step 2** In the **User Defined Groups** block, select the group which must be deleted. Click **Remove** icon. A confirmation window appears.
- Step 3** Click **Yes** to delete the custom group.

## Managing Licenses

This section includes the following topics:

### Viewing Licenses Using the Cisco DCNM Wizard

You can view the existing Cisco DCNM licenses by selecting **Administration > DCNM Server > License**.

**Note**

By default, the **License Assignments** tab appears.

#### License Assignments

The following table displays the **License Assignments** for every switch.

| Field                 | Description                                                               |
|-----------------------|---------------------------------------------------------------------------|
| <b>Group</b>          | Displays if it is a fabric or LAN group.                                  |
| <b>Switch Name</b>    | Displays the name of the switch.                                          |
| <b>WWN/Chassis ID</b> | Displays the World Wide Name or Chassis ID.                               |
| <b>Model</b>          | Displays the model of the device. For example, DS-C9124 or N5K-C5020P-BF. |

| Field                   | Description                                                                                                                                                                                                                                    |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>License State</b>    | Displays the license state of the switch that can be one of the following: <ul style="list-style-type: none"> <li>• Permanent</li> <li>• Eval</li> <li>• Unlicensed</li> <li>• Not Applicable</li> <li>• Expired</li> <li>• Invalid</li> </ul> |
| <b>License Type</b>     | Displays if the license is a switch-based embedded license or a server-based license.                                                                                                                                                          |
| <b>Eval Expiration</b>  | Displays the expiry date of the license.<br><b>Note</b> Text in the eval expiration field will be in Red for licenses that expires in seven days.                                                                                              |
| <b>Assign License</b>   | Select a row and click this option on the tool bar to assign the license.                                                                                                                                                                      |
| <b>Unassign License</b> | Select a row and click this option on the tool bar to unassign the license.                                                                                                                                                                    |
| <b>Assign All</b>       | Click on this option on the tool bar to refresh the table and assign the licenses for all the items in the table.                                                                                                                              |
| <b>Unassign All</b>     | Click on this option on the tool bar to refresh the table and unassign all the licenses.                                                                                                                                                       |

### Server License Files

The following table displays the Cisco DCNM server license fields.

| Field                   | Description                                                                                                                                       |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Filename</b>         | Specifies the license file name.                                                                                                                  |
| <b>Feature</b>          | Specifies the licensed feature.                                                                                                                   |
| <b>PID</b>              | Specifies the product ID.                                                                                                                         |
| <b>SAN (Free/Total)</b> | Display the number of free versus total licenses for SAN.                                                                                         |
| <b>LAN (Free/Total)</b> | Display the number of free versus total licenses for LAN.                                                                                         |
| <b>Eval Expiration</b>  | Displays the expiry date of the license.<br><b>Note</b> Text in the eval expiration field will be in Red for licenses that expires in seven days. |

## Automatic License Assignment

When the fabric is first discovered if the switch does not have a valid switch-based license, a license is automatically assigned to the fabric from the file license pool until no more licenses are left in the pool. Also, if you have an existing fabric and a new switch is added to the fabric, the new switch will be assigned a license if one is available in the file license pool and if it does not already have a switch-based license.

## Adding Cisco DCNM Licenses

You must have network administrator privileges to complete the following procedure.

### Procedure

- 
- Step 1** Choose **Administration > DCNM Server > License** to start the license wizard.
- Step 2** Choose the **Server License Files** tab.  
The valid Cisco DCNM-LAN and DCNM-SAN license files appears.  
Ensure that the security agent is disabled when you load licenses.
- Step 3** Download the license pack file that you received from Cisco into a directory on the local system.
- Step 4** Click **Add License File** and then select the license pack file that you saved on the local machine.  
The file will be uploaded to the server machine, saved into the server license directory and then loaded on to the server.
- Note** Ensure that you do not edit the contents of the .lic file or the Cisco DCNM software ignores any features that are associated with that license file. The contents of the file are signed and must remain intact. When you accidentally copy, rename, or insert the license file multiple times, the duplicate files are ignored, but the original will be counted.
- 

## Assigning Licenses

### Before You Begin

You must have network administrator privileges to complete the following procedure.

### Procedure

- 
- Step 1** Choose **Administration > DCNM Server > License** to start the license wizard.  
The licenses table appears.
- Step 2** From the table, choose the switch that you want to assign the license to.
- Step 3** Click **Assign License**.
-

## Unassigning Licenses to a Switch

### Before You Begin

You must have network administrator privileges to complete the following procedure.

### Procedure

- 
- Step 1** Choose **Administration > DCNM Server > License** to start the license wizard.  
The licenses table appears.
- Step 2** From the table, choose the switch that you want to unassign the license.
- Step 3** Click **Unassign License**.
- 

## Viewing Server Federation

### Procedure

- 
- Step 1** From the menu bar, choose **Administration > DCNM Server > Federation**.  
The list of **Servers** along with its **Status**, **Location**, **Local Time** and **Data Sources** are displayed.
- Step 2** Use the **Enable Automatic Failover** checkbox to turn on/off the failover functionality.
- Step 3** In the **Location** column, double-click to edit the location.  
If the status of one of the servers in the federation is **Inactive**, then some functionality may not work unless the server status changes to **Active** in the federation.
- Note** Before upgrading Cisco DCNM, ensure that **Enable Automatic Failover** is unchecked. Otherwise, if one server within the federation is down, the devices discovered by the server will be moved to the other DCNM server which comes up first after upgrade. To prevent the auto move for DCNM upgrade, you need to disable the auto move on all DCNMs within the federation, and then upgrade the DCNM server one by one. Only after all the DCNMs upgrade successfully and run normally, then enable the auto move again.
- Note** In DCNM Federation with Auto Move enabled, when a DCNM is down, the devices under its management will be moved to other DCNM's. However after the DCNM is back, the devices won't move back.
- 

## Native HA

### Procedure

- 
- Step 1** By default, DCNM is bundled with an embedded database engine PostgreSQL. The native DCNM HA is achieved by two DCNM's running as **Active / Warm Standby**, with their embedded databases synchronized



in real time. So once the active DCNM is down, the standby will take over with the same database data and resume the operation. The *standby host database down* scenario is documented after this procedure.

- Step 2** From the menu bar, choose **Administration > DCNM Server > Native HA**.  
You see the **Native HA** window.
- Step 3** You can allow manual failover of DCNM to the standby host by clicking the **Failover** button, and then click **OK**.
- Alternatively, you can initiate this action from the Linux console.
    - 1 ssh into the DCNM active host.
    - 2 Enter " " /usr/share/heartbeat/hb\_standby"
- Step 4** You can allow manual syncing database and disk files to standby host by clicking **Force Sync** button, and then click **OK**.
- Step 5** You can test or validate the HA setup by clicking **Test** and then click **OK**.
- 

### What to Do Next

Some HA troubleshooting scenarios are noted in this sub section.

**The standby host database is down**--Typically, the DCNM database (PostgreSQL) is up on the active and standby hosts. In DCNM 10.1 and earlier versions, the standby database can be down due to a database synchronization failure.

- Enter "ps -ef | grep post". You should see multiple postgres processes running. If not, it indicates that the database is down.
- Restore database data from a backup file that is created at the beginning of database synchronization. Change directory to "/usr/local/cisco/dcm/db"
- Check existence of file replication/ pgsql-standby-backup.tgz. If the file exists, restore database data files:

```
rm -rf data/*
tar -zxvf replication/ pgsql-standby-backup.tgz data
/etc/init.d/postgresql-9.4 start
ps -ef | grep post
```

The active DCNM host will synchronize the two databases.

**The TFTP server is not bound to the eth1 VIP address on the active host**--The TFTP server should run on the active host (not on the standby host), and it should be bound to the eth1 VIP address. In some setups, the bind address is not the VIP address, as per the TFTP configuration file, and this could cause issues when switches try to use TFTP.

- Enter "grep bind /etc/xinetd.d/tftp" to check if the TFTP configuration file has the right bind address. If the displayed IP address is not the eth1 VIP address, then change the bind address to the VIP address. Repeat the procedure for the standby host. Update the bind address to the VIP address.
- Enter " " /etc/init.d/xinetd restart" on the active host to restart TFTP.

**Note**

The TFTP server can be started or stopped with the “appmgr start/stop ha-apps” command.

## Multi Site Manager

### Procedure

- 
- Step 1** Multi-Site-Manager (MsM) provides a single pane for customer to globally search for switches managed by DCNM. MSM can do realtime search to find out which switch globally handle the traffic for a given virtual machine base on IP address, name or mac address, and supporting VXLAN basing on segment ID as well. It provides hyperlink to launch the switch only. This window also plays the role of remote site registration. The registration only allows the current DCNM server to access the remote DCNM server/site. For the remote site to access the current DCNM server, registration is required on the remote site as well.
- Step 2** From the menu bar, choose **Administration > DCNM Server > Multi Site Manager**. The MsM window displays the overall health/status of the remote site and the application health.
- Step 3** You can search by **Switch, VM IP, VM Name, MAC and Segment ID**.
- Step 4** You can add new DCNM server by clicking **+Add DCNM Server**. The **Enter Remote DCNM Server Information** window opens. Fill in the information required and click **OK** to save.
- Step 5** Click **Refresh All Sites** to display the updated information.
- 

## Management Users

The Management Users menu includes the following submenus:

## Remote AAA

### Procedure

- 
- Step 1** From the menu bar, choose **Administration > Management Users > Remote AAA Properties**. The AAA properties configuration page appears.
- Step 2** Use the radio button to select one of the following authentication modes:
- **Local** ☐ In this mode the authentication will authenticate with the local server.
  - **Radius** ☐ In this mode the authentication will authenticate against the Radius servers specified.
  - **TACACS+** ☐ In this mode the authentication will authenticate against the TACAS servers specified.
  - **Switch** ☐ In this mode the authentication will authenticate against the switches specified.
  - **LDAP** ☐ In this mode the authentication will authenticate against the LDAP server specified.

**Step 3** Click **Apply**.

**Note** You must restart the Cisco DCNM SAN services if you update the Remote AAA properties. You must restart all the instances of Cisco DCNM if federation is deployed.

---

## Local

### Procedure

---

**Step 1** Use the radio button and select **Local** as the authentication mode.

**Step 2** Click **Apply** to confirm the authentication mode.

---

## Radius

### Procedure

---

**Step 1** Use the radio button and select **Radius** as the authentication mode.

**Step 2** Specify the Primary server details and click **Test** to test the server.

**Step 3** (Optional) Specify the Secondary and Tertiary server details and click **Test** to test the server.

**Step 4** Click **Apply** to confirm the authentication mode.

---

## TACACS+

### Procedure

---

**Step 1** Use the radio button and select **TACACS+** as the authentication mode.

**Step 2** Specify the Primary server details and click **Test** to test the server.

**Step 3** (Optional) Specify the Secondary and Tertiary server details and click **Test** to test the server.

**Step 4** Click **Apply** to confirm the authentication mode.

---

## Switch

### Procedure

- 
- Step 1** Use the radio button to select **Switch** as the authentication mode.  
DCNM also supports LAN switches with IPv6 management interface.
  - Step 2** Specify the Primary Switch name and click **Apply** to confirm the authentication mode.
  - Step 3** (Optional) Specify the Secondary and Tertiary Switch name and click **Apply** to confirm the authentication mode.
- 

## LDAP

### Procedure

- 
- Step 1** Use the radio button and select **LDAP** as the authentication mode.
  - Step 2** In the **Host** field, enter DNS address of the host.
  - Step 3** Click **Test** to test the AAA server. The **Test AAA Server** window pops out.
  - Step 4** Enter a valid **Username** and **Password** in the **Test AAA Server** window.  
A dialog box appears confirming the status of the AAA server test. If the test has failed, the **LDAP Authentication Failed** dialog box appears.
  - Step 5** In the **Port** field, enter a port number.
  - Step 6** (Optional) Select the **SSL Enabled** check box, if SSL is enabled on the AAA server.
  - Step 7** In the **Base DN** field, enter the base domain name.
  - Step 8** In the **Filter** field, specify the filter parameters.
  - Step 9** Choose an option to determine a role by either **Attribute** or **Admin Group Map**.
  - Step 10** In the **Role Admin Group** field, enter the name of the role.
  - Step 11** In the **Map to DCNM Role** field, enter the name of the role to be mapped.
  - Step 12** In the **Access Map** field, enter the Role Based Access Control (RBAC) group to be mapped.
  - Step 13** Click Apply Changes icon on the upper right corner to apply the LDAP configuration.
- 

## Managing Local Users

As an admin user, you can use Cisco DCNM Web Client to create a new user, assign the role and associate one or more groups or scope for the user.

This section contains the following:

## Adding Local Users

### Procedure

- 
- Step 1** From the menu bar, choose **Administration > Management Users > Local**. You see the **Local Users** page.
- Step 2** Click **Add User**.  
You see the **Add User** dialog box.
- Step 3** Enter the username in the **User name** field.  
**Note** The username guest is a reserved name (case insensitive). The guest user can only view reports. The guest user cannot change the guest password, or access the Admin options in DCNM Web Client.
- Step 4** From the **Role** drop-down list, select a role for the user.
- Step 5** In the **Password** field, enter the password.
- Step 6** In the **Confirm Password** field, enter the password again.
- Step 7** Click **Add** to add the user to the database.
- Step 8** Repeat Steps 2 through 7 to continue adding users.
- 

## Deleting Local Users

### Procedure

- 
- Step 1** From the menu bar, choose **Administration > Management Users > Local**. You see the **Local Users** page.
- Step 2** Select one or more users from the **Local Users** table and click the **Delete User** button.
- Step 3** Click **Yes** on the warning window to delete the local user. Or click **No** to cancel deletion.
- 

## Editing a User

### Procedure

- 
- Step 1** From the menu bar, choose **Administration > Management Users > Local**.
- Step 2** Use the checkbox to select a user and click the **Edit User** icon.
- Step 3** In the **Edit User** window, the **User Name** and **Role** is mentioned by default. Specify the **Password** and **Confirm Password**.
- Step 4** Click **Apply** to save the changes.
-

## User Access

You can control the local users to access the specific groups on this page.

### Procedure

- 
- Step 1** From the menu bar, choose **Administration > Management Users > Local**. You see the **Local Users** page.
  - Step 2** Select one user from the **Local Users** table. Click **User Access**.  
You see the **User Access** selection window.
  - Step 3** Select the groups allowed to access for the user and click **Apply**.
- 

## Managing Clients

You can use the DCNM Web Client to disconnect DCNM Client Servers.

### Procedure

- 
- Step 1** From the menu bar, click **Administration > Management Users > Clients**.  
A list of DCNM Servers are displayed.
  - Step 2** Use the check box to select a DCNM server and click **Disconnect Client** icon to disconnect the DCNM server.  
**Note** You cannot disconnect a current client session.
- 

## Performance Setup

The Performance Setup menu includes the following submenus:

### Performance Setup LAN Collections

If you are managing your switches with the Performance Manager, you must set up an initial set of flows and collections on the switch. You can use Cisco DCNM Web Client to add and remove performance collections. The switch has to be licensed and in the **Managed Continuously** state before a collection for the switch can be created.

To add a collection follow these steps:

### Procedure

---

- Step 1** From the menu bar, click **Administration > Performance Setup > LAN Collections**.
  - Step 2** For all the licensed LAN switches, use the checkboxes to enable performance data collection for **Trunks**, **Access**, **Errors & Discards**, and **Temperature Sensor**.
  - Step 3** Use the checkboxes to select the type(s) of LAN switches for which you want to collect performance data.
  - Step 4** Click **Apply** to save the configuration.
  - Step 5** In the confirmation dialog box, click **Yes** to restart the performance collector.
- 

## Performance Manager SAN Collections

If you are managing your switches with the Performance Manager, you must set up an initial set of flows and collections on the switch. You can use Cisco DCNM Web Client to add and remove performance collections. The switch has to be licensed and in the Managed Continuously state before a collection for the switch can be created.

To add a collection follow these steps:

### Procedure

---

- Step 1** From the menu bar, click **Administration > Performance Setup > SAN Collections**.
  - Step 2** Select a fabric and select the **Name**, **ISL/NPV Links**, **Hosts**, **Storage**, **FC Flows** and **FC Ethernet** to enable performance collection for these data types.
  - Step 3** Click **Apply** to save the configuration.
  - Step 4** In the confirmation dialog box, click **Yes** to restart the performance collector.
- 

## Performance Setup Thresholds

If you are managing your switches with the Performance Manager, you must set up an initial set of flows and collections on the switch. You can use Cisco DCNM Web Client to add and remove performance collections. The switch has to be licensed and in the **Managed Continuously** state before a collection for the switch can be created.

### Procedure

---

- Step 1** From the menu bar, click **Administration > Performance Setup > Thresholds**.
- Step 2** Under **Generate a threshold event when traffic exceeds % of capacity**, use the checkbox to specify the **Critical at** and **Warning at** values. The range for **Critical at** is from 5 to 95, and the default is 80. The range

for **Warning at** is from 5 to 95, and the default is 60. User can also use the **For ISL/Trunk Only** checkbox to limit the threshold events generated to ISL and Trunk events only and then click Apply.

---

## Configuring the RRD Database

Configuring the Round Robin Database (RRD) allows you to set the intervals at which data samples are collected. After applying the configuration, the database storage format is converted to a new format at those intervals. Because database formats are incompatible with each other, you must copy the old data (before the conversion) to the \$INSTALLDIR/pm directory. See the [Importing the RRD Statistics Index](#) , on page 307.

### Procedure

---

- Step 1** From the menu bar, choose **Administration > Performance Setup > Database**.  
You see the Performance Database (collection interval) page.
- Step 2** In the top row of the **Days** column, enter the number of days to collect samples at 5-minute intervals.
- Step 3** In the second row of the **Days** column, enter the number of days to collect samples at 30-minute intervals.
- Step 4** In the third row of the **Days** column, enter the number of days to collect samples at 2-hour intervals.
- Step 5** In the bottom row of the **Days** column, enter the number of days to collect samples at 1-day intervals.  
As of Cisco SAN-OS Release 3.1(1) and later releases, you can configure the sampling interval for ISLs. Select a sampling interval from the ISLs drop-down list.
- Step 6** Click **Apply** to apply your changes, or click **Defaults** to reset the file sizes to the default values.  
If you are applying new values, or if the current values are not the default values, you see a message indicating that the conversion of the RRD files take a certain amount of time and that the database is unavailable until then. The time it takes depends on the difference between the old and new values.
- Note** The system allows you to convert data, one process at a time. When you start converting the data, the **Apply** and **Defaults** buttons change to **Refresh** and **Cancel** so that another process cannot be inadvertently started. The display is the same for all browsers that access the server during this time. Click **Refresh** to view the latest progress. Click **Cancel** to cancel the process of converting the data. If the job is successfully canceled, you see the **Apply** and **Defaults** buttons again. If the cancel job is not successful, you see a message indicating that the cancellation has failed.  
If you want to perform this procedure, perform it before collecting a lot of data because data conversion can take a long time.
-



## Importing the RRD Statistics Index

### Procedure

- 
- Step 1** Stop Cisco DCNM-SAN Server.
  - Step 2** Copy the original RRD file into \$INSTALLDIR/pm/db.
  - Step 3** Run \$INSTALLDIR/bin/pm.bat s.
  - Step 4** Restart Cisco DCNM-SAN and add the fabric.
- 

## Configuring User Defined Statistics

### Procedure

- 
- Step 1** From the menu bar, choose **Administration > Performance Setup > User Defined**.  
You see the User Defined page.
  - Step 2** Click **Add** icon.  
You see the **Add SNMP Statistic to Performance Collection** dialog box.
  - Step 3** From the **Switch** table, select the switch for which you want to add other statistics.
  - Step 4** From the **SNMP OID** drop-down list, select the OID.  
**Note** For SNMP OID ModuleX\_Temp,IFHCInOctets.IFINDEX,IFHCOutOctets.IFINDEX, selected from drop down box, you must replace 'X' with correct module number or the corresponding IFINDEX.
  - Step 5** In the **Display Name** box, enter a new name.
  - Step 6** From the **SNMP Type** drop-down list, select the type.
  - Step 7** Click **Add** to add this statistic.
- 

## Event Setup

The Event Setup menu includes the following submenus:

## Viewing Events Registration

To enable **Send Syslog**, **Send Traps** and **Delayed Traps** you need to configure the following in the DCNM-SAN client:

- Enabling **Send Syslog** — Log into the DCNM-SAN client. In the **Physical Attributes** pane, Select **Events > Syslog > Servers**. Click the **Create Row** icon, provide the required details and click **Create**.

- Enabling **Send Traps** — Log into the DCNM-SAN client. In the **Physical Attributes** pane, Select **Events > SNMP Traps > Destination**. Click the **Create Row** icon, provide the required details and click Create.
- Enabling **Delayed Traps** — Log into the DCNM-SAN client. In the **Physical Attributes** pane, Select **Events > SNMP Traps > Delayed Traps**. In the **Feature Enable** column, use the checkboxes to enable delayed traps for the switch and specify the delay in minutes.

### Procedure

- 
- Step 1** From the menu bar, choose **Administration > Event Setup > Registration**.  
The SNMP and Syslog receivers along with the statistics information are displayed.
- Step 2** Select **Enable Syslog Receiver** checkbox and click **Apply** to enable the syslog receiver if it is disabled in the server property.  
To configure the Event Registration/Syslog properties, select **Administration > DCNM Server > Server Properties** and follow the on-screen instructions.
- Step 3** Select **Copy Syslog Messages to DB** and click **Apply** to copy the syslog messages to the database.  
If this option is not select, the events will not be displayed in the events page of the Web client.  
The columns in the second table displays the following:
- Switches sending traps
  - Switches sending syslog
  - Switches sending syslog accounting
  - Switches sending delayed traps
- 

## Notification Forwarding

You can use Cisco DCNM Web Client to add and remove notification forwarding for system messages.

This section contains the following:

### Adding Notification Forwarding

You can use Cisco DCNM Web Client to add and remove notification forwarding for system messages.

Cisco DCNM Web Client forwards fabric events through e-mail or SNMPv1 traps.



#### Note

Test forwarding will only work for the licensed fabrics.

## Procedure

- Step 1** From the menu bar, choose **Administration > Event Setup > Forwarding**.
- Step 2** The events forwarding scope, the recipient email address, severity of the event and type of the event is displayed. The description Regex field is applicable only when the forwarding source is selected as Syslog while adding the events forwarder.
- Step 3** Check the **Enable** checkbox to enable events forwarding.
- Step 4** Specify the **SMTP Server** details and the **From** e-mail address.
- Step 5** Click **Apply** to save the configuration, or in the **Apply and Test** icon, use the drop-down to select the fabric and click **Apply and Test** to save and test the configuration.
- Step 6** In the **Event Count Filter**, you can add a filter for event count to event forwarder. The forwarding will stop forwarding an event if the event count exceeds the limit specified by the event count filter. In this field you can specify a count limit. Before an event can be forwarded, the Cisco DCNM will check if its occurrence exceeds the count limit. If it does, the event will not be forwarded.
- Step 7** Select the **Snooze** checkbox and specify the **Start** date and time and the **End** date and time. Click **Apply** to save the configuration.
- Step 8** Under the **Event Forwarder Rules** table, click the + icon to add an event forwarder rule. You see the **Add Event Forwarder Rule** dialog box.
- Step 9** In the **Forwarding Method**, choose either **E-Mail** or **Trap**. If you choose **Trap**, a **Port** field is added to the dialog box.
- Step 10** If you choose the **E-mail** forwarding method, enter the IP address in the **Email Address** field. If you choose the **Trap** method, enter the trap receiver IP address in the **Address** field and specify the port number.
- Step 11** For **Forwarding Scope**, choose the **Fabric/LAN** or **Port Groups** for notification.
- Step 12** In the **Source** field select **DCNM** or **Syslog**.  
If you select **DCNM**, then:
  - a) From the **Type** drop-down list, choose an event type.
  - b) Check the **Storage Ports Only** check box to select only the storage ports.
  - c) From the **Minimum Severity** drop-down list, select the severity level of the messages to receive.
  - d) Click **Add** to add the notification.
 If you select **Syslog**, then:
  - a) In the **Facility** list, select the syslog facility.
  - b) Specify the syslog **Type**.
  - c) In the **Description Regex** field, specify a description that needs to be matched with the event description.
  - d) From the **Minimum Severity** drop-down list, select the severity level of the messages to receive.
  - e) Click **Add** to add the notification.

**Note** The **Minimum Severity** option is available only if the **Event Type** is set to **All**.

The traps sent by Cisco DCNM correspond to the severity type followed by a text description:

```
trap type(s) = 40990 (emergency)
40991 (alert)
40992 (critical)
40993 (error)
40994 (warning)
40995 (notice)
40996 (info)
```

```
40997 (debug)
textDescriptionOid = 1, 3, 6, 1, 4, 1, 9, 9, 40999, 1, 1, 3, 0
```

---

## Removing Notification Forwarding

You can remove notification forwarding.

### Procedure

---

- Step 1** From the menu bar, choose **Administration > Event Setup > Forwarding**.
  - Step 2** Select the check box in front of the notification that you want to remove and click the **Delete** icon.
- 

## Configuring EMC CallHome

Cisco DCNM Release 7.1.x DCNM enhances EMC call home messages. DCNM version information is displayed in with the call home message.

You can configure **EMC Call Home** from the Cisco DCNM Web Client for EMC supported SAN switches.

### Procedure

---

- Step 1** From the menu bar, choose **Administration > Event Setup > EMC Call Home**.
  - Step 2** Select the **Enable** check box to enable this feature.
  - Step 3** Use the check box to select the fabrics or individual switches.
  - Step 4** Enter the general e-mail information.
  - Step 5** Click the **Apply** to update the e-mail options.
  - Step 6** Click **Apply and Test** to update the e-mail options and test the results.
- 

## Event Suppression

Cisco DCNM allows you to suppress the specified events based on the user-specified suppressor rules. Such events will not be displayed on the Cisco DCNM Web Client and SAN Client. The events will neither be persisted to DCNM database, nor forwarded via email/SNMP trap.

You can view, add, modify and delete suppressor rules from the table. You can create a suppressor rule from the existing event table. Select a given event as the template, and invoke the rule dialog window. Event details are automatically ported from the selected event in the event table to the input fields of the rule creation dialog window.

This section includes the following:

## Add Event Suppression Rules

To add rules to the Event Suppression, do the following tasks:

### Procedure

- 
- Step 1** From the menu bar, select **Administration > Event Setup > Suppression**.
- Step 2** Click the **Add** icon above the **Event Suppressors** table.
- Step 3** In the **Add Event Suppressor Rule** window, specify the **Name** for the rule.
- Step 4** Select the required **Scope** for the rule based on the event source.  
In the Scope drop-down list, the LAN groups and the port groups are listed separately. You can choose **SAN**, **LAN**, **Port Groups** or **Any**. For **SAN** and **LAN**, select the scope of the event at the Fabric or Group or Switch level. User can only select group(s) for **Port Group** scope. If use selects **Any** as the scope, the suppressor rule will be applied globally.
- Step 5** Enter the **Facility** name or choose from the **SAN/LAN Switch Event Facility** List.  
If you do not specify a facility, wild card will be applied.
- Step 6** From the drop down list, select the Event **Type**.  
If you do not specify the event type, wild card will be applied.
- Step 7** In the **Description Matching** field, specify a matching string or regular expression.  
The rule matching engine uses regular expression supported by Java Pattern class to find a match against an event description text.
- Step 8** (Optional) Check the **Active Between** box and select a valid time range during which the event will be suppressed.  
By default, the time range is not enabled, i.e., the rule will be always active.
- Note** In general, user should not suppress accounting events. Suppressor rule for Accounting events might be created only for certain rare situations where Accounting events are generated by actions of DCNM or switch software. For example, lots of 'sync-snmp-password' AAA syslog events are automatically generated during password synchronization between DCNM and managed switches. To suppress Accounting events, user can browse web client to Suppressor table and invoke **Add Event Suppressor Rule** dialog window.
- Note** You can go to **Monitor > Switch > Events** table of Web Client to create a suppressor rule for a known event. While there is no such shortcut to create suppressor rules for Accounting events.
- 

## Delete Event Suppression Rule

To delete event suppressor rules, do the following tasks:

### Procedure

---

- Step 1** From the menu bar, select **Administration > Event Setup > Suppression**.
- Step 2** Select the rule from the list and click **Delete** icon.
- Step 3** Click **Yes** to confirm.
- 

## Modify Event Suppression Rule

To modify the event suppressor rules, do the following tasks:

### Procedure

---

- Step 1** From the menu bar, select **Administration > Event Setup > Suppression**.
- Step 2** Select the rule from the list and click **Edit** icon.  
You can edit the **Facility**, **Type**, **Description Matching** string, and the **Valid time range**.
- Step 3** Click **Apply** to save the changes,
-



## Preview Features

---

- [Preview Features](#) , page 313

## Preview Features

In the DCNM 10.4.2 release, the following two features have been introduced as previews for LAN deployments.

The concept of preview features is to get early feedback from customers for subsequent integration into the General Availability (GA) release. Note that preview features have not been qualified for any scaled environments.

- Compute Visibility with VMware vSphere Virtual Center (vCenter)
- Environmental Metrics visibility via streaming telemetry



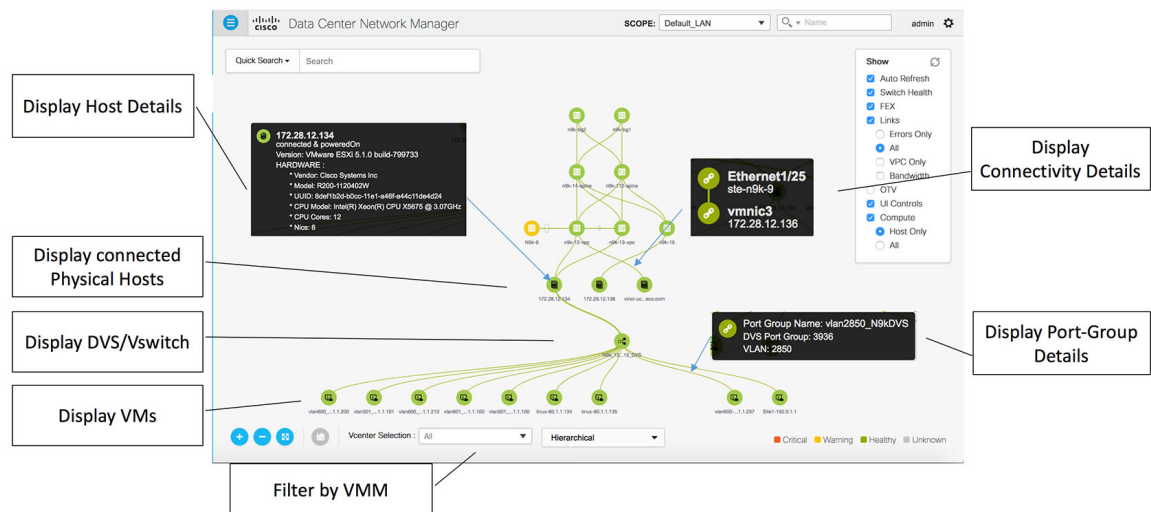
### Note

These features are only available in the OVA form factor for DCNM 10.4.2. The installer options in which these features are supported are (1) VXLAN Fabric (2) LAN, SAN, Auto-Config

This section contains the following topics:

## Compute Visibility

In virtualized environments, any kind of troubleshooting begins with identifying the network attachment point for the virtual machines in question. This means a quick determination of the server, virtual switch, port-group, VLAN, associated network switch and physical port is critical. This may require multiple touch points and interactions between the server and network administrator as well as reference to multiple tools (compute orchestrator, compute manager, network manager, network controller etc.).

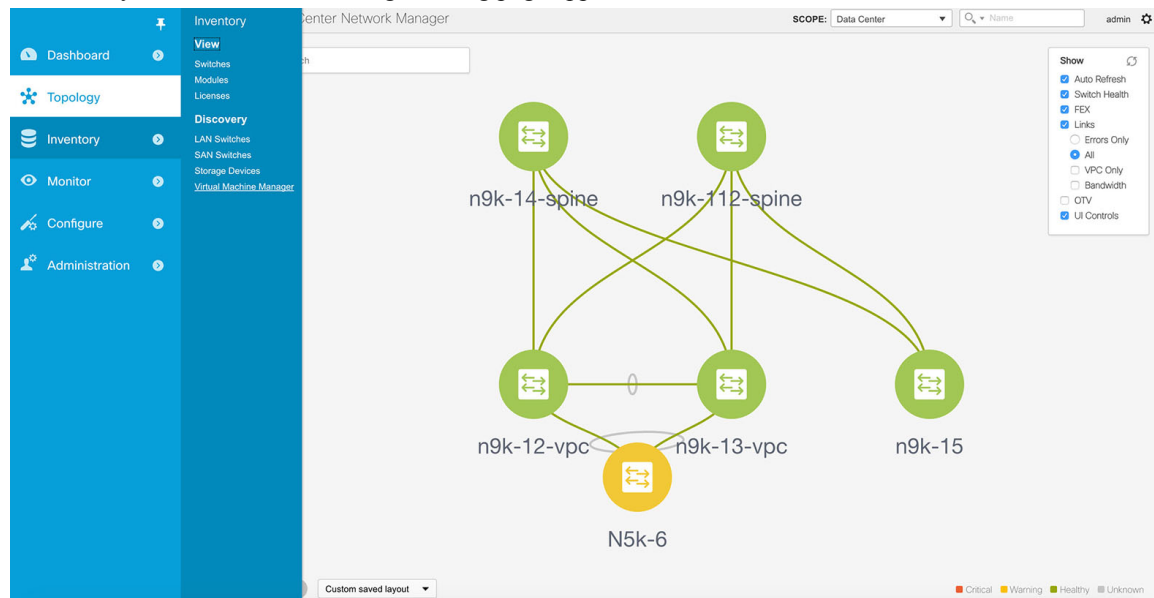


The compute visibility preview feature added in DCNM 10.4.2 strives to provide a single pane of glass that provides the entire attachment path from the end-host all the way up to the network switch. The current DCNM network topology view has been enhanced to optionally display the associated compute nodes including virtualized servers, virtual switches, and virtual machines. Fabric level scope select filters the view to only display compute resources associated with the selected group of switches. This feature is targeted for VMware vSphere vCenter environments.

## Enabling the Compute Visibility Feature

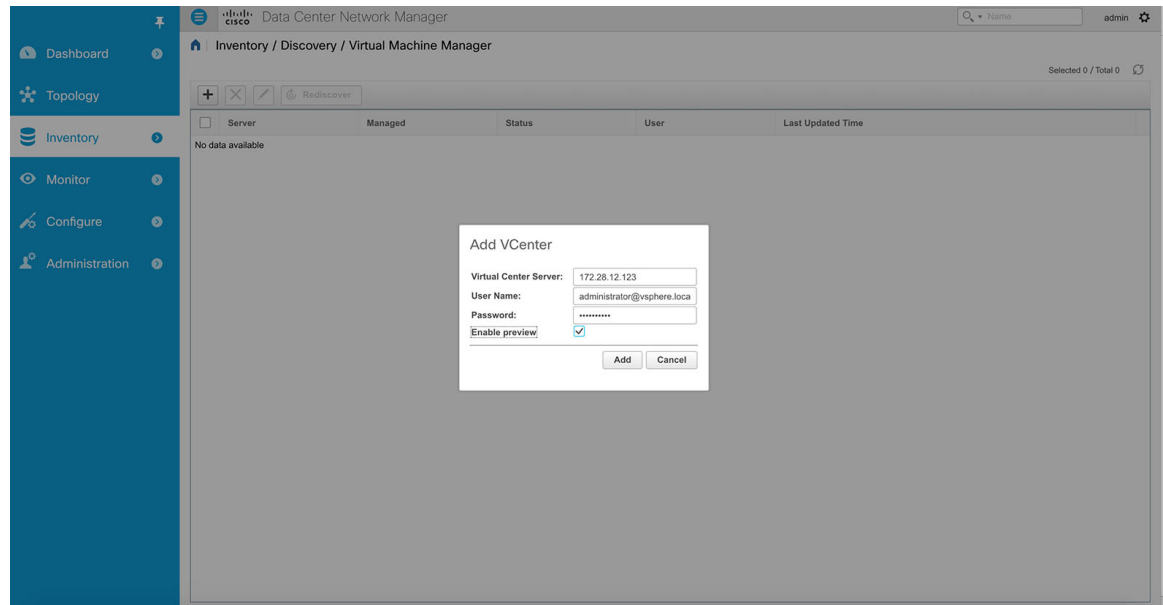
### Procedure

**Step 1** From Cisco DCNM Web Client, choose **Configure > Inventory > Virtual Machine Manager**. The Inventory / Discovery / Virtual Machine Manager listing page appears.



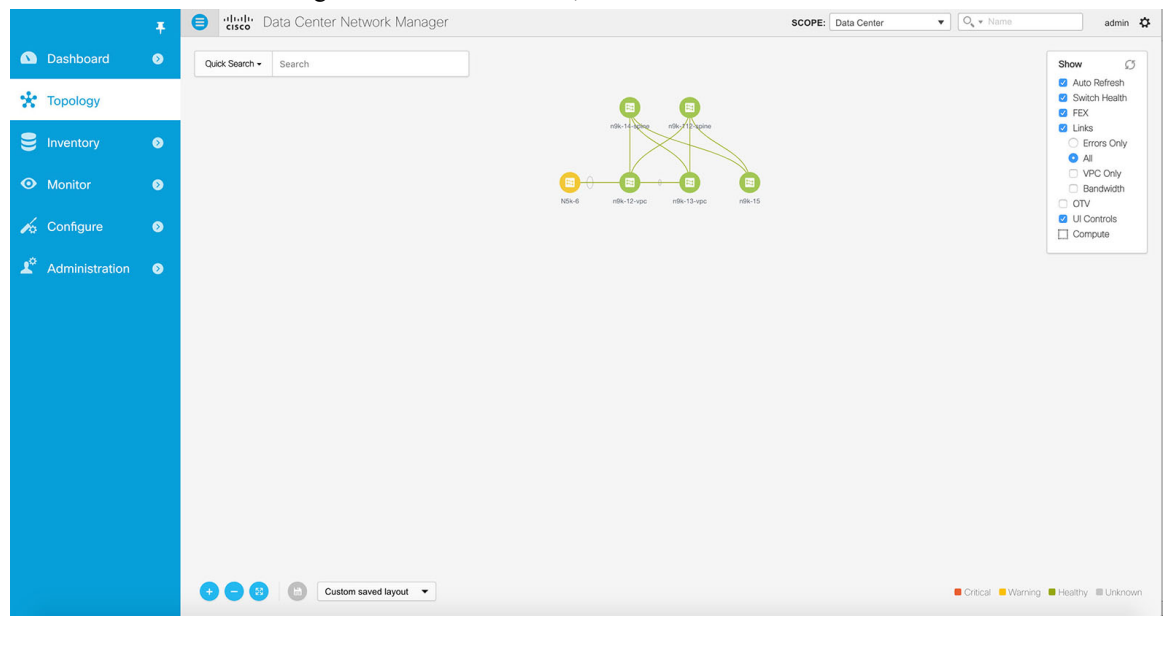


**Step 2** Click the + button to add a new VMware vSphere vCenter.



**Step 3** Add details of the vCenter including its hostname or IP address, and credentials. Please check the button that says “Enable preview”. This will enable the compute visibility preview feature (vCenter version required is 5.5 or higher).

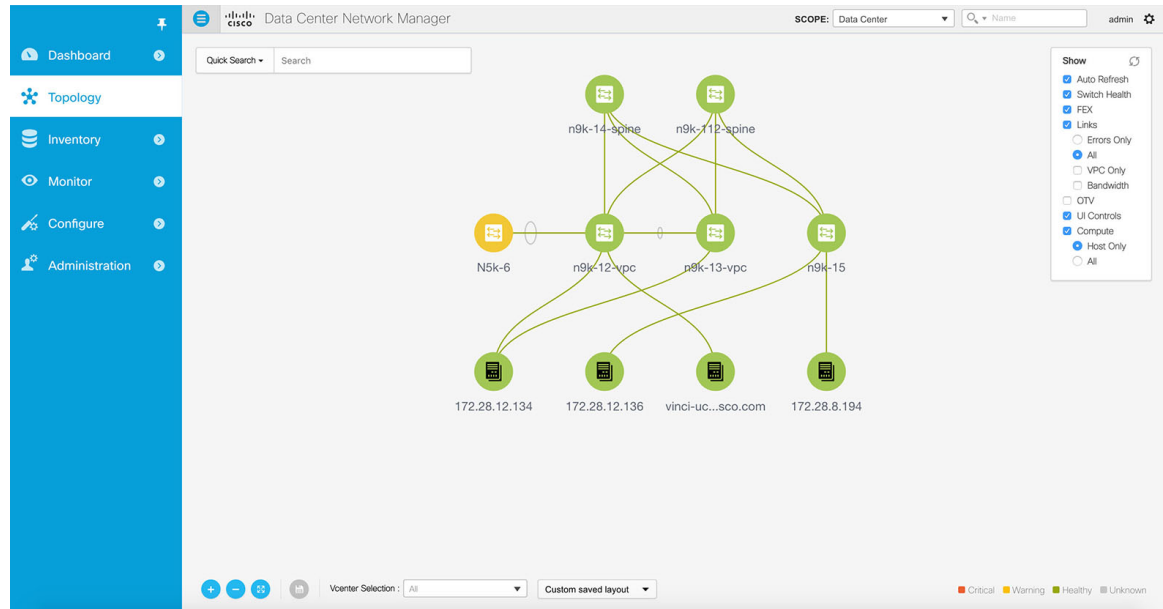
**Step 4** After initial discovery, which will take a couple of minutes, the information received from vCenter will be appropriately organized and available on the main topology screen. An additional menu item labelled “Compute” will become visible on the right hand selection menu, as shown below.



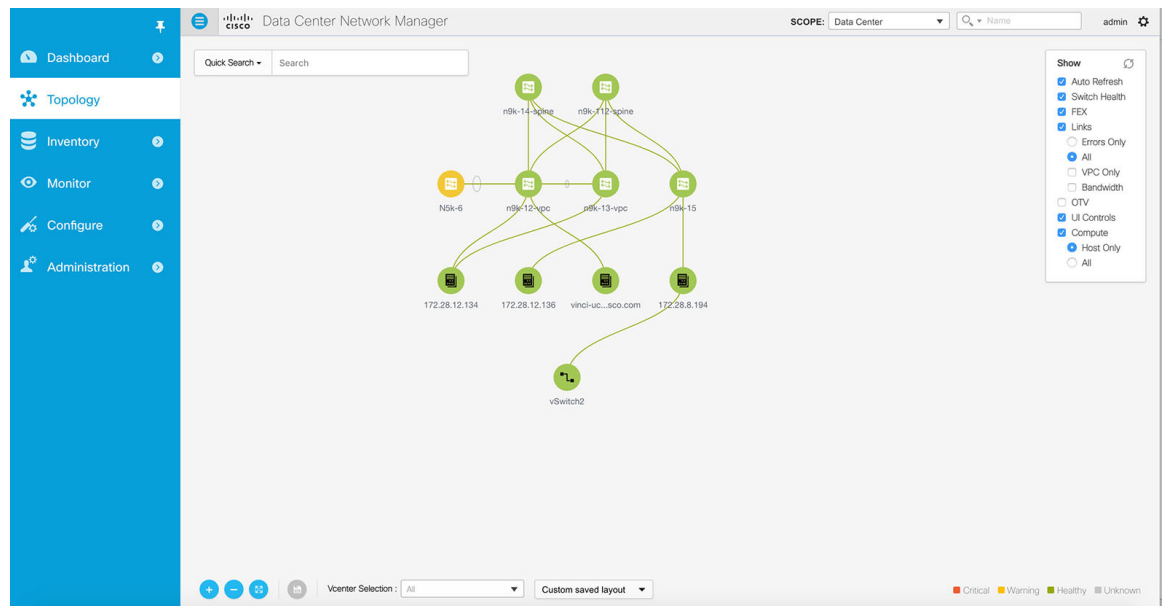
## Using the Compute Visibility Feature

### Procedure

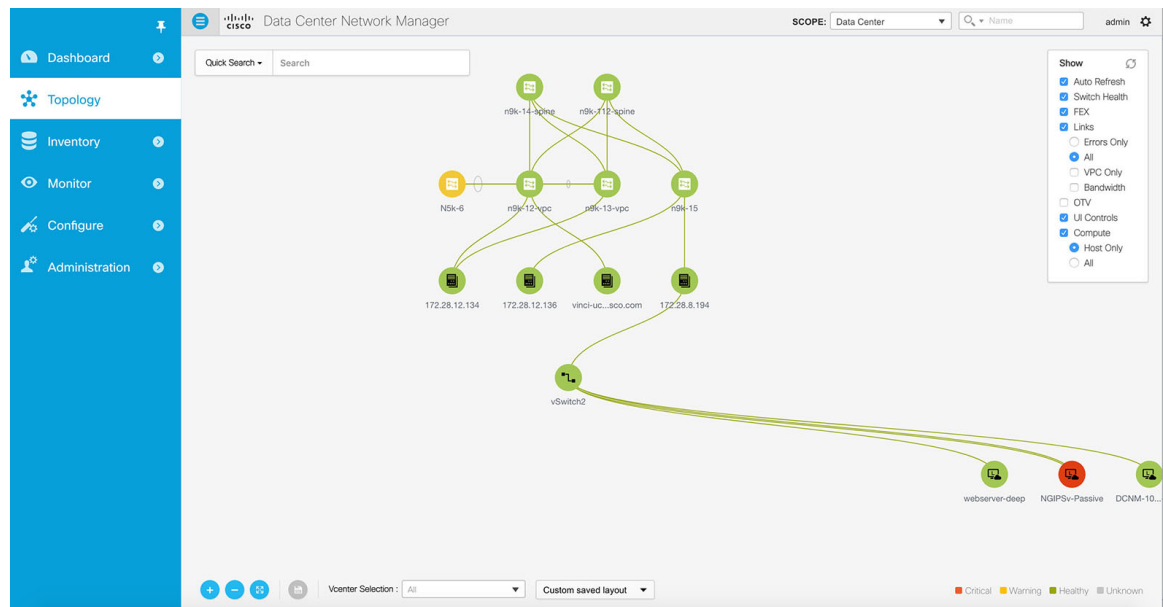
- Step 1** In order to enable the Compute visibility, the topology view must have selected the respective topology SCOPE. Once the Compute option in the topology view menu is checked, you have enabled the compute visibility. By default the “Host Only” sub-option is shown as being selected, which means that the topology will show the VMWare vSphere ESXi hosts (aka servers), which are attached to the network switches.



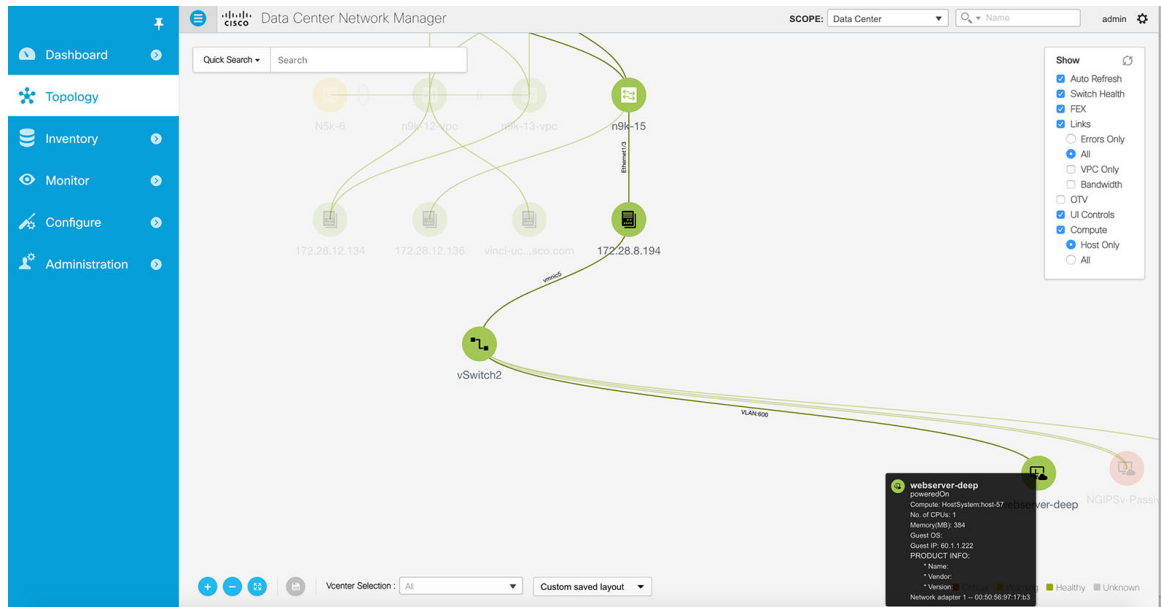
- Step 2** Once the topology is shown with the additional compute visibility, through clicking a specific ESXi host, additional information is depicted. The expanded topology will display the virtual switches (both vSwitch and Distributed Virtual Switch) that are configured on the specific ESXi host.



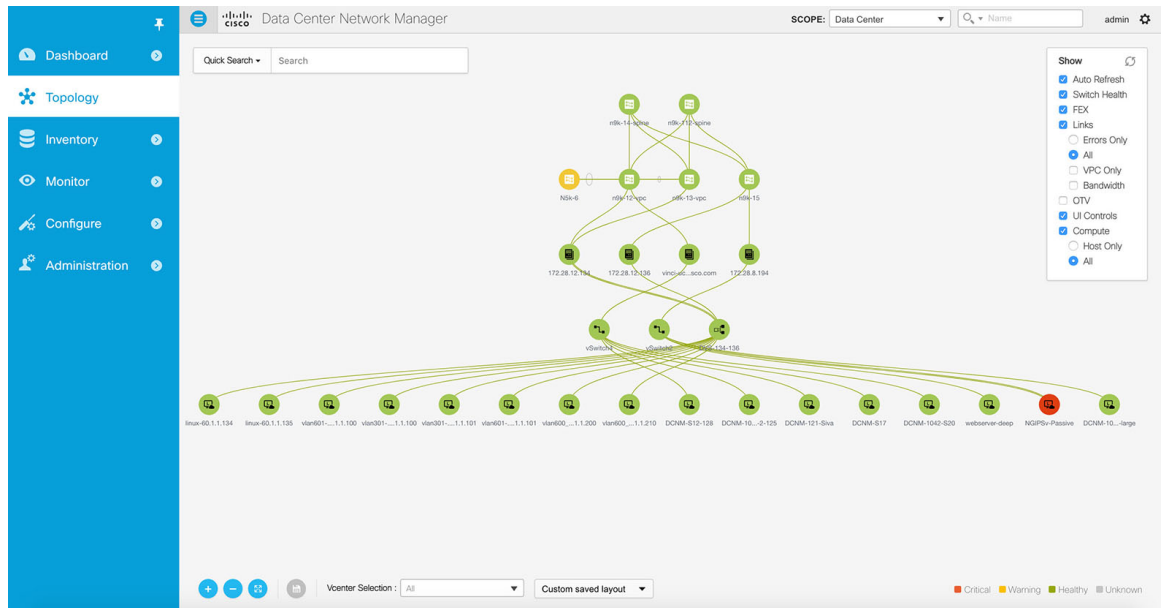
**Step 3** Further expansion of the topology is possible by clicking the virtual switch, which will display the virtual machines connected to the selected virtual switch.



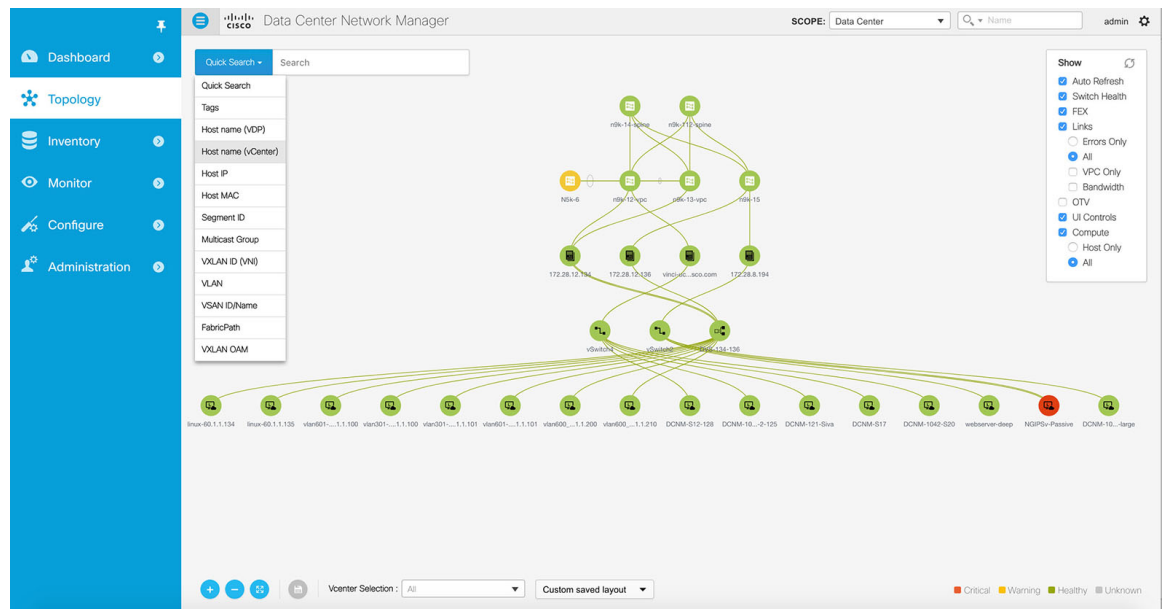
**Step 4** Additional context information is available through mouse-over. The information is overlaid on top of the current topology view.



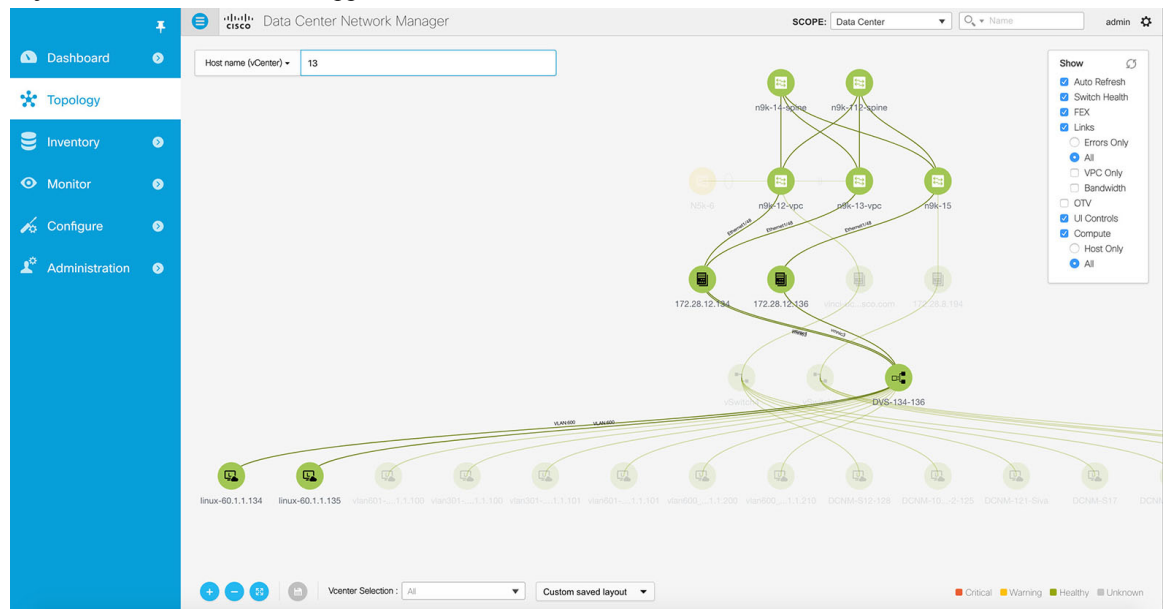
**Step 5** When changing from the “Host Only” sub-option to the “All” sub-option, all the compute resources are expanded. This mode provides an expanded view of all the hosts, virtual switches, virtual machines that are part of the topology. If a VM is powered off, it will be shown in red color else it will be green color.



**Step 6** Instead of browsing through the large set of available information, to quickly focus on a specific VM, a search option is available. In the top left search bar, select the “Host name (vCenter)” option.



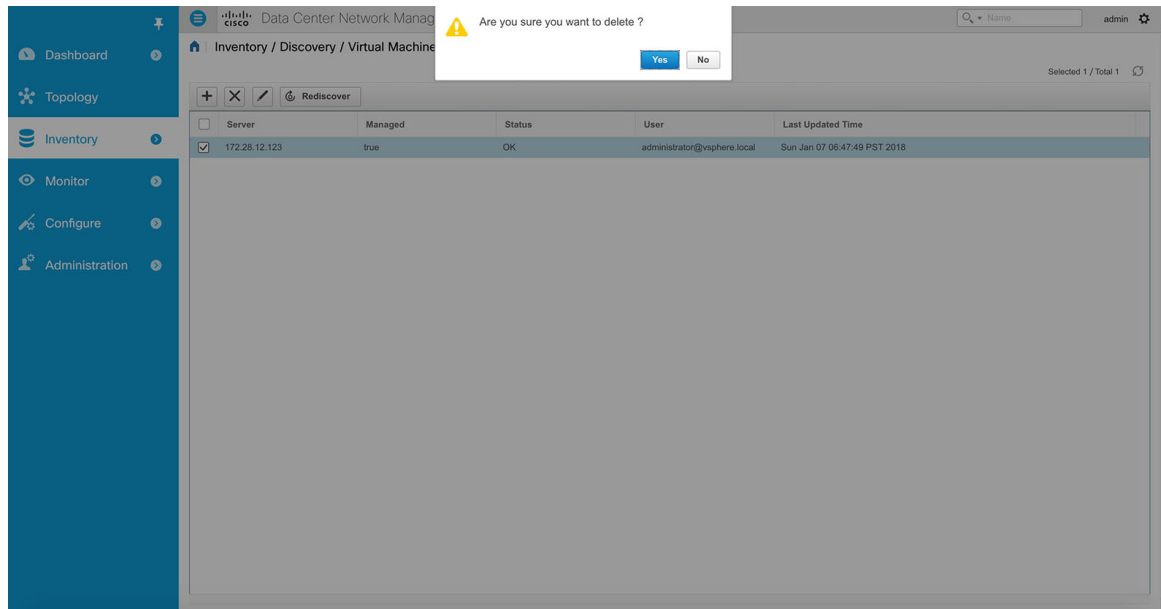
**Step 7** As soon as one starts typing characters, the topology is instantaneously updated to highlight the matching objects. Partial searches are supported.



## Disabling the Compute Visibility Feature

### Procedure

- Step 1** From Cisco DCNM Web Client, choose **Configure > Inventory > Virtual Machine Manager**. The Inventory / Discovery / Virtual Machine Manager listing page appears depicting the vCenters that have been added to the DCNM so far.
- Step 2** Select the vCenter for which the preview functionality has been enabled. Then click the “X” button. Confirm the deletion by clicking “Yes” on the pop-up.



## Streaming Telemetry for LAN Deployments

In today's data center environments, granular visibility and tracking of network events has become extremely critical. The traditional polling based methods that pull network state in predefined intervals need a fork-lift upgrade. More advanced streaming approaches are required that provide network event visibility in closer to real time through a push method. Streaming telemetry not only allows data to be pushed out at a much finer granularity with a lower cadence (shorter interval) but it also enables event based notifications. While getting relevant data in a timely fashion is highly desirable, the data needs to be analyzed and converted into actionable insights.

As a first step toward LAN analytics, DCNM 10.4.2 enables subscriptions for environmental metrics through streaming telemetry for consumption and analysis. The environmental metrics that are streamed include CPU, Memory, Power, and Fan Speed; all of these are enabled with a single click. DCNM configures the streaming updates for CPU, Memory to be streamed out every 30 seconds, and those for Power, Fan Speed to be streamed out every 300 seconds (5 minutes). The per-metric real-time streaming dashboards allow filtering on a per

fabric and per switch level including a per-switch drill-down where applicable. Streaming telemetry is currently supported on the Nexus 9000 platforms.

## Pre-requisites for Enabling the Streaming Telemetry Feature

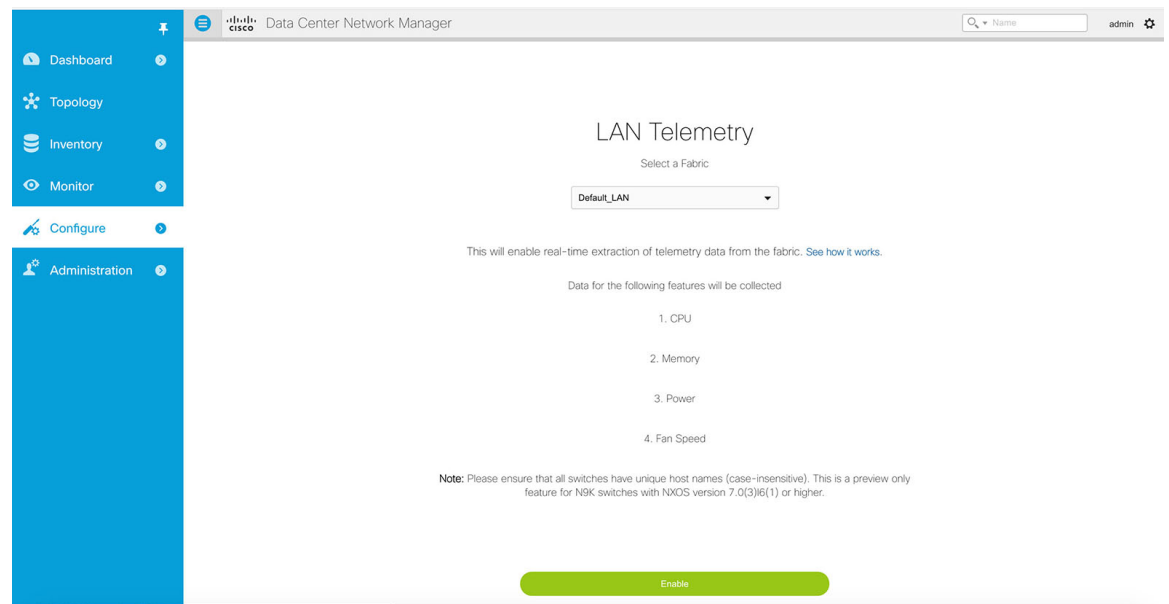
The pre-requisites for enabling this feature are:

- The Cisco Nexus 9000 switches and Cisco DCNM need to be time synchronized (NTP is recommended).
- Minimum software version on the Nexus 9000 switches must be 7.0(3)I6(1) or higher.

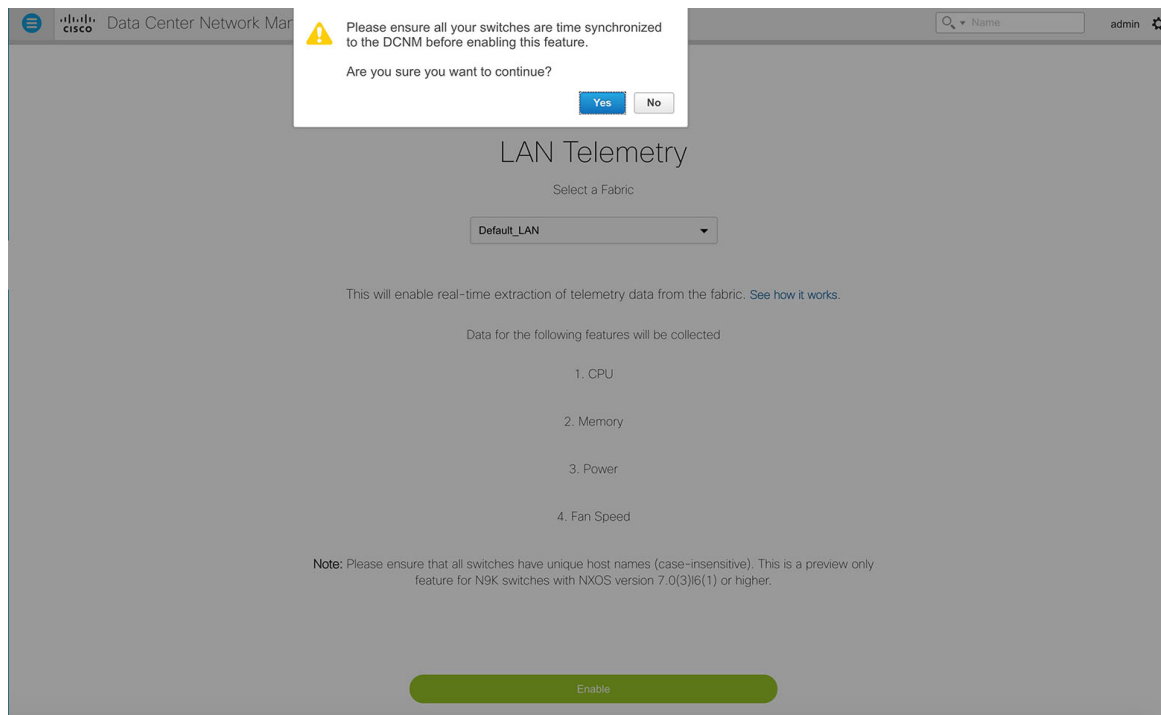
## Enabling the Streaming Telemetry Feature

### Procedure

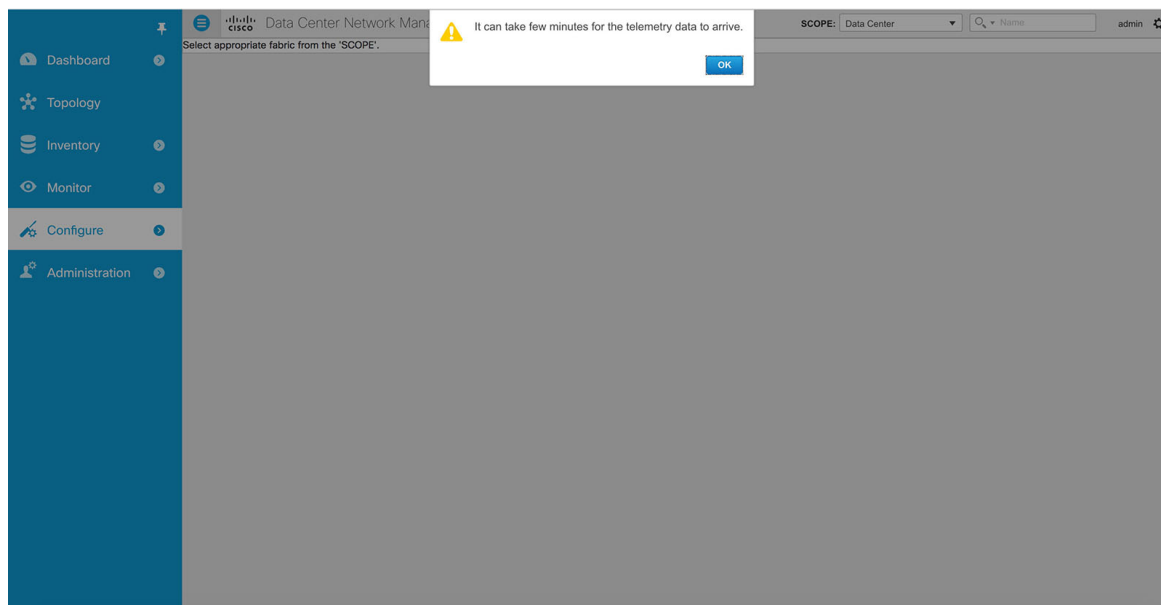
- Step 1** Go to **Configure > LAN Telemetry > Configure**. Select the fabric for which LAN Telemetry has to be enabled. Then press the **Enable** button.



There will be a warning message that will indicate that DCNM and the switches need to be time synchronized before this feature is enabled. Recall, that this is a pre-requisite for this feature. If the pre-requisite is met, please acknowledge by clicking **Yes**.

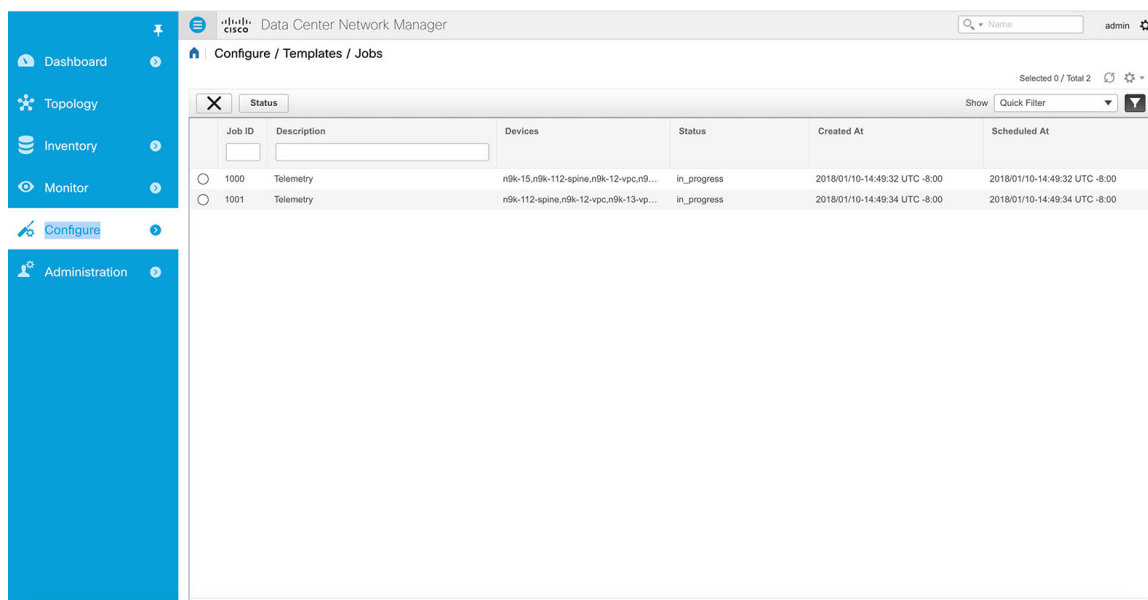


**Step 2** Once the feature is enabled, a message will appear indicating the initialization process has begun, which will take a couple of minutes. This time is needed for the streaming configuration to be pushed to the switches, the initial data to be streamed out from the switches, consumed by DCNM and depicted on the LAN telemetry dashboard.



Once the LAN telemetry preview feature is enabled, DCNM will update the switch telemetry configuration for the environmental metrics. Every switch that does not conform to the telemetry requirements (must be Cisco Nexus 9000) will be excluded from the configuration update. The job status can be monitored by going to **Configure > Template > Jobs**.



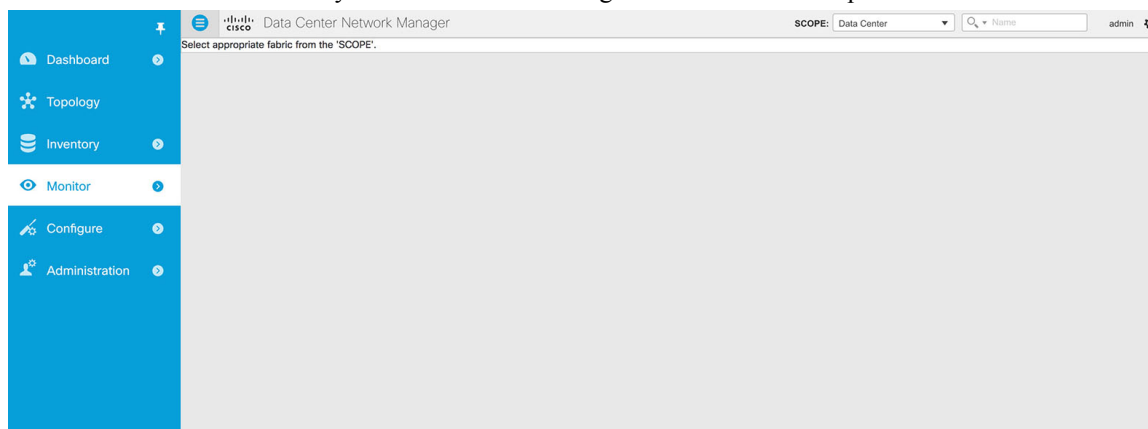


Once the jobs are successfully executed, the required telemetry configuration has been applied to the switches and the streaming data will appear once received and processed.

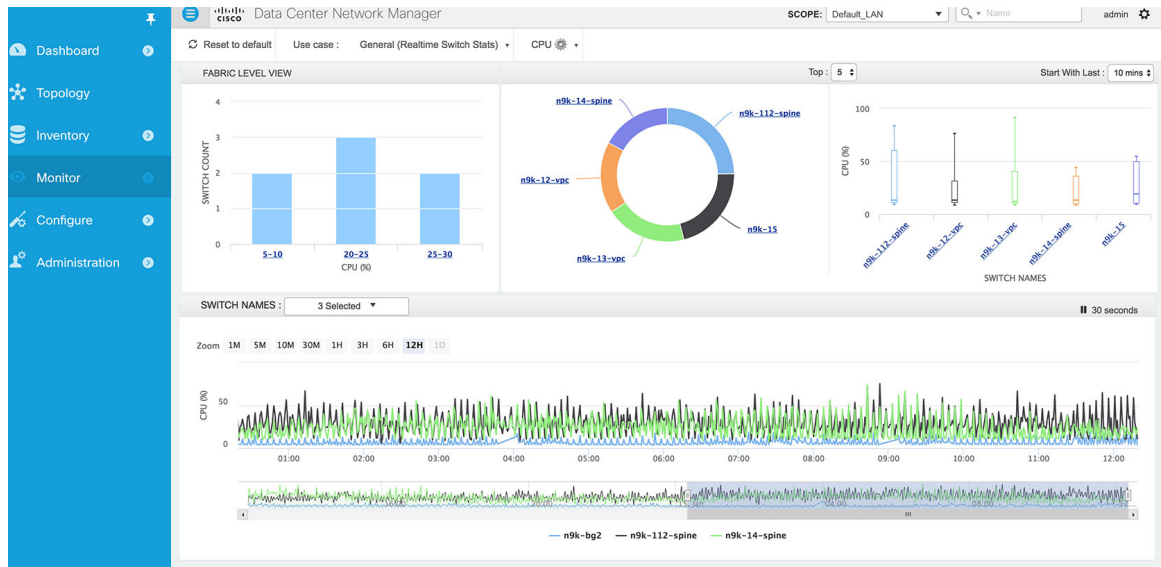
## Using the Streaming Telemetry Feature

### Procedure

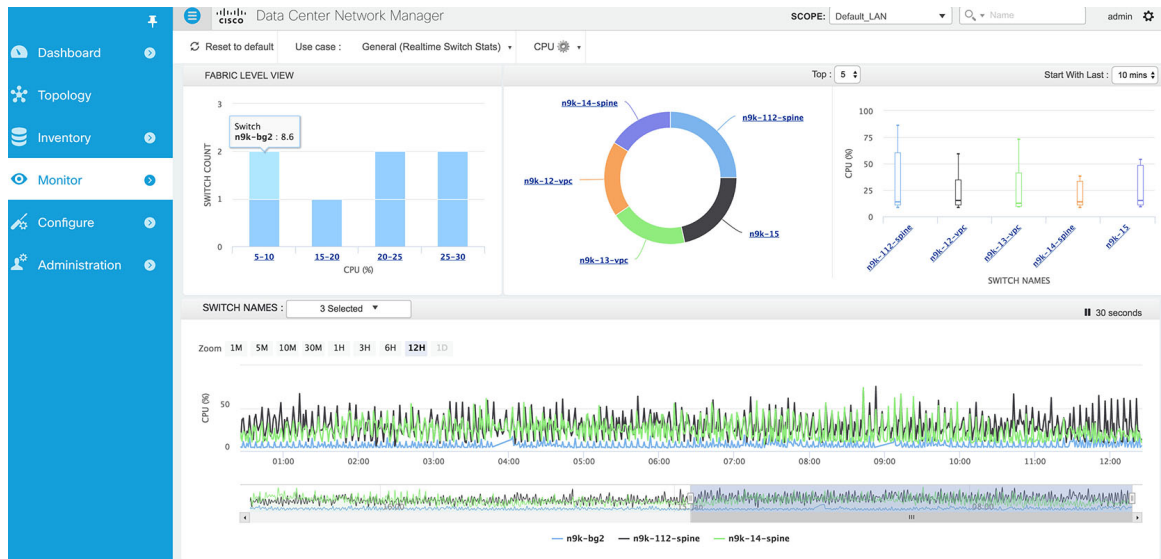
- Step 1** Once LAN telemetry has been successfully enabled, a new Telemetry Explore screen is available. You can navigate to the Telemetry Explore screen by following **Monitor > LAN Telemetry > Explore**. Select the fabric for which LAN telemetry has been enabled through the SCOPE at the top.



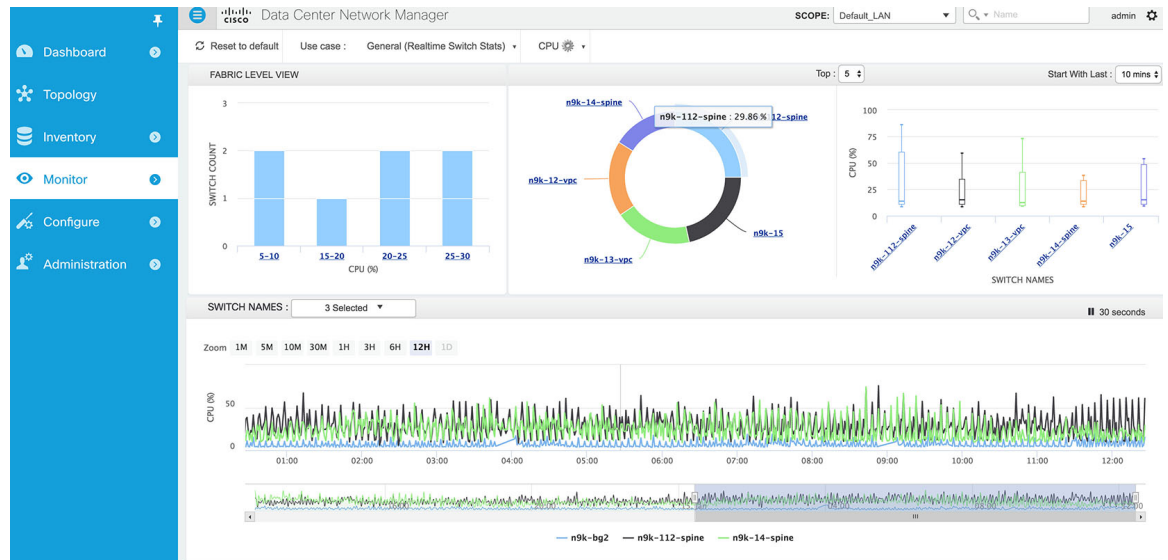
- Step 2** Once the appropriate fabric is selected as part of the scope, the LAN telemetry dashboard shows up, depicting CPU data, by default.



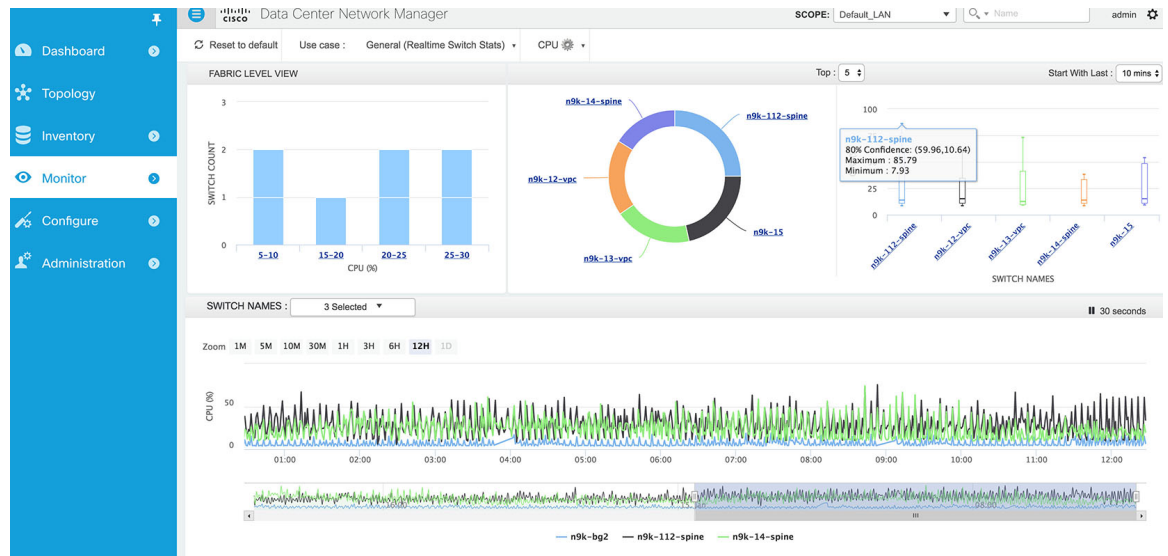
The top three tiles in the screen depict the data collected over the last 10 minutes. This interval can be changed by selecting a different time scale in the pull down. Next, we will describe the details depicted in the various tiles and graphs. The first tile on the left shows a fabric level view; it's a histogram showing the count of switches that fall within a certain CPU range.



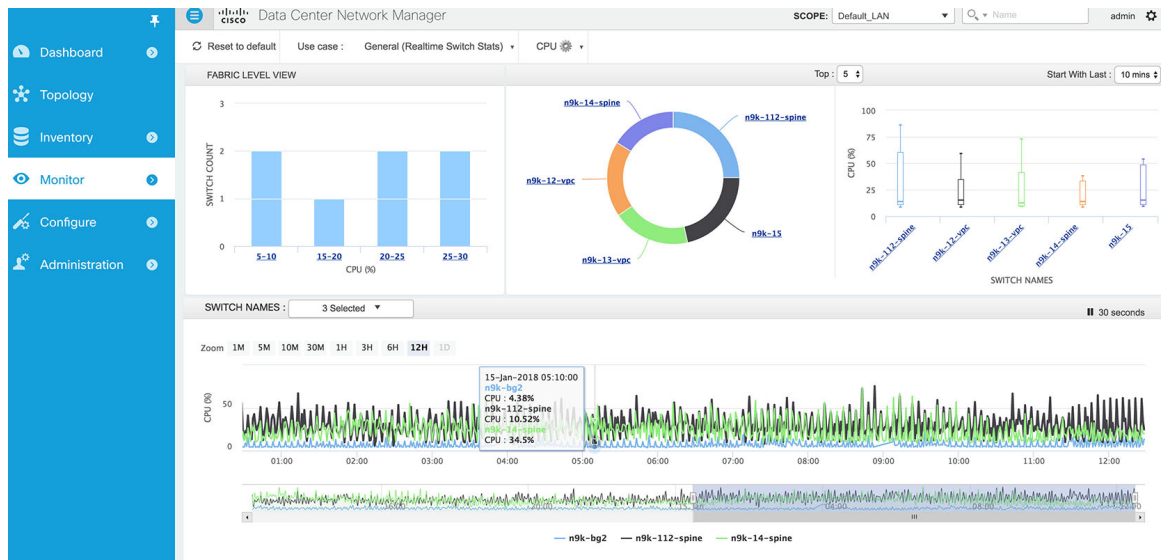
The middle tile depicts the Top 5 switches in the fabric with respect to average CPU usage. The user can select the Top 10 or Top 15 switches by choosing the drop-down menu above the middle tile.



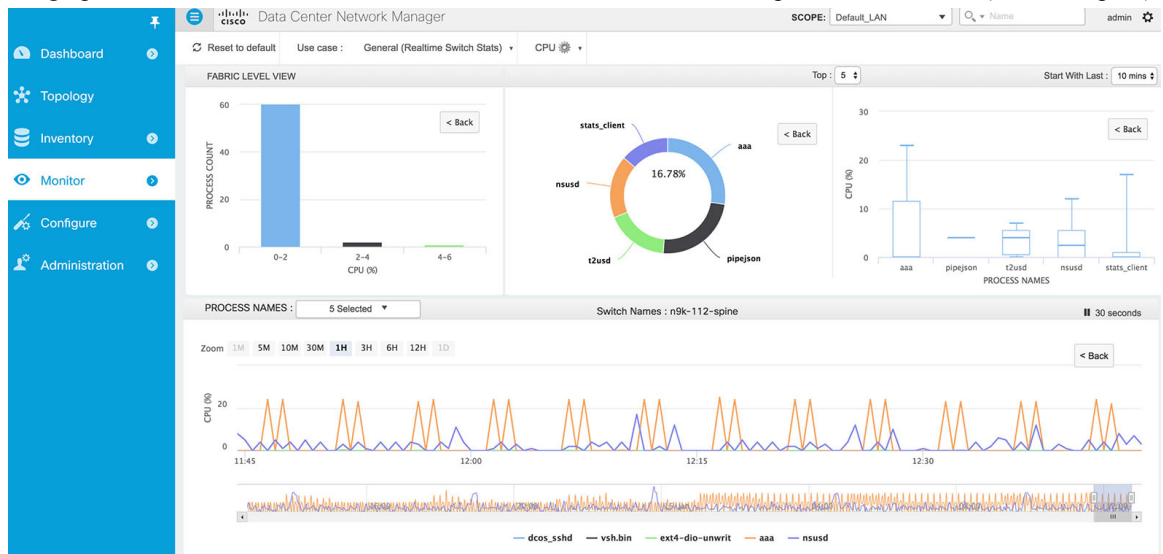
Since averages may not always satisfy your needs, the third tile depicts the spread of the CPU values over the selected time-interval. Specifically, the box plot provides the maximum and minimum CPU values reported from the switch over the selected time-interval as well as the 80% confidence interval for the reported values. In simpler terms, this is the range in which majority of the reported CPU values were reported.



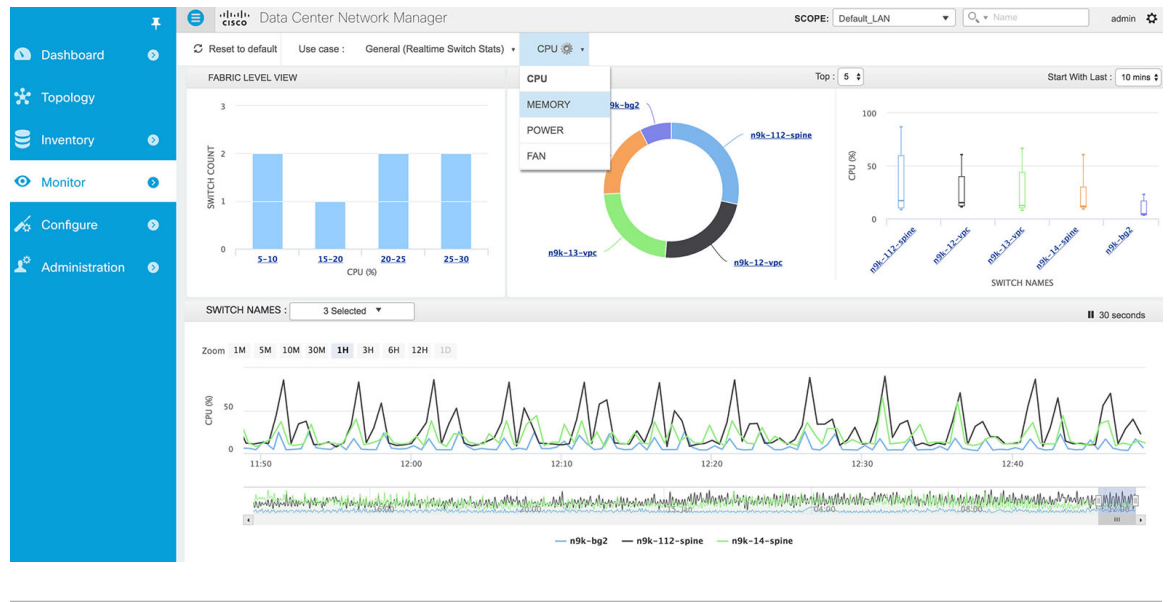
The representation at the bottom shows the real time CPU data feed for every switch. The graph refreshes automatically every 30 seconds. By default, 3 switches are selected to be displayed. The user can select up to a maximum of 5 switches by selecting them in the drop-down menu next to "SWITCH NAMES".



**Step 3** Every graph has a drill-down capability which enables the user to see the live CPU usage on a per switch per process basis. The per-process view can be triggered by simply clicking on the switch of interest in any of the graphs. Below is the drill-down view for the CPU metric with a sample selected switch (n9k-112-spine).



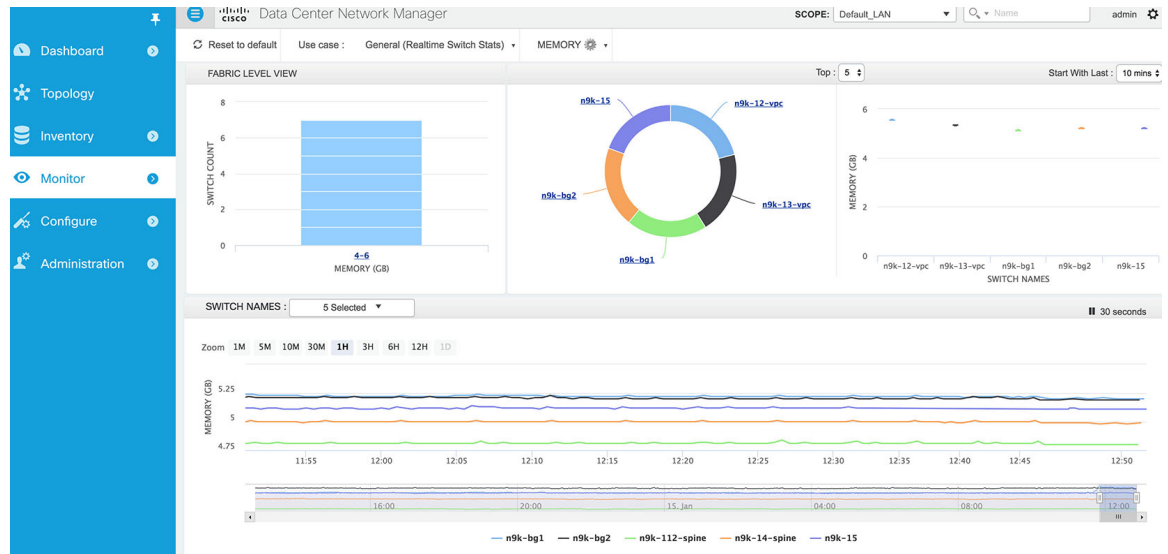
**Step 4** Similar data visualization is available for other metrics such as Memory, Power, and Fan. The metrics can be selected from the dropdown in the top menu.



## Data Visualization For Streaming Telemetry Metrics

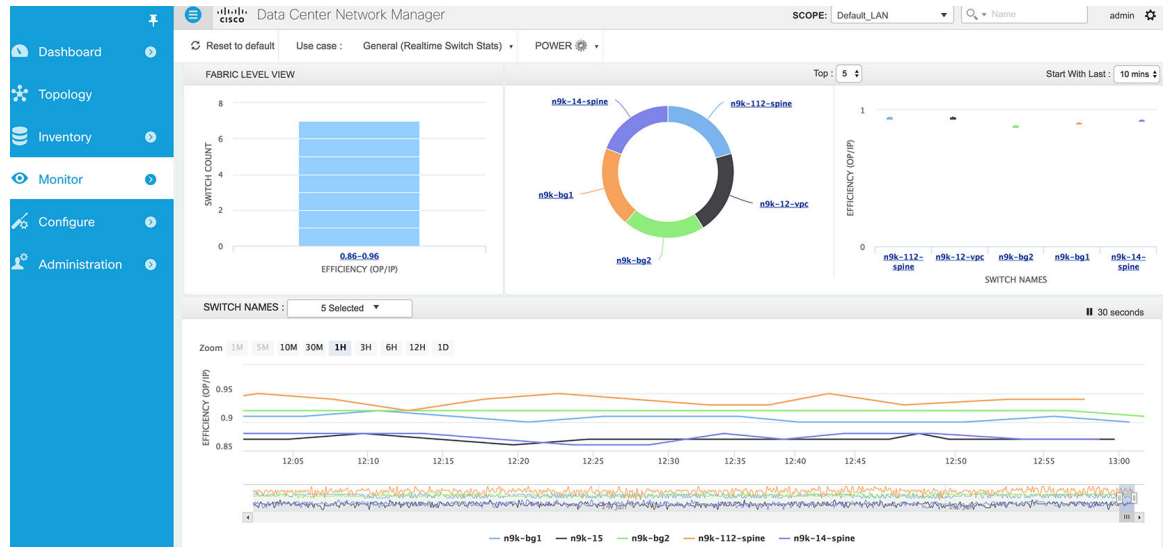
### Memory Data View

The memory dashboard depicts the actual memory consumption (RAM) on every switch in Gigabytes (GB). The per-process memory consumption will be available at a later stage.

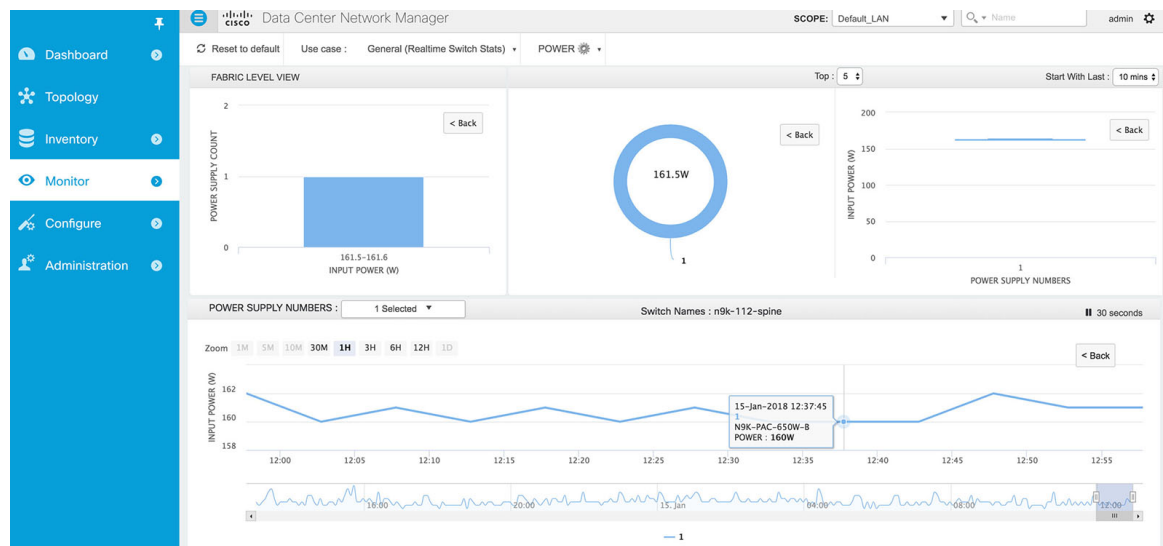


## Power Data View

The top-level view for the power dashboard depicts the efficiency of the power supplies. By definition, efficiency is Output-Power/Input-Power, which consequently results in a maximum efficiency of 1.0.

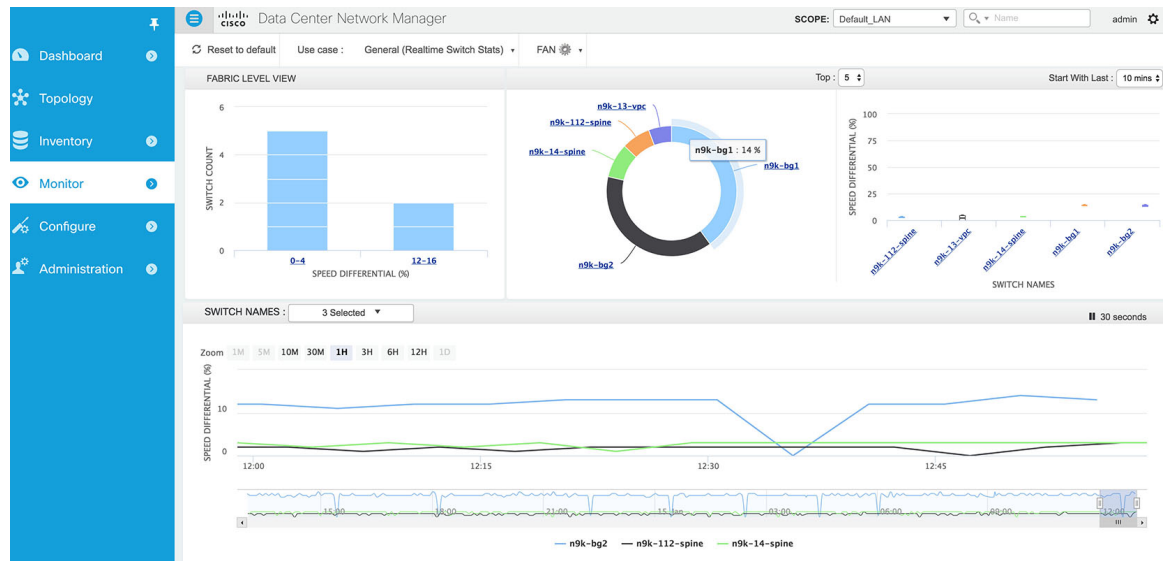


The drill down view indicates the input power in Watts, consumed by the individual power supply of the selected switch. A sample drill-down view for a selected device is shown below (n9k-112-spine):

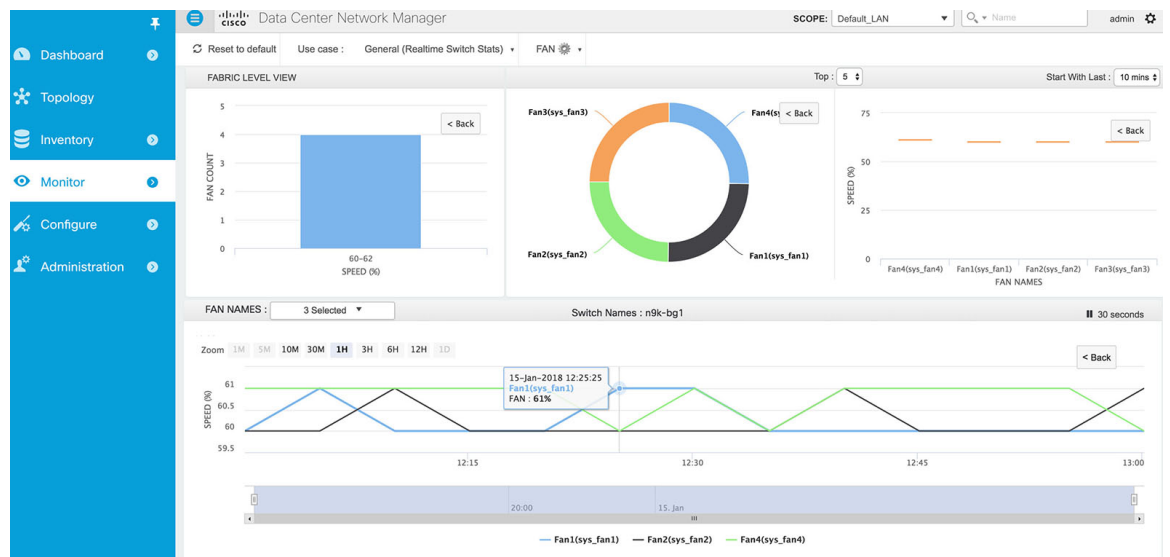


## Fan Data View

The top-level view for the fan dashboard depicts the speed difference between the various fans in the system. In the typical case, the expectation is that all the fans in the same tray, operate at more or less the same speed.



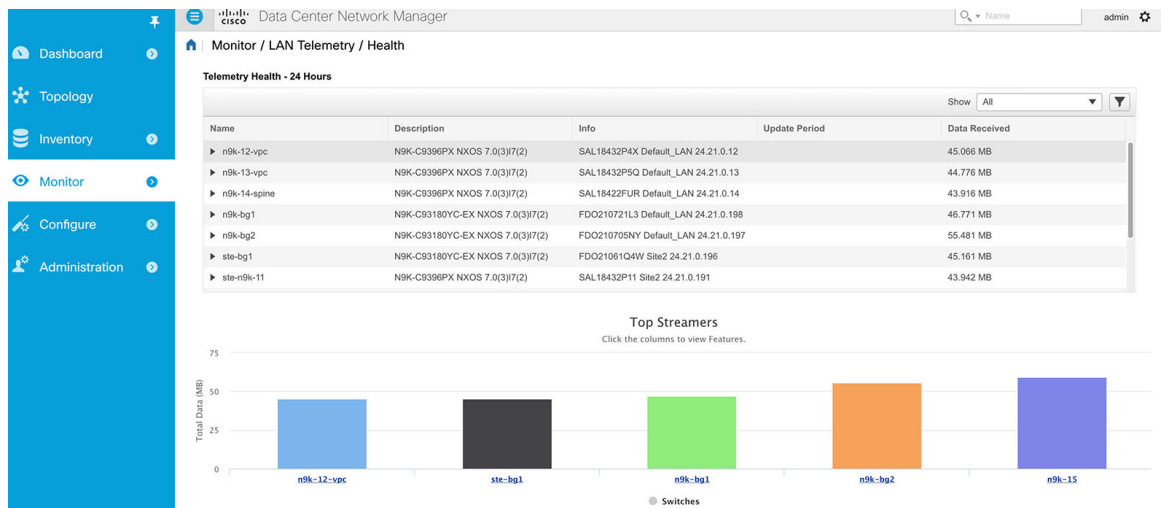
The drill down view provides the fan speed as a percentage metric of each individual fan within a selected device. A sample drill-down view for a selected device is shown below (n9k-bg1):



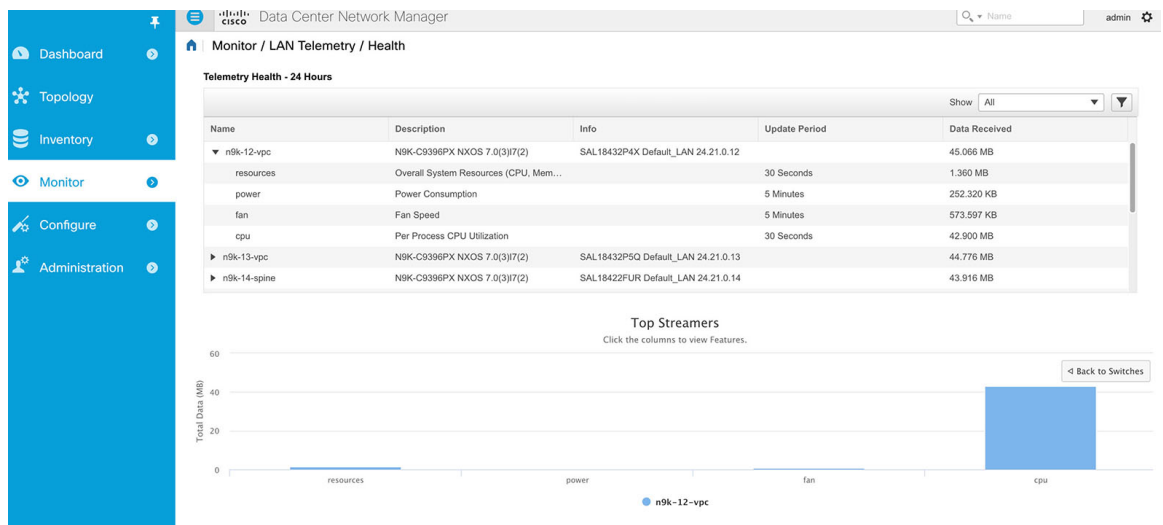
## Telemetry Health View

The LAN Telemetry Health screen, provides a detailed break-down of how much data is being streamed out by each switch per feature for the last 24 hours. This data can be accessed by traversing the menu: **Monitor > LAN Telemetry > Health**.





The bar graph depicts the top 5 streaming switches and has drill-down capability for feature-wise break-down.







## Border Provisioning Use Case in VXLAN BGP EVPN Fabrics - Multi-Site

This chapter explains LAN Fabric border provisioning using EVPN Multi-Site feature.

- [Overview, page 331](#)
- [Prerequisites , page 331](#)
- [Limitations, page 332](#)
- [Sample Scenario, page 332](#)
- [EVPN Multi-Site Configuration , page 334](#)
- [Deploying Networks and VRF Instances, page 350](#)
- [Additional References, page 356](#)
- [Appendix , page 357](#)

### Overview

This document explains how to connect two Virtual eXtensible Local Area Network (VXLAN) Border Gateway Protocol (BGP) Ethernet VPN (EVPN) fabrics through DCNM using EVPN Multi-Site feature. The EVPN Multi-Site configurations are applied on the Border Gateways (BGWs) of the two fabrics. Apart from VXLAN BGP EVPN fabrics, EVPN Multi-Site also allows you to extend Layer 2 and Layer 3 connectivity to data center networks built with older (legacy) technologies (Spanning Tree Protocol, virtual Port Channel [vPC], Cisco FabricPath, etc).

### Prerequisites

- The EVPN Multi-Site feature requires Cisco Nexus 9000 Series NX-OS Release 7.0(3)I7(1) or later.
- Familiarity with VXLAN BGP EVPN data center fabric architecture and configuration through DCNM.
- Fully configured VXLAN BGP EVPN fabrics and connected device (route servers, for example) configurations that are ready to be connected using the EVPN Multi-Site feature.

- VXLAN BGP EVPN fabrics (and their interconnection) can be configured manually or using Cisco® Data Center Network Manager (DCNM). This document explains the process to connect the fabrics through DCNM. So, you should know how to configure and deploy a VXLAN BGP EVPN fabric through DCNM. For more details, see the LAN Fabric Provisioning section under Configure chapter in [Cisco DCNM Web Client Online Help, 10.4\(2\) Release](#).

**Note**

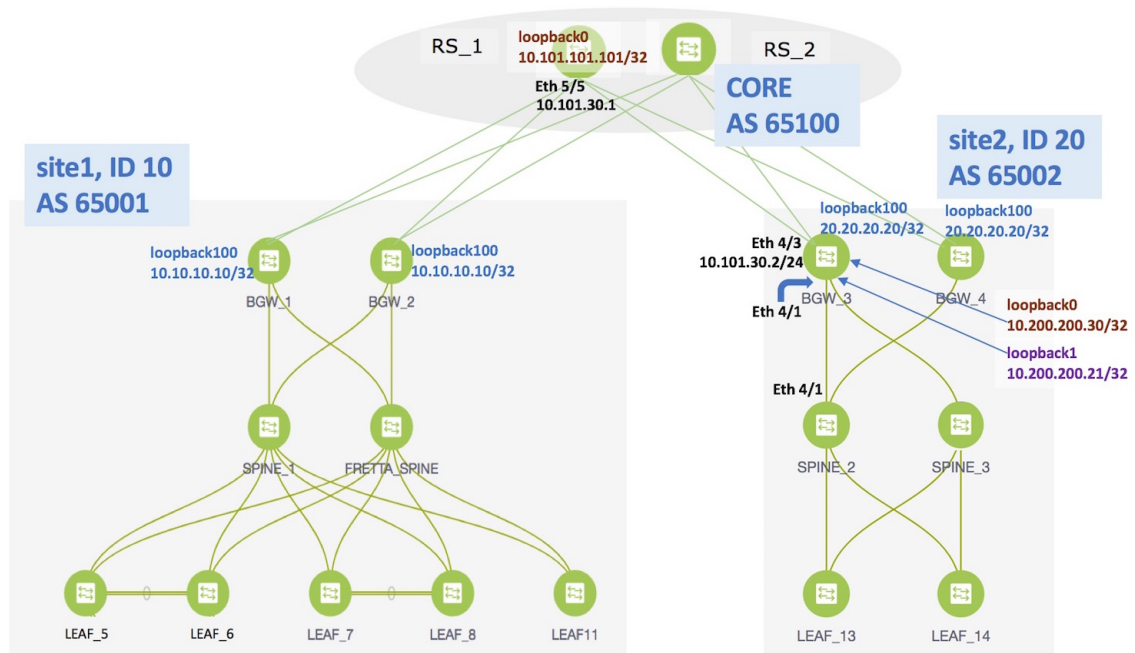
For a detailed explanation on the EVPN Multi-Site feature, see the [VXLAN BGP EVPN Multi-Site Design and Deployment](#) document.

## Limitations

- BGWs cannot form a virtual port channel (vPC) switch pair. This is a switch side limitation and not a DCNM software limitation.

## Sample Scenario

The EVPN Multi-Site feature is explained through an example scenario. Consider two VXLAN BGP EVPN fabrics, site1 and site2. This document will show you how to enable end-to-end Layer 3 and Layer 2 traffic between hosts in site1 and site2.



Network configurations for the two fabrics are provisioned through DCNM software, 10.4(2) release. VXLAN BGP EVPN configurations are configured on the switches in the two fabrics. However, server traffic between the sites is only possible through a Data Center Interconnect (DCI) function. If a server in site1 has to send

traffic to a server in site2 or vice versa, the DCI function (such as the Multi-Site feature, used for this example) should be configured on the BGWs of both the fabrics.

**Note**

The DCI functions VRF Lite and VRF Lite + Multi-Site are in the scope of this document, but MPLS L3VPN and LISP technologies are not in the scope of this document.

The steps involved to enable EVPN Multi-Site feature and traffic flow across the sites/fabrics are:

- 1 Top-Down deployment of the underlay for the IP core at the BGWs. This is a one-time configuration.
- 2 Top-Down deployment of the BGP overlay for the IP core. This is a one-time configuration for each BGW.
- 3 Deployment of networks/virtual routing and forwarding (VRF) instances on the leaf switches. This is a per network/VRF configuration.
- 4 Deployment of networks/VRFs at the BGWs. This is a per network/VRF configuration.

**EVPN Multi-Site feature**—This requires setting up the BGW base configuration for enabling the EVPN Multi-Site feature on the BGWs and the underlay peering to the external devices. This is followed by establishing overlay peering from the BGW to appropriate external devices, either BGWs in other fabrics or route servers. Both the underlay and overlay peering are established over eBGP. BGWs are special devices that allow clear control and data plane segregation from one site to another, allowing for policy enforcement points for any inter-fabric traffic. They allow the same data plane (VXLAN) and control plane (BGP EVPN) to be employed both for inter-fabric and intra-fabric traffic.

**Note**

DCNM 10.4.2 Top-Down provisioning only supports eBGP underlay.

The end-to-end configurations can be split into these 2 steps:

**1 EVPN Multi-Site configurations on the BGWs (BGW\_1, BGW\_2, BGW\_3 and BGW\_4).**

- 1 EVPN Multi-Site feature on the BGWs on site1—Overlay and underlay connections between the BGWs BGW\_1 and BGW\_2, and directly connected route servers RS\_1 and RS\_2.
- 2 EVPN Multi-Site feature on the BGWs on site2—This includes overlay and underlay connections between the BGWs BGW\_3 and BGW\_4, and directly connected route servers RS\_1 and RS\_2.
- 3 Configurations on RS\_1 and RS\_2—These configurations are not in the scope of DCNM provisioning and this document. For completeness, it is mentioned here, and sample configurations provided in the Appendix section.

For this example, BGW\_3 EVPN Multi-Site configurations will be explained.

**2 Deploying Networks and VRF Instances on the leaf switches and the BGWs**

For this example, 2 networks will be configured on the BGWs in site2 (with the assumption that network deployment on leaf switches is already completed).

After successful deployment on both the sites, Layer 2 and Layer 3 traffic will flow between the two sites.

**Note**

In the DCNM GUI, the lines connecting devices managed by DCNM (for example, LEAF\_5 to SPINE\_1 and SPINE\_1 to BGW\_2) symbolize a physical cable connection, and not that the connection is functional and network traffic flows between them.

To start off with, let us consider EVPN Multi-Site provisioning on BGW\_3 through DCNM Top-Down LAN Fabric Provisioning.

## EVPN Multi-Site Configuration

### Prerequisite Configuration for EVPN Multi-Site Feature

- Manual loopback interfaces' configuration.
- Setting the BGW role to *Border Gateway*.

**Manual loopback interfaces' configuration**—Before you begin EVPN Multi-Site configuration through DCNM, you should manually configure loopback interfaces on the BGWs. There are three loopback interfaces configured on a BGW that must be reachable by fabric-internal neighbors and fabric-external neighbors. The fabric internal neighbors will learn these through the fabric interior gateway protocol (IGP). For fabric external

neighbors, these are redistributed into the IPv4 eBGP session. In order to achieve that, the 3 loopback IP addresses must be tagged as shown below:

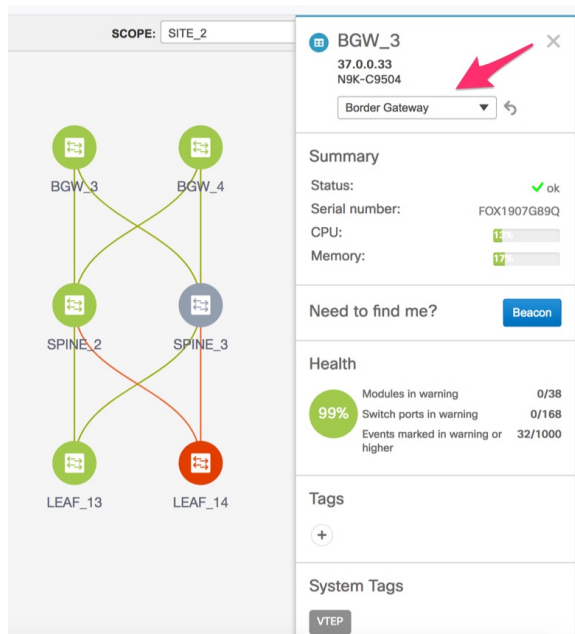
| Loopback configuration                                                                                                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>interface loopback0 description RID AND BGP PEERING ip address 10.200.200.30/32 tag 54321 ip router ospf UNDERLAY area 0.0.0.0 ip pim sparse-mode</pre>      | <ul style="list-style-type: none"> <li>• This is the address used for BGP peering with external and internal neighbors.</li> <li>• In this example, Open Shortest Path First (OSPF) is shown as the fabric underlay routing protocol used for fabric neighbors.</li> <li>• The <b>ip pim sparse-mode</b> setting is needed only for intra-site multicast-based Broadcast, Unknown unicast and Multicast (BUM) replication.</li> </ul> |
| <pre>interface loopback1 description NVE INTERFACE (PIP VTEP) ip address 10.200.200.21/32 tag 54321 ip router ospf UNDERLAY area 0.0.0.0 ip pim sparse-mode</pre> | This is the interface used for local NVE peer address.                                                                                                                                                                                                                                                                                                                                                                                |
| <pre>Interface loopback100 description MULTI-SITE INTERFACE (VIP VTEP)  ip address 20.20.20.20/32 tag 54321 ip router ospf UNDERLAY area 0.0.0.0</pre>            | <p>This is the EVPN Multi-Site loopback address. This is provisioned as part of Top-Down auto-configuration of the underlay/overlay, and only shown here for the sake of completeness. This does not need to be pre-provisioned.</p> <p><b>Note</b> The EVPN Multi-Site loopback IP address should be common for all the BGWs in a VXLAN BGP EVPN site.</p>                                                                           |

### Setting the BGW role to *Border Gateway*

After configuring the loopback interfaces on the BGWs, you should change the role of each designated BGW to *Border Gateway*, since, by default a device will be treated as a leaf switch.

To update the switch role, login to DCNM, and click **Topology** from the main menu at the left part of the screen. In the Topology screen, select the fabric/site from the **Scope** drop down box (site2 or site1 in this case), and click on the switch icon. A screen pops up with the switch information.

Change the entry from *Leaf* to *Border Gateway* as shown in the image.



Likewise, update the role for BGW\_4 in site2 and then select site1 from the scope box and update roles for BGW\_1 and BGW\_2. This is required for configuring the EVPN Multi-Site feature through the DCNM GUI.

After completing the EVPN Multi-Site specific prerequisites, start EVPN Multi-Site configuration on BGW\_3 with extensions to the route server RS\_1.

## EVPN Multi-Site Extensions from BGW\_3 to RS\_1

From the Cisco DCNM Web Client, choose **Configure > LAN Fabric Provisioning > Network Deployment**. The LAN Fabric Provisioning page appears.

Click **Continue**. The **Select a Fabric** page comes up.

## Select a Fabric

Choose a fabric with appropriate switches where you want the Top Down functionality to be enabled or create a new fabric.

SITE\_2

 [Fabric Extension Settings](#)

OR

[+ Create a new fabric](#)

Select **site2** from the drop-down box since you are configuring BGW *BGW\_3* on site2.

Click **Fabric Extension Settings** since the purpose of this task is to allow site2 to communicate to external fabrics through RS\_1 and RS\_2. The **Fabric Extension** screen comes up.

Fabric Extension

Inter-Fabric Connections

Selected 0 / Total 0

| Type | Source Fabric | Source Device | Source Interface | Destination Fabric | Destination Device | Destination Interface | Configuration | Status |
|------|---------------|---------------|------------------|--------------------|--------------------|-----------------------|---------------|--------|
|      |               |               |                  |                    |                    |                       |               |        |

No data available

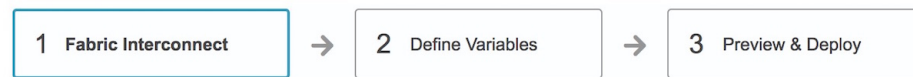
The **Inter-Fabric Connections** section lists previously created external connections from the BGWs on site2. Each line represents a physical or logical connection between a BGW in site2 and an external device in another fabric. For each connection, the source fabric, source device, source interface, destination fabric, destination device, and destination interface are listed along with the type of external connectivity. This section is empty as this is the first time you are adding an external connection.

*To extend the fabric through EVPN Multi-Site, you should first create an underlay extension and then an overlay extension.*

## Underlay Extension from BGW\_3 to RS\_1

Click on the + icon to add a new external connection. The **Add Inter-Fabric Connection** screen appears.

## Add Inter-Fabric Connections



|                         |               |   |                                                                                     |
|-------------------------|---------------|---|-------------------------------------------------------------------------------------|
| * Extension Type        | VRF_LITE      | ▼ |                                                                                     |
| * Base Template         | BorderBase_v1 | ▼ |                                                                                     |
| * Extension Template    | FabricSetup   | ▼ |                                                                                     |
| * Source Fabric         | SITE_2        |   |                                                                                     |
| * Destination Fabric    |               | ▼ |                                                                                     |
| * Source Device         |               | ▼ | ① VRF_LITE: Set switch role - Border; MULTISITE: Set switch role - "Border Gateway" |
| * Source Interface      |               | ▼ |                                                                                     |
| * Destination Device    |               | ▼ |                                                                                     |
| * Destination Interface |               | ▼ |                                                                                     |

Previous

Next

Save &amp; Deploy

Cancel

By default, VRF\_LITE is populated in the **Extension Type** field. Change the selection to MULTISITE\_UNDERLAY.

## Add Inter-Fabric Connections



|                         |                        |   |                                                                                     |
|-------------------------|------------------------|---|-------------------------------------------------------------------------------------|
| * Extension Type        | MULTISITE_UNDERLAY     | ▼ |                                                                                     |
| * Base Template         | BorderBase_v1          | ▼ |                                                                                     |
| * Extension Template    | MultiSiteUnderlaySetup | ▼ |                                                                                     |
| * Source Fabric         | SITE_2                 |   |                                                                                     |
| * Destination Fabric    |                        | ▼ |                                                                                     |
| * Source Device         |                        | ▼ | ① VRF_LITE: Set switch role - Border; MULTISITE: Set switch role - "Border Gateway" |
| * Source Interface      |                        | ▼ |                                                                                     |
| * Destination Device    |                        | ▼ |                                                                                     |
| * Destination Interface |                        | ▼ |                                                                                     |

Previous

Next

Save &amp; Deploy

Cancel



**Base Template**—By default, the BorderBase\_v1 base template is populated. This template is a one-time configuration pushed to the BGW.

**Extension Template**—*MultiSiteUnderlaySetup* is a setup template that contains the configuration that will be generated and pushed to the BGW to setup the corresponding inter-fabric connection.

These templates are auto-populated with corresponding pre-packaged default templates based on your selection.

**Source Fabric**—This field is pre-populated with *site2* since the EVPN Multi-Site underlay connection is between BGW\_3 in site2 and RS\_1 in the CORE fabric.

**Destination Fabric**—Choose CORE.

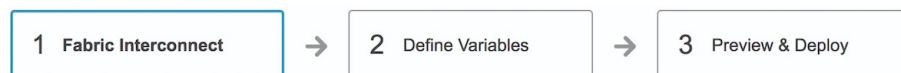
**Source Device** and **Source Interface**—Choose BGW\_3 as the source device and an Ethernet interface that needs to be connected to RS\_3.

**Destination Device** and **Destination Interface**—Choose RS\_1 as the destination device and the Ethernet interface that connects to the BGW BGW\_3

Note that based on the selection of the source device and source interface, the destination information will be auto-populated based on Cisco Discovery Protocol information, if available. There is extra validation performed to ensure that the destination external device is indeed part of the destination fabric.

After filling up the Fabric Interconnect section, the screen looks like this.

### Add Inter-Fabric Connections

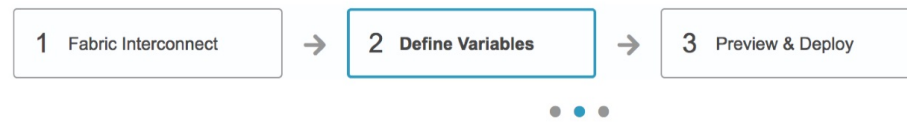


|                         |                          |                                                                                   |
|-------------------------|--------------------------|-----------------------------------------------------------------------------------|
| * Extension Type        | MULTISITE_UNDERLAY ▼     |                                                                                   |
| * Base Template         | ▼                        |                                                                                   |
| * Extension Template    | MultiSiteUnderlaySetup ▼ |                                                                                   |
| * Source Fabric         | SITE_2 ▼                 |                                                                                   |
| * Destination Fabric    | CORE ▼                   |                                                                                   |
| * Source Device         | BGW_3 ▼                  | VRF_LITE: Set switch role - Border; MULTISITE: Set switch role - "Border Gateway" |
| * Source Interface      | Ethernet4/3 ▼            |                                                                                   |
| * Destination Device    | RS_1 ▼                   |                                                                                   |
| * Destination Interface | Ethernet5/5 ▼            |                                                                                   |

[Previous](#)
[Next](#)
[Save & Deploy](#)
[Cancel](#)

Click **Next** to go to the **Define Variables** section.

## Add Inter-Fabric Connections



## ▼ Network Profile

| General             |                  |
|---------------------|------------------|
| MULTISITE           |                  |
| * IF_NAME           | Ethernet4/3 ?    |
| * Interface IP/Mask | 10.101.30.2/24 ? |
| * Neighbor IP       | 10.101.30.1 ?    |
| * NEIGHBOR_ASN      | 65100 ?          |
| * Extension Type    | MULTISITE ?      |

**IF\_NAME**—In this field, the interface name is auto-populated from the previous step.

**Interface IP\_MASK**—Fill up this field with the IP address of the BGW\_3 interface that connects to RS\_1.

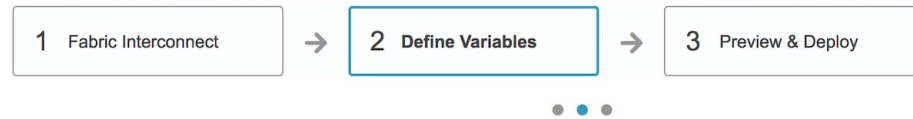
**NEIGHBOR\_IP**—Fill up this field with the IP address of the RS\_1 interface that connects to BGW\_3.

**NEIGHBOR\_ASN**—In this field, the AS number of RS\_1 will be auto-populated.

The corresponding connection in the topology is displayed:



## Add Inter-Fabric Connections



## Network Profile

| General   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MULTISITE | <p>* Fabric Site ID <input type="text" value="20"/> ?</p> <p>* NVE Identifier <input type="text" value="1"/> ?</p> <p>* Fabric Interfaces <input type="text"/> ? E.g. e1/1-4, e2/2</p> <p>* Multisite Loopback ID <input type="text" value="100"/> ? [0-1023]</p> <p>* MultiSite Loopback IP <input type="text"/> ? IPv4 address</p> <p>* Routing Protocol <input type="text" value="is-is"/> ? Select IGP (ospf or is-is)</p> <p>* IS-IS/OSPF Router ID <input type="text" value="UNDERLAY"/> ? String</p> <p>* OSPF Area # <input type="text" value="0"/> ? String</p> |

**Fabric Site ID**—This is the identification for the VXLAN BGP EVPN fabric site2 to which BGW\_3 belongs. When you configure the EVPN Multi-Site feature on BGW\_4 (or any other BGW on site2), the site ID will be 20. The site *site1* will be assigned with a unique ID.

**NVE Identifier**—This is the VXLAN overlay ID.

**Fabric Interfaces**—Fill up this field with the interfaces on BGW\_3 that connects to other intra-fabric device ports. Since Ethernet 4/1 connects to SPINE\_2 and Ethernet 4/2 connects to SPINE\_3 in the topology, the interfaces should be entered over here.

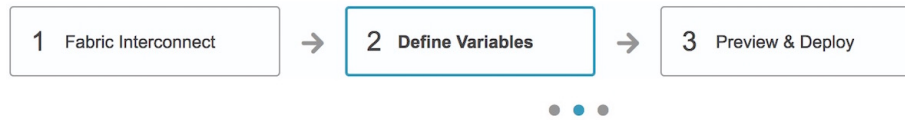
**Multisite Loopback ID and Multisite Loopback IP**—These are the loopback ID and IP address of this EVPN Multi-Site instance.

**Routing Protocol and Router ID**—This is the IGP and the IGP instance ID within the fabric. Note that, if the IGP used in your setup is OSPF, the field has to be updated to *OSPF*.

**OSPF AREA**—OSPF area ID within the fabric.

A fully filled screen looks like this.

## Add Inter-Fabric Connections

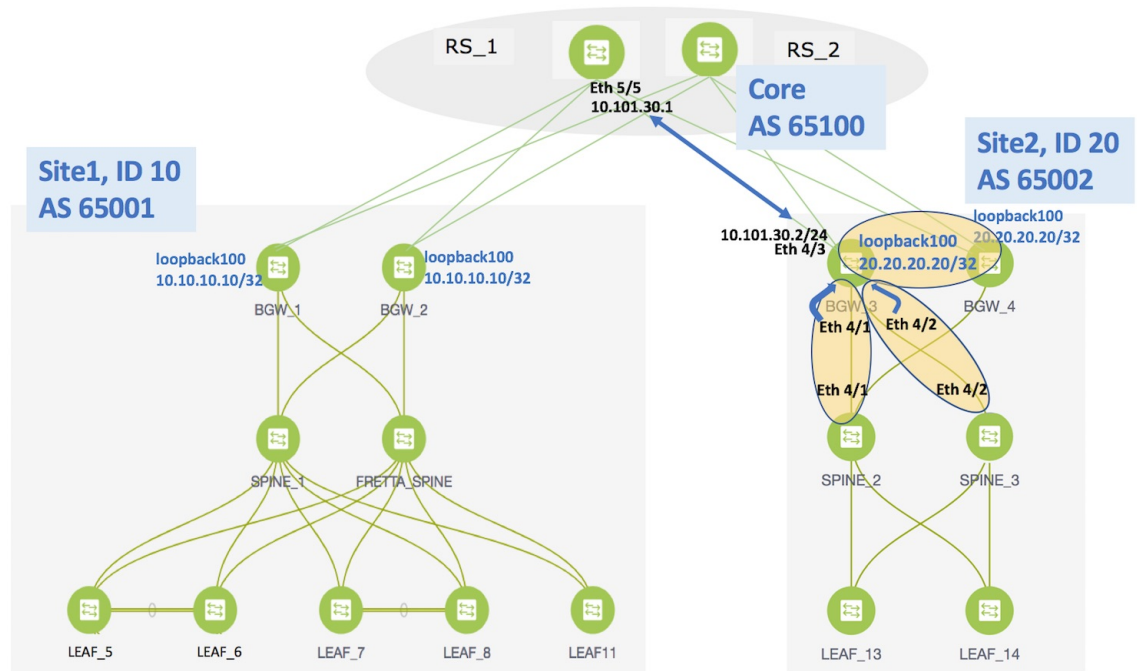


## ▼ Network Profile

| General                 |                                    |
|-------------------------|------------------------------------|
| <b>MULTISITE</b>        |                                    |
| * Fabric Site ID        | 20 ?                               |
| * NVE Identifier        | 1 ?                                |
| * Fabric Interfaces     | Eth4/1, Eth4/2 ? E.g. e1/1-4, e2/2 |
| * Multisite Loopback ID | 100 ? [0-1023]                     |
| * MultiSite Loopback IP | 20.20.20.20 ? IPv4 address         |
| * Routing Protocol      | ospf ? Select IGP (ospf or is-is)  |
| * IS-IS/OSPF Router ID  | UNDERLAY ? String                  |
| * OSPF Area #           | 0 ? String                         |

[Previous](#)
[Next](#)
[Save & Deploy](#)
[Cancel](#)

The corresponding topology depiction is given below:



Now that all the information is filled in, click **Next** to go to the **Preview and Deploy** section.

## Add Inter-Fabric Connections

1 Fabric Interconnect

→

2 Define Variables

→

3 Preview & Deploy

● ● ●

**Switch:**

**Generated Configuration:**

```

route-map RMAP-REDIST-DIRECT permit 10
 match tag 54321

evpn multisite border-gateway 20

interface loopback100
 description Used for EVPN Multi-Site
 ip address 20.20.20.20/32 tag 54321

 ip router ospf UNDERLAY area 0
 no shutdown

interface nve 1
 multisite border-gateway interface loopback100

interface e4/1
 evpn multisite fabric-tracking

```

Previous
Next
Save & Deploy
Cancel

Here, you can preview the configuration that will be deployed to BGW\_3. Note that no configuration will be pushed to the external device itself.

Click **Save and Deploy** to complete the task. This results in the configuration getting pushed to BGW\_3. The external connection will appear in the Fabric Extension screen.

Fabric Extension ×

Inter-Fabric Connections Selected 0 / Total 1

| Type               | Source Fabric | Source Device | Source Interf... | Destination ... | Destination De... | Destination Interf... | Configuration               | Status   |
|--------------------|---------------|---------------|------------------|-----------------|-------------------|-----------------------|-----------------------------|----------|
| MULTISITE_UNDERLAY | SITE_2        | BGW_3         | Ethernet4/3      | CORE            | RS_1              | Ethernet5/5           | <a href="#">View Config</a> | DEPLOYED |

The view doesn't auto-refresh, hence the refresh button on the top right part of the screen needs to be clicked to trigger refresh. You can check the status of the deployment (Deployment Pending, Deployed, Failed) in the **Status** column. In this case, the status changes from *Deployment Pending* to *Deployed* after you click on the refresh button.

In case of FAILED or UNDEPLOYMENT FAILED status, use the hyperlink in the **Status** column to check the error messages for failure.

To view the configurations, click on *View Config* in the **Configuration** field.

After the underlay configuration, you need to configure the overlay configuration from BGW\_3 to RS\_1 (the external device connected to BGW\_3), as shown in the next section.

## Overlay Extension from BGW\_3 to RS\_1


**Note**

You can have multiple underlay connections to an external device but only one overlay connection from BGW\_3 to each external device.

In the **Fabric Extension** page, click on the + icon to add an external overlay connection. The **Add Inter-Fabric Connection** screen appears.

By default, VRF\_LITE is populated in the **Extension Type** field. Change the selection to MULTISITE\_OVERLAY. The screen changes accordingly.

### Add Inter-Fabric Connections



|                         |                         |                                                                                                    |
|-------------------------|-------------------------|----------------------------------------------------------------------------------------------------|
| * Extension Type        | MULTISITE_OVERLAY ▼     |                                                                                                    |
| * Base Template         | BorderBase_v1 ▼         |                                                                                                    |
| * Extension Template    | MultiSiteOverlaySetup ▼ |                                                                                                    |
| * Source Fabric         | SITE_2                  |                                                                                                    |
| * Destination Fabric    | ▼                       |                                                                                                    |
| * Source Device         | ▼                       | <small>① VRF_LITE: Set switch role - Border; MULTISITE: Set switch role - "Border Gateway"</small> |
| * Source Interface      | ▼                       |                                                                                                    |
| * Destination Device    | ▼                       |                                                                                                    |
| * Destination Interface | ▼                       |                                                                                                    |

**Base Template**—*BorderBase\_v1* is auto-populated in this field. The *BorderBase\_v1* base template is a one-time configuration pushed to the BGW.

**Extension Template**—*MultiSiteOverlaySetup* is a setup template that contains the configuration that will be generated and pushed to the BGW to setup the corresponding inter-fabric connection. These templates are auto-populated with corresponding pre-packaged default templates based on your selection.

**Source Fabric**—This field is pre-populated with site2 since you are deploying the configurations in site2.

**Destination Fabric**—For the destination fabric, select the fabric that contains RS\_1, CORE.

**Source Device**—Choose BGW\_3 since the overlay connection is from BGW\_3 to RS\_1.

**Source Interface**—Typically, a loopback interface is created for the overlay. Choose the loopback interface amongst the 3 loopback interfaces you created as prerequisites. In this example, loopback0 is the BGP peer address.

**Destination Device**—Choose RS\_1 since the overlay connection is from BGW\_3 to RS\_1.

**Destination Interface**—Choose the destination interface. Choose the interface which is the BGP peer address. Note that the destination interface is not used in generating the configuration.

After filling up the Fabric Interconnect section, the screen looks like this.

### Add Inter-Fabric Connections



|                         |                         |
|-------------------------|-------------------------|
| * Extension Type        | MULTISITE_OVERLAY ▼     |
| * Base Template         | ▼                       |
| * Extension Template    | MultiSiteOverlaySetup ▼ |
| * Source Fabric         | SITE_2 ▼                |
| * Destination Fabric    | CORE ▼                  |
| * Source Device         | BGW_3 ▼                 |
| * Source Interface      | Loopback0 ▼             |
| * Destination Device    | RS_1 ▼                  |
| * Destination Interface | Loopback0 ▼             |

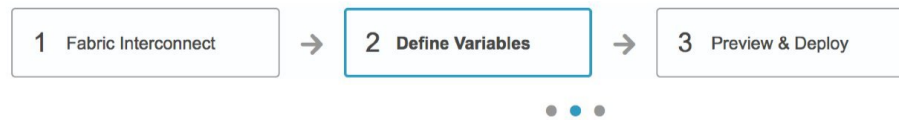
① VRF\_LITE: Set switch role - Border; MULTISITE: Set switch role - "Border Gateway"

|          |      |               |        |
|----------|------|---------------|--------|
| Previous | Next | Save & Deploy | Cancel |
|----------|------|---------------|--------|

Click **Next** to go to the **Define Variables** section.



## Add Inter-Fabric Connections



## ▼ Network Profile

| General               |                                                                   |
|-----------------------|-------------------------------------------------------------------|
| * IF_NAME             | <input type="text" value="Loopback0"/> ?                          |
| * Overlay Neighbor IP | <input type="text" value="10.101.101.101"/> ? <i>IPv4 address</i> |
| * NEIGHBOR_ASN        | <input type="text" value="65100"/> ?                              |

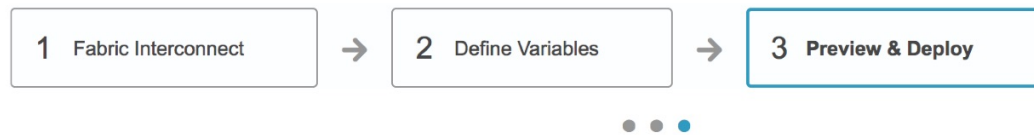
**IF\_NAME**—In this field, the source interface is auto-populated from the previous step.

**Overlay Neighbor IP**—Enter the IP address on RS\_1 that the overlay peers with. This is typically a loopback address.

**NEIGHBOR\_ASN**—This field is populated with the RS\_1's AS Number.

Click **Next** to go to the **Preview and Deploy** section.

## Add Inter-Fabric Connections

Switch: 

Generated Configuration:

```

router bgp 65002
 neighbor 10.101.101.101 remote-as 65100
 update-source Loopback0
 ebgp-multihop 5
 peer-type fabric-external
 address-family l2vpn evpn
 send-community
 send-community extended
 rewrite-evpn-rt-asn

```

[Previous](#)[Next](#)[Save & Deploy](#)[Cancel](#)

Here, you can preview the overlay configuration that will be deployed to BGW\_3. In this section, you can see that an overlay connection is being established from Loopback0 on BGW\_3 to the neighbor with AS Number 65100.

Note that no configuration will be pushed to the external device itself.

Click **Save and Deploy** to complete the task. This results in the configuration getting pushed to BGW\_3. The external connection will appear in the Fabric Extension screen.

Fabric Extension

Inter-Fabric Connections

Selected 0 / Total 2

| + X                                      |              | Show Quick Filter |                  |                   |                   |                    |                             |          |  |  |
|------------------------------------------|--------------|-------------------|------------------|-------------------|-------------------|--------------------|-----------------------------|----------|--|--|
| Type                                     | Source Fa... | Source Device     | Source Interface | Destination Fa... | Destination De... | Destination Int... | Configuration               | Status   |  |  |
| <input type="radio"/> MULTISITE_OVERLAY  | SITE_2       | BGW_3             | Loopback0        | CORE              | RS_1              | Loopback0          | <a href="#">View Config</a> | DEPLOYED |  |  |
| <input type="radio"/> MULTISITE_UNDERLAY | SITE_2       | BGW_3             | Ethernet4/3      | CORE              | RS_1              | Ethernet5/5        | <a href="#">View Config</a> | DEPLOYED |  |  |

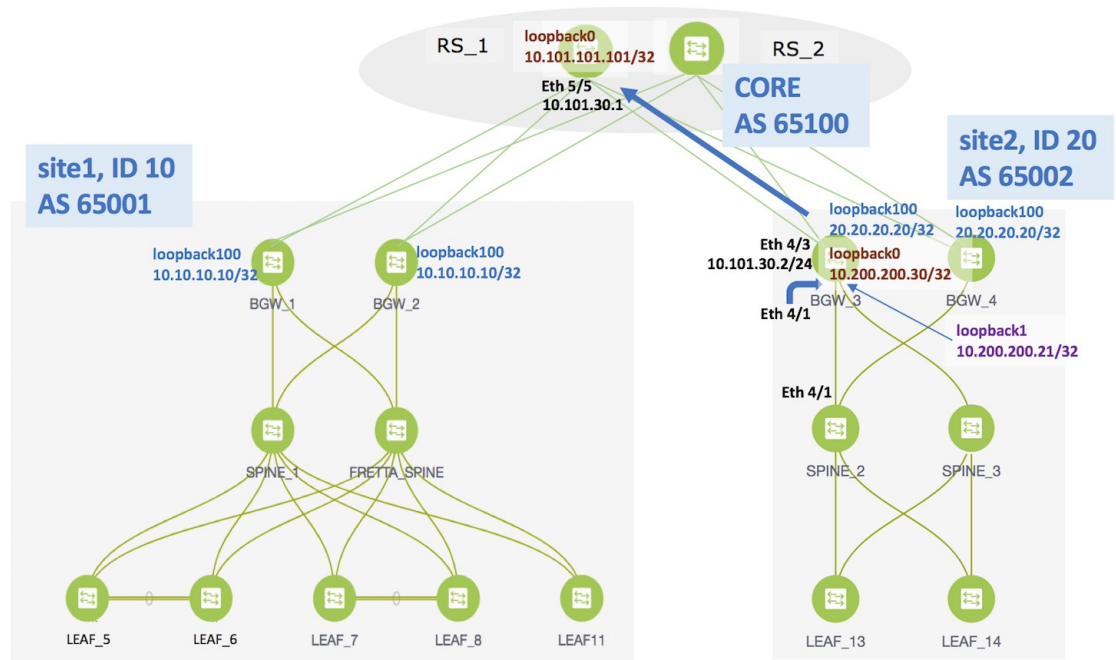
The view doesn't auto-refresh, hence the refresh button on the top right part of the screen needs to be clicked to trigger refresh. You can check the status of the deployment (Pending, Deployed, Failed) in the **Status** column. In case of FAILED or UNDEPLOYMENT FAILED status, use the hyperlink in the **Status** column to check the error messages for failure.

**Note**

Extensions will need to be deleted and then reconfigured in case of deployment failures. Currently there is no option to edit or redeploy an overlay or underlay extension.

## Other EVPN Multi-Site Configurations

At this stage, overlay and underlay EVPN Multi-Site configurations are provisioned on BGW\_3 towards RS\_1 (as shown by the arrow in the figure).



To complete EVPN Multi-Site configurations between site1 and site2 using DCNM, you should also configure as follows:

- **On site2**
  - EVPN Multi-Site configurations from BGW\_3 to RS\_2.
  - EVPN Multi-Site configurations from BGW\_4 to RS\_1 and RS\_2.
- **On site1**
  - EVPN Multi-Site configurations from BGW\_1 to RS\_1 and RS\_2.
  - EVPN Multi-Site configurations from BGW\_2 to RS\_1 and RS\_2.
- **On the route servers**
  - Apart from the DCNM provisioning on the BGWs of site1 and site2, you should enable appropriate configurations on RS\_1 and RS\_2 for connectivity between the route servers and the BGWs.

Sample RS\_1 configurations are provided in the Appendix for your reference.

As noted earlier, the end-to-end Multi-Site configurations through DCNM Top-Down provisioning include these 2 steps:

**(1) Multi-Site configurations on the BGWs (BGW\_1, BGW\_2, BGW\_3 and BGW\_4).**

**(2) Deploying Networks and VRF Instances on the leaf switches and the BGWs.**

At this stage, the first step explanation is complete. In the next part of the document, the networks' configuration (second step), is explained. After appropriate network configurations on the leaf switches and BGWs, server traffic will flow across the 2 sites for the deployed and extended networks and VRFs.

## Deploying Networks and VRF Instances

Typically, you create a fabric in DCNM, then create and deploy networks and VRFs on devices within the fabric on leaf switches, and then configure the BGWs for external connectivity. Though the focus of the document is external connectivity with EVPN Multi-Site configurations on BGWs using DCNM, for completeness and right context, network deployment on the BGWs is explained in this section. When EVPN Multi-Site deployment is completed, server traffic from these networks and VRFs on site2 will pass through a BGW (BGW\_3 or BGW\_4) towards site1.

### Deploying Networks on the BGWs

*Before you begin*—In this scenario, we will deploy two networks in site2, *MyNetwork\_10000* and *MyNetwork\_10001*, on the BGWs BGW\_3 and BGW\_4. You should ensure that you have already deployed the networks that you want to extend to site1 on the leaf switches ( LEAF\_13 and LEAF\_14 in this case).

After deploying the 2 networks on the leaf switches and the BGWs, the networks will be extended to site1. To know how to create a new fabric, network, and VRF, see LAN Fabric Provisioning section in the [DCNM user guide](#).

In the Select a Fabric page, click the **Continue** button at the top right part of the screen.

(After Multi-Site overlays and underlays are created, the DCNM GUI automatically takes you to the Select a Fabric page).

## Select a Fabric

Choose a fabric with appropriate switches where you want the Top Down functionality to be enabled or create a new fabric.

SITE\_2

 Fabric Extension Settings

OR

 Create a new fabric

After clicking **Continue**, the **Networks** page comes up.

We will deploy two new networks *MyNetwork\_10000* and *MyNetwork\_10001* on the BGWs. To do that, select the checkboxes (in the extreme left column).

Fabric Selection > Network Selection > Network Deployment > VRF View | Continue

Fabric Selected: SITE\_2

Selected 2 / Total 4

|                                     | Network Name    | Network ID | VRF Name     | IPv4 Gateway/Subnet | IPv6 Gateway/Prefix | Status     | VLAN ID |
|-------------------------------------|-----------------|------------|--------------|---------------------|---------------------|------------|---------|
| <input checked="" type="checkbox"/> | MyNetwork_10000 | 10000      | MyVRF_200000 | 10.1.10.1/24        | 10:1:A::1/48        | UNDEPLOYED |         |
| <input checked="" type="checkbox"/> | MyNetwork_10001 | 10001      | MyVRF_200000 | 10.1.11.1/24        |                     | UNDEPLOYED | 11      |
| <input type="checkbox"/>            | MyNetwork_10002 | 10002      | MyVRF_200002 | 10.1.12.1/24        | 10:1:C::1/48        | UNDEPLOYED |         |
| <input type="checkbox"/>            | MyNetwork_10003 | 10003      | NA           | 10.1.13.1/24        |                     | UNDEPLOYED |         |

Click the **Continue** button at the top right part of the screen. The Network Deployment page (Topology View) comes up. You can deploy networks on multiple switches simultaneously, but with the same role. So, deploy the selected networks on the BGWs.

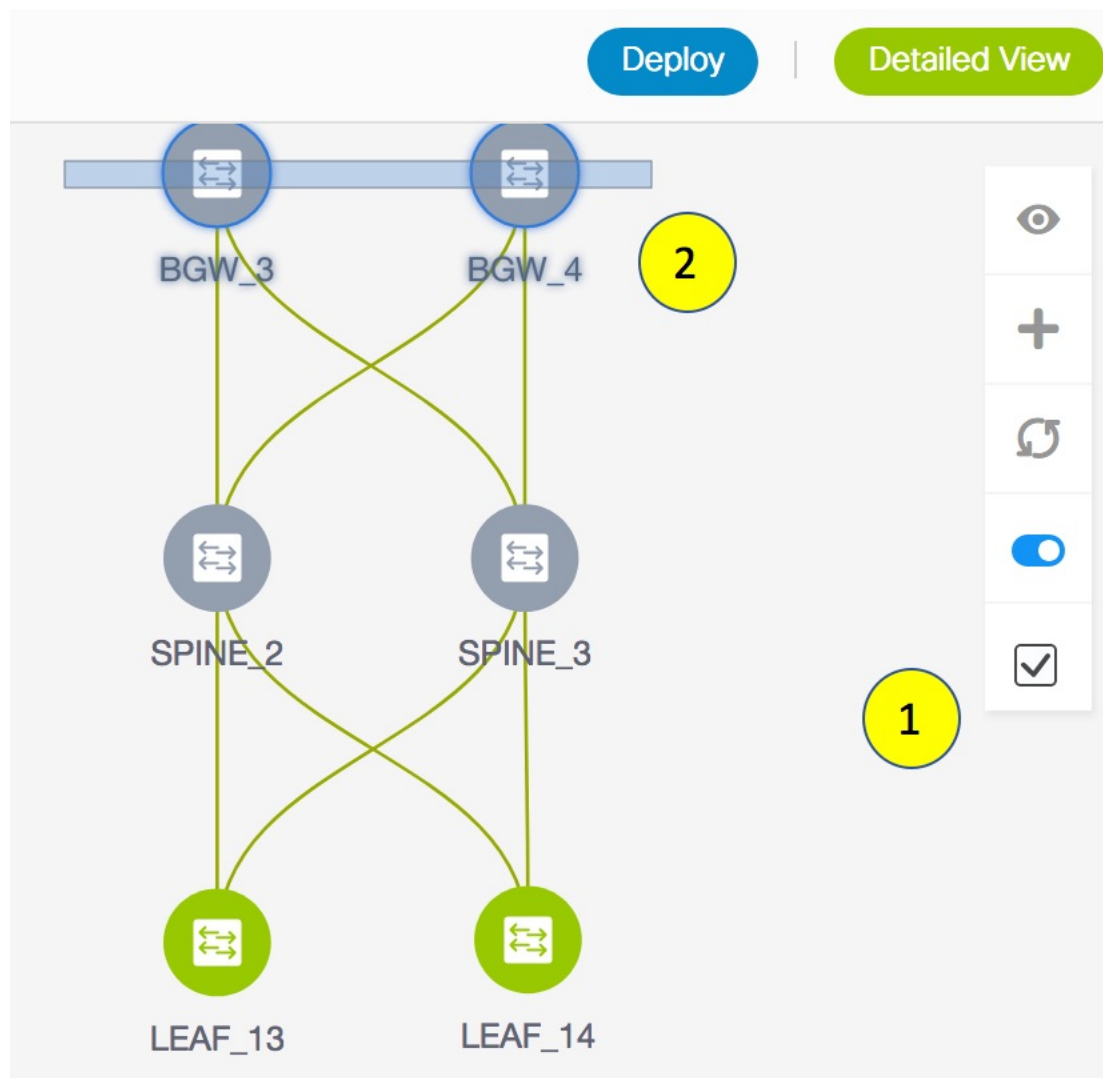


### Note

In the image, you can see that the networks are deployed on the leaf switches (green color indicates *deployed* status). Note that the color code (and hence the deployment state) on switches is contextual and specific to the selection. In this scenario, the deployed state only depicts that networks MYNetwork10000 and MYNetwork10001 are deployed on leaf switches LEAF\_13 and LEAF\_14. It does not display information about other (networks and VRFs) deployment instances, if any.

Select the multi-select check box at the bottom of the panel of options available at the right part of the page. (displayed as step 1 in the image).

Then, click your mouse (or track pad) and drag the cursor across BGW\_3 and BGW\_4. (step 2).



Immediately, the **Switches Deploy** screen (for networks) appears.

## Switches Deploy

**Fabric Name:** *SITE\_2*

MyNetwork\_10000

MyNetwork\_10001

**Deploy Options:**

Select the row and click on the cell to edit and save changes

| <input type="checkbox"/> | Switch | ▲ | VLAN | Extend    | Status     |
|--------------------------|--------|---|------|-----------|------------|
| <input type="checkbox"/> | BGW_3  |   | 10   | MULTISITE | NA         |
| <input type="checkbox"/> | BGW_4  |   | 10   | MULTISITE | UNDEPLOYED |

Save

A tab is displayed for each network. Click the checkbox next to the **Switch** column. Both the BGW check boxes will be selected automatically and the **Extension Details** section will appear at the bottom part of the screen.

In the **Extension Details** section, select the **Switch** checkbox (or ensure that you select the check box in each row) and click **Save** (bottom right part of your screen).

## Switches Deploy

*Fabric Name: SITE\_2*

MyNetwork\_10000

MyNetwork\_10001

*Deploy Options:*

Select the row and click on the cell to edit and save changes

| <input checked="" type="checkbox"/> | Switch | ▲ | VLAN | Extend    | Status     |
|-------------------------------------|--------|---|------|-----------|------------|
| <input checked="" type="checkbox"/> | BGW_3  |   | 10   | MULTISITE | NA         |
| <input checked="" type="checkbox"/> | BGW_4  |   | 10   | MULTISITE | UNDEPLOYED |

☒ *Extension Details*

| <input checked="" type="checkbox"/> | Switch | ▲ | Type      | IF_NAME   |
|-------------------------------------|--------|---|-----------|-----------|
| <input checked="" type="checkbox"/> | BGW_3  |   | MULTISITE | Loopback0 |
| <input checked="" type="checkbox"/> | BGW_3  |   | MULTISITE | Loopback0 |
| <input checked="" type="checkbox"/> | BGW_4  |   | MULTISITE | Loopback0 |

Save

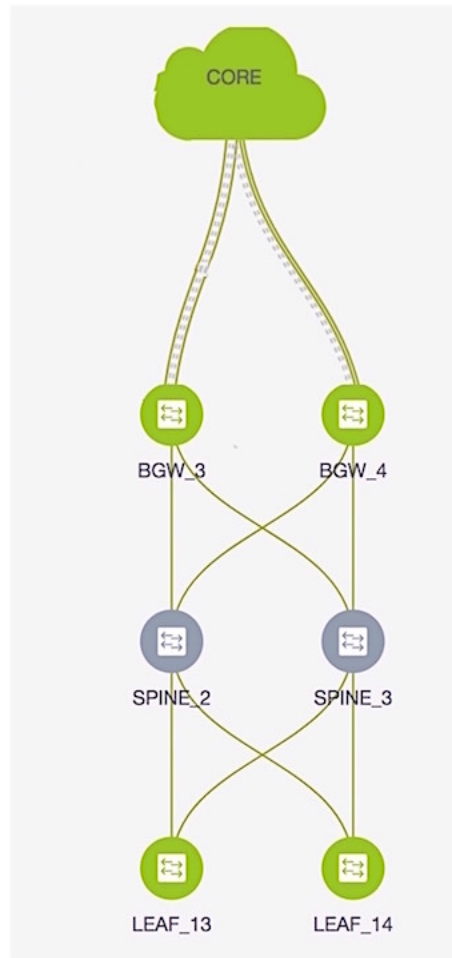
After saving the details in this screen, the Network Deployment screen (Topology view) appears.

BGW\_3 and BGW\_4 will be displayed in blue color, indicating pending deployment. If you want to check your configurations again, click on the Preview (eye) icon.

After you verify that the configurations that are generated from the profiles are correct for the selected switches, click the **Deploy** button (on the top right part of the screen) to deploy the MYNetwork10000 and MYNetwork10001 network configurations on BGW\_3 and BGW\_4.

DCNM shows the deployment status in the topology by highlighting the switch icons with different colors, yellow for *In Progress* and green for *Deployed*.



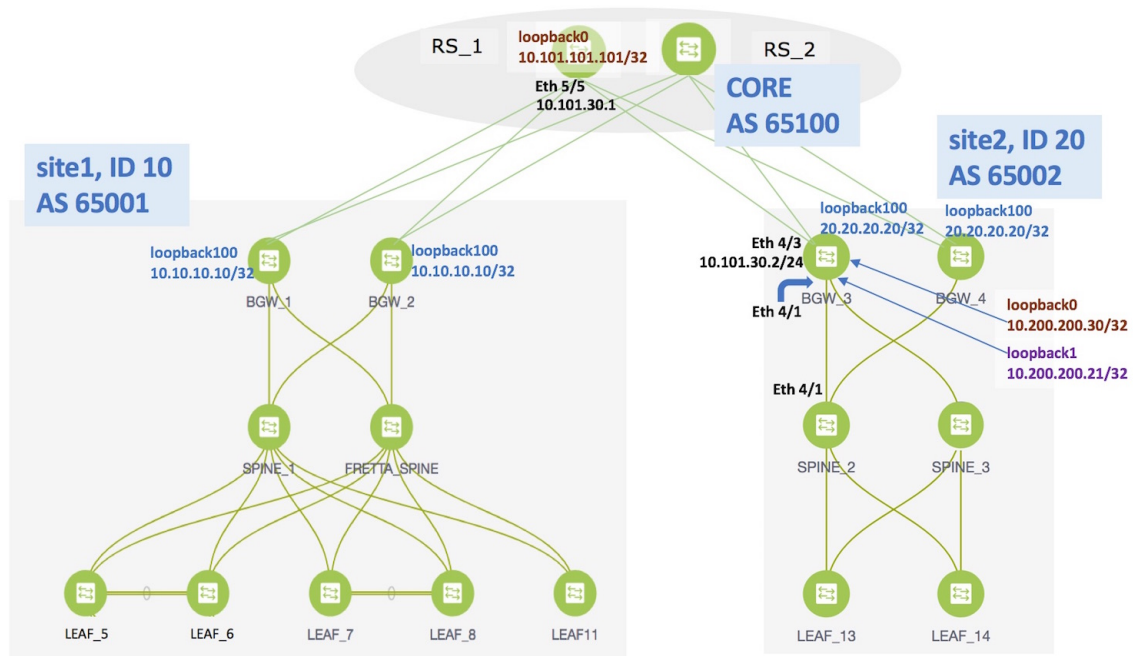


From the snapshot, you can see that the 2 networks MYNetwork10000 and MYNetwork10001 have been implemented on the leaf switches and BGWs.

After configurations in site2 are complete, configure the following in site1 too.

## Configurations in site1

Provision the networks MYNetwork10000 and MYNetwork10001 on the leaf switches (LEAF\_5, LEAF\_6, LEAF\_7, LEAF\_8, LEAF\_11) and the BGWs (BGW\_1 and BGW\_2).



As noted in the EVPN Multi-Site configuration section, enable the following for end-to-end configuration:

- Since DCNM does not provision configurations for RS\_1 and RS\_2 (devices directly connected to the BGWs), enable appropriate configurations on these devices.
- Configure the EVPN Multi-Site feature on the site1 BGWs (as explained in this document) so that server traffic from the 2 networks can flow to site2 and back.

## Additional References

| Document Title and Link                                                 | Document Description                                                      |
|-------------------------------------------------------------------------|---------------------------------------------------------------------------|
| <a href="#">VXLAN EVPN Multi-Site Design and Deployment White Paper</a> | This document explains Multi-Site design and deployment in detail.        |
| <a href="#">Configuring VXLAN EVPN Multi-Site</a>                       | This document explains manual configurations for the Multi-Site solution. |

# Appendix

## Route Server Configurations

**RS\_1 configuration example for the overlay**—The following configurations are enabled on RS1, and reproduced here for reference.



### Note

*switch(config)#* refers to the global configuration mode. To access this mode, type the following on your switch: **switch# configure terminal**.

```
switch(config)#

route-map ALL-PATHS permit 100
 set path-selection all advertise
route-map RMAP-REDIST-DIRECT permit 10
 match tag 12345
route-map UNCHANGED permit 10
 set ip next-hop unchanged

switch(config)#

interface loopback0
 ip address 10.101.101.101/32 tag 12345
line vty
router bgp 65100
 router-id 10.101.101.101
 address-family ipv4 unicast
 redistribute direct route-map RMAP-REDIST-DIRECT
 maximum-paths 4
 additional-paths send
 additional-paths receive
 additional-paths selection route-map ALL-PATHS
 address-family l2vpn evpn
 retain route-target all
 template peer OVERLAY-PEERING
 update-source loopback0
 ebgp-multihop 5
 address-family l2vpn evpn
 send-community both
 route-map UNCHANGED out
 neighbor 10.100.100.10
 inherit peer OVERLAY-PEERING
 remote-as 65001
 address-family l2vpn evpn
 rewrite-evpn-rt-asn
 route-map UNCHANGED out
 neighbor 10.100.100.20
 inherit peer OVERLAY-PEERING
 remote-as 65001
 address-family l2vpn evpn
 rewrite-evpn-rt-asn
 route-map UNCHANGED out
 neighbor 10.101.11.2
 remote-as 65101
 update-source Ethernet5/1
 address-family ipv4 unicast
 next-hop-self
 neighbor 10.101.12.2
 remote-as 65101
 update-source Ethernet5/2
 address-family ipv4 unicast
```

```

 next-hop-self
neighbor 10.101.13.2
 remote-as 65102
 update-source Ethernet5/3
 address-family ipv4 unicast
 next-hop-self
neighbor 10.101.14.2
 remote-as 65102
 update-source Ethernet5/4
 address-family ipv4 unicast
 next-hop-self
neighbor 10.101.30.2
 remote-as 65002
 update-source Ethernet5/5
 address-family ipv4 unicast
 next-hop-self
neighbor 10.101.40.2
 remote-as 65002
 update-source Ethernet5/6
 address-family ipv4 unicast
 next-hop-self
neighbor 10.200.200.30
 remote-as 65002
 update-source loopback0
 ebgp-multihop 5
 address-family l2vpn evpn
 rewrite-evpn-rt-asn
 send-community both
 route-map UNCHANGED out
neighbor 10.200.200.40
 remote-as 65002
 update-source loopback0
 ebgp-multihop 5
 address-family l2vpn evpn
 rewrite-evpn-rt-asn
 send-community both
 route-map UNCHANGED out

```



## Border Provisioning Use Case in VXLAN BGP EVPN Fabrics - VRF Lite

External connectivity from data centers is a prime requirement. Virtual eXtensible Local Area Network (VXLAN) Border Gateway Protocol (BGP) Ethernet VPN (EVPN) based data center fabrics provide east-west connectivity by distributing IP-MAC reachability information among various devices within the fabric. Tenants, typically represented by virtual routing and forwarding instances (VRFs) can procure external connectivity via special nodes called borders. In this way, tenant workloads in one data center fabric can have Layer 3 connectivity to the global Internet as well as to workloads in other data center fabrics. This chapter describes LAN Fabric provisioning of the Nexus 9000-based border devices through the Cisco® Data Center Network Manager (DCNM) for the VRF Lite use case. Two common deployment models are covered:

- IP Core model - VRF extension from border devices connected to edge routers that in turn provide connectivity to other fabrics and/or connectivity to the global Internet.
- B2B model - VRF extension from border devices directly connected to border devices in other fabrics.
- [Prerequisites](#) , page 359
- [Sample Scenario](#), page 360
- [VRF Lite Inter-Fabric Configuration](#) , page 362
- [Deploying VRF Instances on Border Leafs](#), page 372
- [Undeploying VRF Instances on the Border Leafs](#) , page 381
- [Additional References](#), page 386
- [Appendix](#) , page 386

### Prerequisites

- The DCNM version required to support this feature is 10.4(2).
- The VRF Lite feature requires Cisco Nexus 9000 Series NX-OS Release 7.0(3)I6(2) or later.

- Familiarity with VXLAN BGP EVPN data center fabric architecture and top-down based LAN fabric provisioning through the DCNM.
- Fully configured VXLAN BGP EVPN fabrics including underlay and overlay configurations on the various leaf and spine devices.
  - VXLAN BGP EVPN fabrics (and their interconnection) can be configured manually or using DCNM. This document explains the process to connect the fabrics through DCNM. So, you should know how to configure and deploy a VXLAN BGP EVPN fabric through DCNM. For more details, see the LAN Fabric Provisioning section under the Configure chapter in [Cisco DCNM Web Client Online Help, 10.4\(2\) Release](#).

**Note**

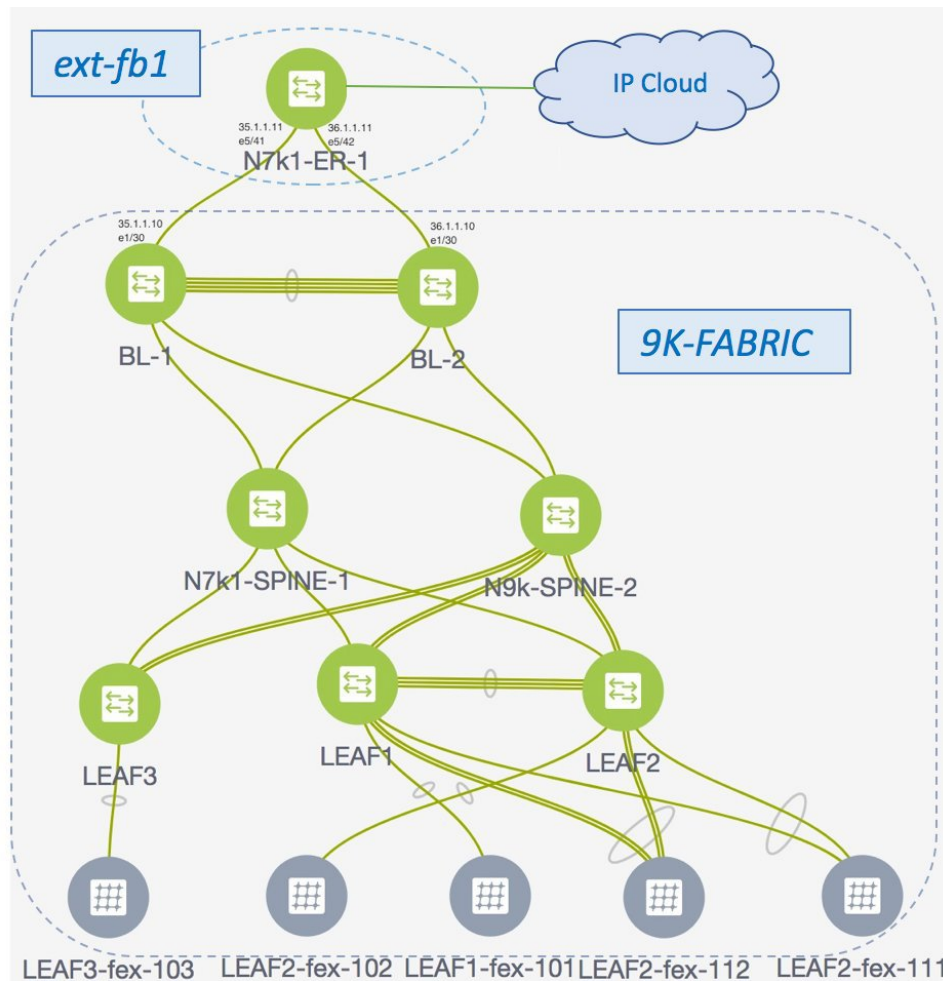
For an explanation on the VRF Lite feature, see the [Cisco Programmable Fabric with VXLAN BGP EVPN Configuration Guide](#) document.

## Sample Scenario

The VRF Lite feature is explained through an example scenario. Consider a VXLAN BGP EVPN fabric, *9K-FABRIC*, where the border devices are connected through an edge router to a shared IP core. This document will show you how to enable Layer 3 traffic between hosts in the two fabrics.

**Note**

In the IP core scenario, DCNM allows provisioning for fabric switches and the border devices. The Edge Router (ER) connected to the border devices needs to be manually configured (in *9K-FABRIC*, the edge router N7k1-ER1 [or ER1] is connected to BL1 and BL2). Appropriate CLI templates can also be employed to deploy this configuration on the Cisco Nexus 7000 Series edge devices using DCNM. In the B2B setup, the border leafs on both fabrics can be configured through DCNM.



Network configurations for the fabric is provisioned through DCNM. For external Layer 3 reachability from hosts connected to leaf switches within the fabric, border devices need to be provisioned with the appropriate VRF configuration. Multiple border devices in the fabric ensure redundancy in the case of failures as well as effective load distribution.

**Note**

The DCI functions VRF Lite and VRF Lite + Multi-Site are in the scope of this document, but MPLS L3VPN and LISP technologies are not in the scope of this document.

**VRF Lite**—This requires setting up the border leaf configuration for enabling the VRF Lite feature by establishing eBGP peering from the border leaf to appropriate external devices, either ERs or border leafs in other fabrics. In this context, border leafs are special devices that allow clear control and data plane segregation from one site to another while allowing for policy enforcement points for any inter-fabric traffic.

The steps involved to enable VRF Lite and traffic flow across the fabric are:

- 1 **Inter-Fabric Connect**—Top-Down deployment for the VRF Lite feature configures route maps and an eBGP session in the default VRF through an interface (parent interface) connected to the ER. This is a one-time setup for each ER connected to a border leaf.

- 2 *VRF Extensions*—For each VRF that is to be extended, a unique sub interface towards the ER and an eBGP session through this sub interface is configured on the border leaf. This is a per-VRF configuration. For a B2B scenario, VRF extension configurations on all border leafs can be deployed through DCNM itself. For the IP core setup, the corresponding configurations have to be manually enabled on the ERs.

**Note**

VRF extensions on a vPC setup of a pair of border leafs have to be enabled on both the vPC peers. DCNM does not allow you to enable extensions on a single vPC switch.

The end-to-end configurations can be split into these 2 steps:

### 1 VRF Lite inter-fabric configurations on the border leafs (BL-1, BL-2)

- 1 VRF Lite function on BL-1 and BL-2, the vPC pair of border leafs in *9K-FABRIC* that are directly connected to ER-1.
- 2 Configurations on edge routers ER-1 and ER-2 - These configurations are not in the scope of DCNM provisioning and this document. It is mentioned here for completeness and sample configurations are provided in the Appendix section. Again, as mentioned earlier, appropriate CLI templates can be employed to provision the edge router if it is a Nexus device.

### 2 Deploying VRF instances on the border leafs (BL-1, BL-2)

For this example, multiple VRFs will be configured on the vPC pair of border leafs in *9K-FABRIC*.

After successful VRF Lite deployment at the border leaf and on the edge routers, traffic will flow between them.

**Note**

In the DCNM topology view, the lines connecting devices managed by DCNM (for example, BL-1 to N7k1-SPINE-1) symbolize a physical cable connection. They do not indicate that the connection is functional and traffic flows between them.

To start off with, let us consider VRF Lite provisioning on border leafs BL-1 and BL-2 through DCNM Top-Down LAN Fabric Provisioning.

# VRF Lite Inter-Fabric Configuration

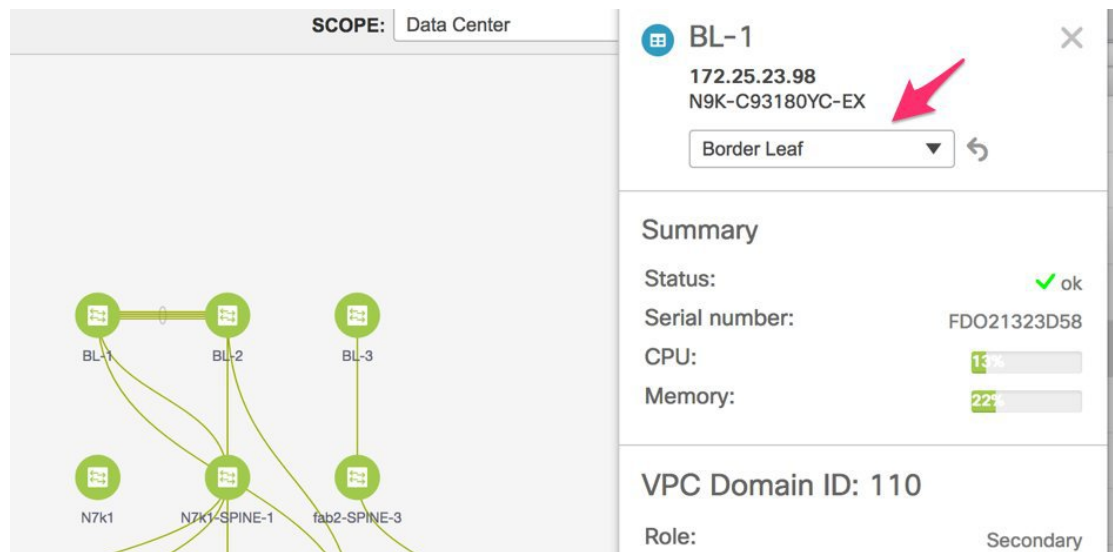
## Prerequisite Configuration for VRF Lite Configuration

- Setting the *Leaf* role to *Border Leaf*— By default a device will be treated as a leaf switch. You need to change its role to that of a border leaf.

To update the switch role, login to DCNM, and click **Topology** from the main menu at the left part of the screen. In the Topology screen, from the **Scope** drop down box, select the fabric and click on the BL-1. A screen pops up with the switch information.

Change the entry from *Leaf* to *Border Leaf* as shown in the image.





This is required for configuring the VRF Lite feature through the DCNM GUI. After completing the VRF Lite specific prerequisites, start DCNM VRF Lite configuration on BL-1 with extensions to the edge router ER-1.

## VRF Lite Inter-Fabric Configuration (on BL-1 towards ER-1 in 9K-FABRIC)

From the Cisco DCNM Web Client, choose **Configure > LAN Fabric Provisioning > Network Deployment**. The LAN Fabric Provisioning page appears.

Click **Continue**. The **Select a Fabric** page comes up.

### Select a Fabric

Choose a fabric with appropriate switches where you want the Top Down functionality to be enabled or create a new fabric.

9K-FABRIC

Fabric Extension Settings

OR

Create a new fabric

Select *9K-FABRIC* from the drop-down box since you are configuring border leaf *BL-1* in the fabric *9K-FABRIC*.

In the same page, click **Fabric Extension Settings** since the purpose of this task is to allow *9K-FABRIC* to communicate to external fabrics through ER-1 and ER-2. The **Fabric Extension** screen comes up.

Fabric Extension ✕

Inter-Fabric Connections Selected 0 / Total 0 ↻

+ ✕
Show Quick Filter ▼

| Type              | Source Fabric | Source Device | Source Interface | Destination Fabric | Destination Device | Destination Interface | Configuration | Status |
|-------------------|---------------|---------------|------------------|--------------------|--------------------|-----------------------|---------------|--------|
| No data available |               |               |                  |                    |                    |                       |               |        |

The **Inter-Fabric Connections** section lists previously created external connections from the border leafs in *9K-FABRIC*. This section is empty as this is the first time you are adding an external connection. Each row represents a physical or logical connection between a border leaf in *9K-FABRIC* and an external device in another fabric. For each connection, the source fabric, source device, source interface, destination fabric, destination device, and destination interface are listed along with the type of external connectivity.

*To extend the fabric through VRF-Lite, you should first create an extension.*

## Extension from BL-1 to ER-1

Click on the + icon (at the top left part of the screen) to add a new external connection. The **Add Inter-Fabric Connection** screen appears.

Add Inter-Fabric Connections ✕

1 Fabric Interconnect

→

2 Define Variables

→

3 Preview & Deploy

● ● ●

\*

Extension Type

VRF\_LITE ▼

Base Template

BorderBase\_v1 ▼

Extension Template

FabricSetup ▼

Source Fabric

9K-FABRIC

Destination Fabric

▼

Source Device

▼

Source Interface

▼

Destination Device

▼

Destination Interface

▼

ⓘ VRF\_LITE: Set switch role - Border; MULTISITE: Set switch role - "Border Gateway"

Previous

Next

Save & Deploy

Cancel

By default, VRF\_LITE is populated in the **Extension Type** field. Since the inter-fabric extension is through VRF Lite, retain this entry.

**Base Template**—By default, the *BorderBase\_v1* base template is populated. This template represents a one-time configuration pushed to the border leaf BL-1.

Cisco DCNM Web Client Online Help, 10.4(2) Release

364

**Extension Template**—*FabricSetup*, as the name indicates, represents the template that outputs the configuration required to setup the inter-fabric connection. As opposed to the configuration represented by the Base Template that is applied only once per border leaf, the Extension Template generated configuration is executed once for every inter-fabric connection.

These templates are auto-populated with corresponding pre-packaged default templates based on your selection.

**Source Fabric**—This field is pre-populated with *9K-FABRIC* since the VRF Lite connection is between BL-1 in *9K-FABRIC* and ER-1 in the *ext-fb1* fabric.

**Destination Fabric**—Choose *ext-fb1*.

**Source Device** and **Source Interface**—Choose *BL-1* as the source device and an Ethernet interface that needs to be connected to ER-1.

**Destination Device** and **Destination Interface**—Choose *ER-1* as the destination device and the Ethernet interface that connects to the border leaf BL-1.

Note that based on the selection of the source device and source interface, the destination information will be auto-populated based on CDP information if available. There is extra validation performed to ensure that the destination external device is indeed part of the destination fabric.

After filling up the Fabric Interconnect section, the screen looks like this.

### Add Inter-Fabric Connections

1 Fabric Interconnect → 2 Define Variables → 3 Preview & Deploy

• • •

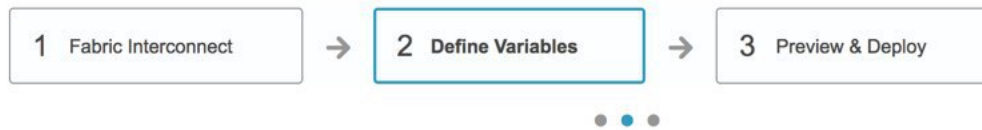
|                         |               |   |
|-------------------------|---------------|---|
| * Extension Type        | VRF_LITE      | ▼ |
| * Base Template         | BorderBase_v1 | ▼ |
| * Extension Template    | FabricSetup   | ▼ |
| * Source Fabric         | 9K-FABRIC     |   |
| * Destination Fabric    | ext-fb1       | ▼ |
| * Source Device         | BL-1          | ▼ |
| * Source Interface      | Ethernet1/30  | ▼ |
| * Destination Device    | N7k1-ER-1     | ▼ |
| * Destination Interface | Ethernet5/41  | ▼ |

① VRF\_LITE: Set switch role - Border; MULTISITE: Set switch role - "Border Gateway"

Previous Next Save & Deploy Cancel

Click **Next** to go to the **Define Variables** section.

## Add Inter-Fabric Connections



## ▼ Network Profile

| General          |                |
|------------------|----------------|
| * IF_NAME        | Ethernet1/30 ? |
| * IP_MASK        | 35.1.1.10/24 ? |
| * NEIGHBOR_IP    | 35.1.1.11 ?    |
| * NEIGHBOR_ASN   | 3000 ?         |
| * Extension Type | VRF_LITE ?     |

**IF\_NAME**—In this field, the interface name is auto-populated from the previous step.

**Interface IP\_MASK**—Fill up this field with the IP address of the BL-1 interface that connects to ER-1.

**NEIGHBOR\_IP**—Fill up this field with the IP address of the ER-1 interface that connects to BL-1.

**NEIGHBOR\_ASN**—In this field, the AS number of ER-1 will be auto-populated.

Now that all the information is filled in, click **Next** to go to the **Preview and Deploy** section. The two sections of the screen are shown in the 2 images:

### Add Inter-Fabric Connections

1 Fabric Interconnect

→

2 Define Variables

→

3 Preview & Deploy

Switch:

Generated Configuration:

```
ip prefix-list default-route seq 5 permit 0.0.0.0/0 le 1
ip prefix-list host-route seq 5 permit 0.0.0.0/0 eq 32
route-map EXTCON-RMAP-FILTER deny 10
 match ip address prefix-list default-route
route-map EXTCON-RMAP-FILTER deny 20
 match ip address prefix-list host-route
route-map EXTCON-RMAP-FILTER permit 1000

ipv6 prefix-list default-route-v6 seq 5 permit 0::/0
ipv6 prefix-list host-route-v6 seq 5 permit 0::/0 eq 128
route-map EXTCON-RMAP-FILTER-V6 deny 10
 match ipv6 address prefix-list default-route-v6
route-map EXTCON-RMAP-FILTER-V6 deny 20
 match ip address prefix-list host-route-v6
route-map EXTCON-RMAP-FILTER-V6 permit 1000

interface Ethernet1/30
```

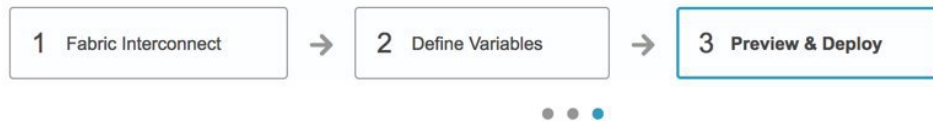
Previous

Next

Save & Deploy

Cancel

## Add Inter-Fabric Connections

Switch: 

Generated Configuration:

```

interface Ethernet1/30
 no switchport
 ip address 35.1.1.10/24
 no shutdown

router bgp 2000
 address-family ipv4 unicast
 redistribute direct route-map RMAP-REDIST-DIRECT
 neighbor 35.1.1.11 remote-as 3000
 update-source Ethernet1/30
 address-family ipv4 unicast
 next-hop-self

```

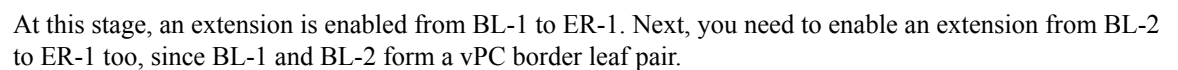
**Note**

In an Inter-Fabric connection, if one border leaf is connected to more than one ER or border leaf, the prefix-list and route map configurations are pushed only for the first fabric extension instance. Similarly when deleting fabric extension instances on a border leaf, the global configurations (prefix-list and route-maps) are removed from the border leaf only after the last fabric extension instance is deleted.

In this screen, you can preview the configuration that will be deployed to BL-1. Note that no configuration will be pushed to the external device (also known as edge router) itself.

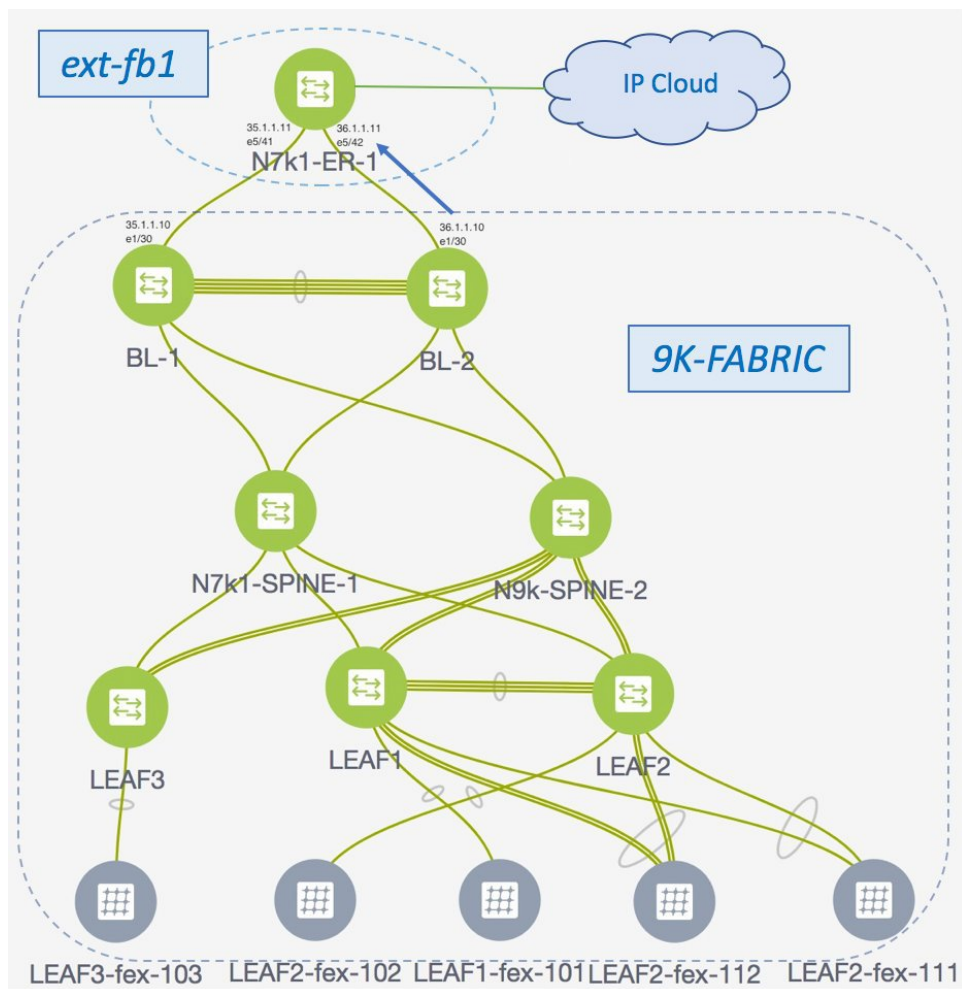
A one-time configuration of route maps along with the parent interface connection is displayed. Also, you can see that BGP peering information in the default routing table is configured for BL-1. The corresponding BGP configurations should be enabled manually on ER-1.

Click **Save and Deploy** to complete the task. This results in the configuration getting pushed to BL-1. The external connection will appear in the Fabric Extension screen.



As described in the previous section, enable an extension from BL-2 to ER-1. After configurations are pushed to BL-2, an extension will be enabled from BL-2 to ER-1, as shown in the screen shot.





A preview of the configurations on BL-2 is given in these 2 screen shots.



## Add Inter-Fabric Connections



1 Fabric Interconnect



2 Define Variables



3 Preview &amp; Deploy

Switch: 

## Generated Configuration:

```
ip prefix-list default-route seq 5 permit 0.0.0.0/0 le 1
ip prefix-list host-route seq 5 permit 0.0.0.0/0 eq 32
route-map EXTCON-RMAP-FILTER deny 10
 match ip address prefix-list default-route
route-map EXTCON-RMAP-FILTER deny 20
 match ip address prefix-list host-route
route-map EXTCON-RMAP-FILTER permit 1000

ipv6 prefix-list default-route-v6 seq 5 permit 0::/0
ipv6 prefix-list host-route-v6 seq 5 permit 0::/0 eq 128
route-map EXTCON-RMAP-FILTER-V6 deny 10
 match ipv6 address prefix-list default-route-v6
route-map EXTCON-RMAP-FILTER-V6 deny 20
 match ip address prefix-list host-route-v6
route-map EXTCON-RMAP-FILTER-V6 permit 1000

interface Ethernet1/30
```

Generated Config

Previous

Next

Save &amp; Deploy

Cancel

## Add Inter-Fabric Connections



1 Fabric Interconnect

→

2 Define Variables

→

3 Preview & Deploy

Switch: BL-2

Generated Configuration:

```

interface Ethernet1/30
 no switchport
 ip address 36.1.1.10/24
 no shutdown

router bgp 2000
 address-family ipv4 unicast
 redistribute direct route-map RMAP-REDIST-DIRECT
 neighbor 36.1.1.11 remote-as 3000
 update-source Ethernet1/30
 address-family ipv4 unicast
 next-hop-self

```

Previous

Next

Save & Deploy

Cancel

## Edge Router Configurations

Apart from the DCNM provisioning on the border leafs in the two fabrics, you should also enable appropriate configurations on ER-1 for connectivity between the edge router and the border leafs. Sample ER-1 configuration is provided in the *Appendix* section for your reference.

**What to do next**—As noted earlier, the end-to-end VRF-Lite configurations through DCNM Top-Down provisioning includes these 2 steps:

- 1 VRF Lite inter-fabric configurations on the border leafs (BL-1, BL-2)
- 2 Deploying VRF Instances on the border leafs (BL-1, BL-2)

At this stage, the first step explanation is complete. The next section explains how VRF extension configuration is pushed to the border leafs.

## Deploying VRF Instances on Border Leafs

*Before you begin*—In this scenario, we will deploy three VRF instances, *MyVRF-50016*, *MyVRF-50018*, and *MyVRF-50019* on the border leafs BL-1 and BL-2 in *9K-FABRIC*. You should ensure that you have already deployed the corresponding network(s) on the fabric's leaf switches.

After deploying one network on the leaf switches, you will have to deploy the associated VRF on the border leafs so that the network(s) can be extended from/to the *9K-FABRIC*. To know how to create a new fabric, network, and VRF, see LAN Fabric Provisioning section in the [DCNM user guide](#).

**Note**

VRF extension on vPC switch pairs can be either deployed or undeployed together on both the peers.

In the Select a Fabric page, click the **Continue** button at the top right part of the screen.

(After VRF Lite extensions are created, the DCNM GUI automatically takes you to the Select a Fabric page).

## Select a Fabric

Choose a fabric with appropriate switches where you want the Top Down functionality to be enabled or create a new fabric.

9K-FABRIC

 [Fabric Extension Settings](#)

OR

[+ Create a new fabric](#)



Ensure that you select *9K-FABRIC* in the drop-down box and click **Continue** (at the top right part of the screen). After clicking **Continue**, the **Networks** page comes up.

Click on **VRF View**. The **VRFs** page comes up.

We will deploy 3 new VRF instances *MyVRF-50016*, *MyVRF-50018*, and *MyVRF-50019* on the border leafs. To do that, select the checkboxes (in the extreme left column).

Fabric Selection > Network Selection > Network Deployment > [Network View](#) | [Continue](#)

Fabric Selected: 9K-FABRIC

VRFs Selected 3 / Total 138  

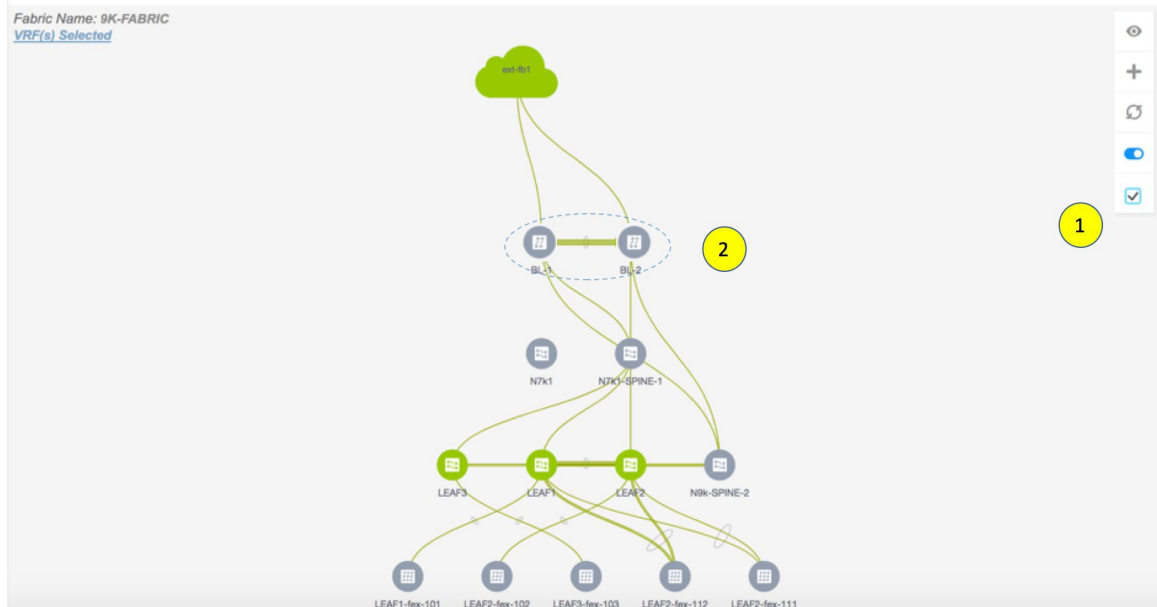
| <input type="checkbox"/>            | VRF Name    | VRF ID | Status   |
|-------------------------------------|-------------|--------|----------|
| <input type="checkbox"/>            | MyVRF_50000 | 50000  | DEPLOYED |
| <input checked="" type="checkbox"/> | MyVRF_50016 | 50016  | DEPLOYED |
| <input checked="" type="checkbox"/> | MyVRF_50018 | 50018  | NA       |
| <input checked="" type="checkbox"/> | MyVRF_50019 | 50019  | NA       |
| <input type="checkbox"/>            | MyVRF_50500 | 50500  | DEPLOYED |

DEPLOYED

Click the **Continue** button at the top right part of the screen. The VRF Deployment page (Topology View) comes up. You can deploy VRFs on multiple switches simultaneously, but with the same role. So, deploy the selected VRFs on the border leafs.

**Note**

In the image, you can see that the VRF instances are deployed on the leaf switches (green color indicates deployed status). Note that the color code, and hence the deployment state on switches is contextual and specific to the selection. In this scenario, the deployed state only depicts that the 3 selected VRFs are deployed on leaf switches LEAF3, LEAF1 and LEAF2. It does not display information about other VRF deployment instances, if any.



Select the multi-select check box at the bottom of the panel of options available (Step 1 in the image) at the right part of the page.

Then, click your mouse (or track pad) and drag the cursor across BL-1 and BL-2 (Step 2 in the image). Note that this is a vPC switch pair of border leafs.

Immediately, the **Switches Deploy** screen (for VRFs) appears.

**Note**

For VRF extension on vPC switches, error messages will be displayed if only one border leaf is selected for VRF Lite extension, or if both the switches are selected for extension but only one (on no) border leaf extension is selected with extension details. Error messages:

**Switches Deploy**

**Deploy Options:**

Select the row and click on the cell to edit and save changes

| <input type="checkbox"/>            | Switch | VLAN | Extend   | Status |
|-------------------------------------|--------|------|----------|--------|
| <input checked="" type="checkbox"/> | BL-1   | 2002 | VRF_LITE | NA     |
| <input checked="" type="checkbox"/> | BL-2   | 2002 | NONE     | NA     |

☒ **Extension Details**

| <input type="checkbox"/> | Switch | Type     | IF_NAME      | DOT1Q_ID | IP_MASK      |
|--------------------------|--------|----------|--------------|----------|--------------|
| <input type="checkbox"/> | BL-1   | VRF_LITE | Ethernet1/30 | 4        | 35.1.1.10/24 |

**Save**

**Warning:** You have edited a VPC device BL-1. Edit the Extension-type of the Paired Device to match its peer. **OK**

**Switches Deploy**

**Deploy Options:**

Select the row and click on the cell to edit and save changes

| Switch                                   | VLAN | Extend   | Status |
|------------------------------------------|------|----------|--------|
| <input checked="" type="checkbox"/> BL-1 | 2002 | VRF_LITE | NA     |
| <input checked="" type="checkbox"/> BL-2 | 2002 | VRF_LITE | NA     |

☒ **Extension Details**

| Switch                                   | Type     | IF_NAME      | DOT1Q_ID | IP_MASK      |
|------------------------------------------|----------|--------------|----------|--------------|
| <input checked="" type="checkbox"/> BL-1 | VRF_LITE | Ethernet1/30 | 4        | 35.1.1.10/24 |
| <input type="checkbox"/> BL-2            | VRF_LITE | Ethernet1/30 | 4        | 36.1.1.10/24 |

**Save**

In the VRF extension on vPC switch pairs scenario, a tab is displayed for each VRF.

Click the checkbox next to the **Switch** column. Both the border leaf check boxes will be selected automatically and the **Extension Details** section will appear at the bottom part of the screen.

In the **Extension Details** section, select the **Switch** checkbox (or ensure that you select the check box in each row). This is how the screen looks when you select both the switches and the Extension Details section.

## Switches Deploy

Fabric Name: 9K-FABRIC

MyVRF\_50016 MyVRF\_50018 MyVRF\_50019

## Deploy Options:

① Select the row and click on the cell to edit and save changes

| <input type="checkbox"/>            | Switch | ▲ | VLAN | Extend   | Status             |
|-------------------------------------|--------|---|------|----------|--------------------|
| <input checked="" type="checkbox"/> | BL-1   |   | 2001 | VRF_LITE | DEPLOYMENT PENDING |
| <input checked="" type="checkbox"/> | BL-2   |   | 2001 | VRF_LITE | DEPLOYMENT PENDING |

☒ Extension Details

| <input type="checkbox"/>            | Switch | ▲ | Type     | IF_NAME      | DOT1Q_ID | IP_MASK      |
|-------------------------------------|--------|---|----------|--------------|----------|--------------|
| <input checked="" type="checkbox"/> | BL-1   |   | VRF_LITE | Ethernet1/30 | 3        | 35.1.1.10/24 |
| <input checked="" type="checkbox"/> | BL-2   |   | VRF_LITE | Ethernet1/30 | 3        | 36.1.1.10/24 |

OK

Cancel

Now, select the MyVRF\_50018 and MyVRF\_50019 and similarly update relevant parameters.

## Switches Deploy

Fabric Name: 9K-FABRIC

MyVRF\_50016 MyVRF\_50018 MyVRF\_50019

## Deploy Options:

① Select the row and click on the cell to edit and save changes

| <input type="checkbox"/>            | Switch | ▲ | VLAN | Extend   | Status             |
|-------------------------------------|--------|---|------|----------|--------------------|
| <input checked="" type="checkbox"/> | BL-1   |   | 2002 | VRF_LITE | DEPLOYMENT PENDING |
| <input checked="" type="checkbox"/> | BL-2   |   | 2002 | VRF_LITE | DEPLOYMENT PENDING |

☒ Extension Details

| <input type="checkbox"/>            | Switch | ▲ | Type     | IF_NAME      | DOT1Q_ID | IP_MASK      |
|-------------------------------------|--------|---|----------|--------------|----------|--------------|
| <input checked="" type="checkbox"/> | BL-1   |   | VRF_LITE | Ethernet1/30 | 4        | 35.1.1.10/24 |
| <input checked="" type="checkbox"/> | BL-2   |   | VRF_LITE | Ethernet1/30 | 4        | 36.1.1.10/24 |

## Deploying VRF Instances on Border Leafs

## Switches Deploy

Fabric Name: 9K-FABRIC

MyVRF\_50016 MyVRF\_50018 MyVRF\_50019

## Deploy Options:

① Select the row and click on the cell to edit and save changes

| <input type="checkbox"/>            | Switch | ▲ | VLAN | Extend   | Status             |
|-------------------------------------|--------|---|------|----------|--------------------|
| <input checked="" type="checkbox"/> | BL-1   |   | 2003 | VRF_LITE | DEPLOYMENT PENDING |
| <input checked="" type="checkbox"/> | BL-2   |   | 2003 | VRF_LITE | DEPLOYMENT PENDING |

☒ Extension Details

| <input type="checkbox"/>            | Switch | ▲ | Type     | IF_NAME      | DOT1Q_ID | IP_MASK      |
|-------------------------------------|--------|---|----------|--------------|----------|--------------|
| <input checked="" type="checkbox"/> | BL-1   |   | VRF_LITE | Ethernet1/30 | 5        | 35.1.1.10/24 |
| <input checked="" type="checkbox"/> | BL-2   |   | VRF_LITE | Ethernet1/30 | 5        | 36.1.1.10/24 |

Click the **Save** button at the bottom right part of the Switches Deploy screen to save all VRFs' configurations on the selected switches. The VRF Deployment screen (Topology view) appears.

BL-1 and BL-2 icons will be displayed in blue color, indicating that a deployment is pending. If you want to check your configurations, click on the Preview (eye) icon.

The screenshot displays the Cisco DCNM Web Client interface. On the left, a 'Preview Configuration' window is open, showing the generated configuration for switch BL-1 and VRF MyVRF\_50016. The configuration includes BGP settings, route maps, and interface configurations for Ethernet1/30.3. On the right, the 'Network Deployment' topology view is visible, showing a hierarchical network diagram with a cloud at the top, followed by N7K1 and N7K2, then N7K-SPINE-1 and N7K-SPINE-2, and finally a row of LEAFs (LEAF3, LEAF1, LEAF2, LEAF4, LEAF5) at the bottom. The BL-1 and BL-2 icons are highlighted in blue, indicating a pending deployment.

**Preview Configuration**

Select a Switch: BL-1 Select a VRF: MyVRF\_50016

Generated Configuration:

```

maximum-paths ibgp 2

network 0::/0

neighbor 35.1.1.11 remote-as 3000
address-family ipv4 unicast
send-community both
route-map EXTCON-RMAP-FILTER out

neighbor 35:1:1:1:2 remote-as 3000
address-family ipv6 unicast
send-community both
route-map EXTCON-RMAP-FILTER-V6 out

interface Ethernet1/30.3
encapsulation dot1q 3
vrf member MyVRF_50016
ip address 35.1.1.10/24
ipv6 address 35:1:1:1:1/64
no shutdown

configure terminal

```

Generated Config



## Preview Configuration

Select a Switch:

BL-2

Select a VRF

MyVRF\_50019

Generated Configuration:

```

configure profile 9K-FABRIC-Default_VRF_Extension-50019
vlan 2003
 vn-segment 50019
 interface vlan 2003
 vrf member MyVRF_50019
 ip forward
 ipv6 forward
 no ip redirects
 no ipv6 redirects
 mtu 9216
 no shut

interface nve 1
 member vni 50019 associate-vrf

vrf context MyVRF_50019
 vni 50019
 rd auto
 address-family ipv4 unicast
 route-target both auto
 route-target both auto evpn

 ip route 0/0 36.1.1.11
 address-family ipv6 unicast
 route-target both auto
 route-target both auto evpn

 ipv6 route 0::/0 36.1.1.1::2

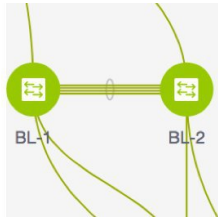
```

Generated Co

You can select a switch and a VRF to view corresponding configurations. Configuration details of MyVRF\_5016 that is pushed to BL-1 are included in the *Appendix* section.

After you verify that the configurations that are generated from the profiles are correct for the selected switches, click the **Deploy** button (on the top right part of the Topology View screen) to deploy the MyVRF\_50016, MyVRF\_50018, and MyVRF\_50019 VRF configurations on BL-1 and BL-2.

DCNM shows the deployment status in the topology by highlighting the switch icons with different colors, yellow for *In Progress*, green for *Deployed*, and red for *Error* status.



From the snapshot, you can see that the MyVRF\_50016, MyVRF\_50018, and MyVRF\_50019 VRF configurations have been implemented on the vPC border leafs of the *9K-FABRIC*. You can also click the **Detailed View** option to see the status.

| Fabric Selection > Network Selection > Network Deployment > |             |         | Topology View        |          |
|-------------------------------------------------------------|-------------|---------|----------------------|----------|
| Fabric Name: 9K-FABRIC VRF(s) Selected                      |             |         | Selected 0 / Total 9 |          |
| <input type="checkbox"/>                                    | Deploy      | Preview | History              | Show All |
| <input type="checkbox"/>                                    | Name        | Switch  | Ports                | Status   |
| <input type="checkbox"/>                                    | MyVRF_50016 | BL-1    |                      | DEPLOYED |
| <input type="checkbox"/>                                    | MyVRF_50016 | BL-2    |                      | DEPLOYED |
| <input type="checkbox"/>                                    | MyVRF_50016 | LEAF1   |                      | DEPLOYED |
| <input type="checkbox"/>                                    | MyVRF_50016 | LEAF2   |                      | DEPLOYED |
| <input type="checkbox"/>                                    | MyVRF_50016 | LEAF3   |                      | DEPLOYED |
| <input type="checkbox"/>                                    | MyVRF_50018 | BL-1    |                      | DEPLOYED |
| <input type="checkbox"/>                                    | MyVRF_50018 | BL-2    |                      | DEPLOYED |
| <input type="checkbox"/>                                    | MyVRF_50019 | BL-1    |                      | DEPLOYED |
| <input type="checkbox"/>                                    | MyVRF_50019 | BL-2    |                      | DEPLOYED |

After configurations in *9K-FABRIC* are complete, you should enable configurations in Fabric2 too.

## Resource Manager

Resource Manager gives information of all the resources allocated/deployed on each device per fabric. This includes the network VLANs, VRF VLANs, and the sub interface dot1q identifiers employed for the VRF Lite extension. Once a VRF is undeployed, the associated resources on the Resource Manager will be unallocated/updated immediately.

To access the Resource Manager page, click **Configure > LAN Fabric Provisioning > Resource Manager**

As we can see in the screenshot below, after deploying VRF instances *MyVRF\_50016*, *MyVRF\_50018* and *MyVRF\_50019* on the vPC border leafs, the Resource Manager has the associated VLAN-VRF mapping displayed.

Configure / LAN Fabric Provisioning / Resource Manager

Fabrics: 9K-FABRIC Switches: BL-1

Resource Objects

Selected 0 / Total 4

Show All

| <input type="checkbox"/> | Scope Type ▲ | Allocated ID | Allocated To | Resource Type     | Is Allocated? | Allocated On           |
|--------------------------|--------------|--------------|--------------|-------------------|---------------|------------------------|
| <input type="checkbox"/> | Device       | 2002         | MyVRF_50018  | TOP_DOWN_VRF_VLAN | Yes           | 2/14/2018, 4:18:52 PM  |
| <input type="checkbox"/> | Device       | 2000         | MyVRF_50000  | TOP_DOWN_VRF_VLAN | Yes           | 1/31/2018, 12:59:06 AM |
| <input type="checkbox"/> | Device       | 2001         | MyVRF_50016  | TOP_DOWN_VRF_VLAN | Yes           | 2/6/2018, 2:27:46 PM   |
| <input type="checkbox"/> | Device       | 2003         | MyVRF_50019  | TOP_DOWN_VRF_VLAN | Yes           | 2/14/2018, 4:20:16 PM  |

The VRF instances MyVRF\_50016, MyVRF\_50018, and MyVRF\_50019 are deployed on BL-1, with their corresponding VLANs 2001, 2002, and 2003.

## Undeploying VRF Instances on the Border Leafs

VRFs can be deployed/undeployed on the border leafs. The following steps will demonstrate undeployment of VRFs on the vPC border leafs.

For *9K-FABRIC*, navigate to the **Networks** page and click **VRF View**. The VRFs page will be displayed.

Select MyVRF-50018 and MyVRF-50019 and click **Continue**.

Fabric Selection > Network Selection > Network Deployment > Network View | Continue

Fabric Selected: 9K-FABRIC

VRFs

Selected 2 / Total 138

Show All

| <input type="checkbox"/>            | VRF Name ▲  | VRF ID | Status     |
|-------------------------------------|-------------|--------|------------|
| <input type="checkbox"/>            | MyVRF_50000 | 50000  | DEPLOYED   |
| <input type="checkbox"/>            | MyVRF_50016 | 50016  | DEPLOYED   |
| <input checked="" type="checkbox"/> | MyVRF_50018 | 50018  | DEPLOYED   |
| <input checked="" type="checkbox"/> | MyVRF_50019 | 50019  | DEPLOYED   |
| <input type="checkbox"/>            | MyVRF_50500 | 50500  | DEPLOYED   |
| <input type="checkbox"/>            | VRF 50011   | 50011  | UNDEPLOYED |

The Topology View page is displayed. Follow similar steps as described in the Deploying VRFs section on the vPC border leafs.

Select BL-1 and BL-2 switches in the topology page. The **Switches Deploy** screen will be displayed.

A tab is displayed for each VRF. MyVRF\_50018 is currently selected in the below screenshot.

## Undeploying VRF Instances on the Border Leafs

## Switches Deploy

Fabric Name: 9K-FABRIC

MyVRF\_50018 MyVRF\_50019

## Deploy Options:

Select the row and click on the cell to edit and save changes

| <input type="checkbox"/>            | Switch | ▲ | VLAN | Extend   | Status   |
|-------------------------------------|--------|---|------|----------|----------|
| <input checked="" type="checkbox"/> | BL-1   |   | 2002 | VRF_LITE | DEPLOYED |
| <input checked="" type="checkbox"/> | BL-2   |   | 2002 | VRF_LITE | DEPLOYED |

☒ Extension Details

| <input type="checkbox"/>            | Switch | ▲ | Type     | IF_NAME      | DOT1Q_ID | IP_MASK      |
|-------------------------------------|--------|---|----------|--------------|----------|--------------|
| <input checked="" type="checkbox"/> | BL-1   |   | VRF_LITE | Ethernet1/30 | 4        | 35.1.1.10/24 |
| <input checked="" type="checkbox"/> | BL-2   |   | VRF_LITE | Ethernet1/30 | 4        | 36.1.1.10/24 |

Double click the checkbox next to the Switch column or uncheck the check box next to BL-1 and BL-2. Both of the check boxes will be de-selected and the Extension Details section will disappear at the bottom part of the screen.

## Switches Deploy

Fabric Name: 9K-FABRIC

MyVRF\_50018 MyVRF\_50019

## Deploy Options:

Select the row and click on the cell to edit and save changes

| <input type="checkbox"/> | Switch | ▲ | VLAN | Extend   | Status   |
|--------------------------|--------|---|------|----------|----------|
| <input type="checkbox"/> | BL-1   |   | 2002 | VRF_LITE | DEPLOYED |
| <input type="checkbox"/> | BL-2   |   | 2002 | VRF_LITE | DEPLOYED |

Save

Now, select the MyVRF\_50019 and update similarly.

## Switches Deploy

Fabric Name: 9K-FABRIC

MyVRF\_50018 MyVRF\_50019

## Deploy Options:

① Select the row and click on the cell to edit and save changes

| <input type="checkbox"/> | Switch | VLAN | Extend   | Status   |
|--------------------------|--------|------|----------|----------|
| <input type="checkbox"/> | BL-1   | 2003 | VRF_LITE | DEPLOYED |
| <input type="checkbox"/> | BL-2   | 2003 | VRF_LITE | DEPLOYED |

Status: Sortable

Save

Click on the **Save** button at the bottom right part of the Switches Deploy screen to save undeployment of all VRFs configurations on the selected switches. The VRF Deployment screen (Topology view) appears.

Similar to the deployment process, the BL-1 and BL-2 switch icons will be displayed in blue color, indicating pending undeployment. You can preview the information by clicking the Preview (eye) icon.

The configurations for MyVRF\_50018 on BL-1 switch will be removed as displayed in the following screen. You can select a switch and VRF to view corresponding configurations.

## Preview Configuration

Select a Switch:

BL-1

Select a VRF

MyVRF\_50018

## Generated Configuration:

```
configure terminal
no apply profile 9K-FABRIC-Default_VRF_Extension-50018
no configure profile 9K-FABRIC-Default_VRF_Extension-50018
```

After you verify that the configuration profiles that will be removed are correct for the selected switches, click the **Deploy** button (on the top right part of the screen) to undeploy the MyVRF\_50018 and MyVRF\_50019 configurations on BL-1 and BL-2.

## Resource Manager Update

As we can see in the screenshot below, after undeploying the VRFs *MyVRF\_50018* and *MyVRF\_50019* on the vPC border leafs, the Resource Manager has the associated VLAN-VRF mapping removed/unallocated.

## Remove VRF Lite Inter-fabric configuration on vPC border leafs

Configure / LAN Fabric Provisioning / Resource Manager

Fabrics: 9K-FABRIC Switches: BL-1

Resource Objects Selected 0 / Total 2

Show All

| <input type="checkbox"/> | Scope Type ▲ | Allocated ID | Allocated To | Resource Type     | Is Allocated? | Allocated On           |
|--------------------------|--------------|--------------|--------------|-------------------|---------------|------------------------|
| <input type="checkbox"/> | Device       | 2000         | MyVRF_50000  | TOP_DOWN_VRF_VLAN | Yes           | 1/31/2018, 12:59:06 AM |
| <input type="checkbox"/> | Device       | 2001         | MyVRF_50016  | TOP_DOWN_VRF_VLAN | Yes           | 2/6/2018, 2:27:46 PM   |

In the screenshot, it shows that MyVRF\_50018 and MyVRF\_50019 that was deployed on BL-1 with VLAN 2002 and 2003 is now removed/unallocated.

Configure / LAN Fabric Provisioning / Resource Manager

Fabrics: 9K-FABRIC Switches: BL-2

Resource Objects Selected 0 / Total 2

Show All

| <input type="checkbox"/> | Scope Type ▲ | Allocated ID | Allocated To | Resource Type     | Is Allocated? | Allocated On           |
|--------------------------|--------------|--------------|--------------|-------------------|---------------|------------------------|
| <input type="checkbox"/> | Device       | 2000         | MyVRF_50000  | TOP_DOWN_VRF_VLAN | Yes           | 1/31/2018, 12:59:06 AM |
| <input type="checkbox"/> | Device       | 2001         | MyVRF_50016  | TOP_DOWN_VRF_VLAN | Yes           | 2/6/2018, 2:27:46 PM   |

## Remove VRF Lite Inter-fabric configuration on vPC border leafs

VRF Lite inter-fabric configuration can also be removed in a similar manner as long as there are no VRF extensions enabled over that connection. The following steps will demonstrate removal of BL-1 and BL-2 VRF Lite inter-fabric connections.

Follow similar steps as described in the VRF Lite inter-fabric configuration for BL-1 in *9K-FABRIC*.

From the Cisco DCNM Web Client, choose **Configure > LAN Fabric Provisioning > Network Deployment**.

Select *9K-FABRIC* from the drop-down box and click **Fabric Extension Settings**. The **Fabric Extension** screen comes up.

## Fabric Extension

## Inter-Fabric Connections

Selected 0 / Total 2

| Type                           | Source Fabric | Source Device | Source Interface | Destination Fa... | Destination De... | Destination Int... | Configuration               | Status   |
|--------------------------------|---------------|---------------|------------------|-------------------|-------------------|--------------------|-----------------------------|----------|
| <input type="radio"/> VRF_LITE | 9K-FABRIC     | BL-1          | Ethernet1/30     | ext-fb1           | N7k1-ER-1         | Ethernet5/41       | <a href="#">View Config</a> | DEPLOYED |
| <input type="radio"/> VRF_LITE | 9K-FABRIC     | BL-2          | Ethernet1/30     | ext-fb1           | N7k1-ER-1         | Ethernet5/42       | <a href="#">View Config</a> | DEPLOYED |

Click on the radio button next to VRF\_LITE in the first row with Source Device *BL-1*.

Then, click the **X** button to delete this entry.

## Fabric Extension

## Inter-Fabric Connections

Selected 1 / Total 2

| Type                                      | Source Fabric | Source Device | Source Interface | Destination Fa... | Destination De... | Destination Int... | Configuration               | Status     |
|-------------------------------------------|---------------|---------------|------------------|-------------------|-------------------|--------------------|-----------------------------|------------|
| <input checked="" type="radio"/> VRF_LITE | 9K-FABRIC     | BL-1          | Ethernet1/30     | ext-fb1           | N7k1-ER-1         | Ethernet5/41       | <a href="#">View Config</a> | DEPLOYMENT |
| <input type="radio"/> VRF_LITE            | 9K-FABRIC     | BL-2          | Ethernet1/30     | ext-fb1           | N7k1-ER-1         | Ethernet5/42       | <a href="#">View Config</a> | DEPLOYED   |

The next screen shows that the BL-1 inter-fabric connection is removed from the fabric extension list.

## Fabric Extension

## Inter-Fabric Connections

Selected 0 / Total 1

| Type                           | Source Fabric | Source Device | Source Interface | Destination Fa... | Destination De... | Destination Int... | Configuration               | Status   |
|--------------------------------|---------------|---------------|------------------|-------------------|-------------------|--------------------|-----------------------------|----------|
| <input type="radio"/> VRF_LITE | 9K-FABRIC     | BL-2          | Ethernet1/30     | ext-fb1           | N7k1-ER-1         | Ethernet5/42       | <a href="#">View Config</a> | DEPLOYED |

Similarly, select BL-2 and click **X** to remove the BL-2 inter-fabric connection. After both BL-1 and BL-2 VRF Lite inter-fabric connections are removed, the Fabric Extension screen will have no entries.

Fabric Extension

Inter-Fabric Connections Selected 0 / Total 0

Show Quick Filter

| Type              | Source Fabric | Source Device | Source Interface | Destination Fa... | Destination De... | Destination Int... | Configuration | Status |
|-------------------|---------------|---------------|------------------|-------------------|-------------------|--------------------|---------------|--------|
| No data available |               |               |                  |                   |                   |                    |               |        |

## Additional References

| Document Title and Link                                                           | Document Description                                         |
|-----------------------------------------------------------------------------------|--------------------------------------------------------------|
| <a href="#">Cisco Programmable Fabric with VXLAN BGP EVPN Configuration Guide</a> | This document explains external connectivity using VRF Lite. |

## Appendix

### Edge Router Configurations

**ER-1 Configuration Example for vPC Border Leafs**—The following configurations are enabled on ER-1 for inter-fabric connections to BL-1 and BL-2 (vPC border leafs), and reproduced here for reference.



**Note**

*switch(config)#* refers to the global configuration mode. To access this mode, type the following on your switch: **switch# configure terminal**.

```
switch(config)#

interface Ethernet5/41 ## ER-1 interface to BL-1 (vpc BL peer)
 ip address 35.1.1.11/24
 no shutdown

interface Ethernet5/42 ## ER-1 interface to BL-2 (vpc BL peer)
 ip address 36.1.1.11/24
 no shutdown

router bgp 3000 ## eBGP sessions
 neighbor 35.1.1.10 remote-as 2000 ###Peering to BL-1 (eBGP)
 update-source Ethernet5/41
 address-family ipv4 unicast
 next-hop-self
```



```

neighbor 36.1.1.10 remote-as 2000 ###Peering to BL-2 (eBGP)
update-source Ethernet5/42
address-family ipv4 unicast
next-hop-self

```

The following configurations are manually enabled on ER-1 for VRF extension to the vPC border leafs:

```

configure profile 9K-FABRIC-Default_VRF_Extension-50016
vrf context MyVRF_50016
vni 50016
address-family ipv4 unicast
route-target import 65000:3
route-target export 65000:3
rd 3000:3
interface Ethernet5/41.3
encapsulation dot1Q 3
vrf member MyVRF_50016
ip address 35.1.1.11/24
ipv6 address 35:1:1:1::2/64
no shutdown
interface Ethernet5/42.3
encapsulation dot1Q 3
vrf member MyVRF_50016
ip address 36.1.1.11/24
ipv6 address 36:1:1:1::2/64
no shutdown
router bgp 3000
vrf MyVRF_50016
address-family ipv4 unicast
maximum-paths ibgp 2
neighbor 35.1.1.10 remote-as 2000
address-family ipv4 unicast
send-community both
neighbor 36.1.1.10 remote-as 2000
address-family ipv4 unicast
send-community both

```

### Configurations Pushed to BL-1 Through DCNM:

VRF extension pushed to BL-1 through DCNM

```

Route map
ip prefix-list default-route seq 5 permit 0.0.0.0/0 le 1
ip prefix-list host-route seq 5 permit 0.0.0.0/0 eq 32
route-map EXTCON-RMAP-FILTER deny 10
match ip address prefix-list default-route
route-map EXTCON-RMAP-FILTER deny 20
match ip address prefix-list host-route
route-map EXTCON-RMAP-FILTER permit 1000

ipv6 prefix-list default-route-v6 seq 5 permit 0::/0
ipv6 prefix-list host-route-v6 seq 5 permit 0::/0 eq 128
route-map EXTCON-RMAP-FILTER-V6 deny 10
match ipv6 address prefix-list default-route-v6
route-map EXTCON-RMAP-FILTER-V6 deny 20
match ip address prefix-list host-route-v6
route-map EXTCON-RMAP-FILTER-V6 permit 1000

VRF-Lite interface of BL-1
interface Ethernet1/30
no switchport
ip address 35.1.1.10/24
no shutdown

External BGP (eBGP) session of BL-1
router bgp 2000
address-family ipv4 unicast
redistribute direct route-map RMAP-REDIST-DIRECT
neighbor 35.1.1.11 remote-as 3000

```

```

update-source Ethernet1/30
address-family ipv4 unicast
next-hop-self

```

The following configuration profile is pushed through DCNM when MyVRF\_50016 is deployed on BL-1:

```

configure profile 9K-FABRIC-Default_VRF_Extension-50016
vlan 2001
 vn-segment 50016
 interface vlan 2001
 vrf member MyVRF_50016
 ip forward
 ipv6 forward
 no ip redirects
 no ipv6 redirects
 mtu 9216
 no shut

interface nve 1
 member vni 50016 associate-vrf

vrf context MyVRF_50016
 vni 50016
 rd auto
 address-family ipv4 unicast
 route-target both auto
 route-target both auto evpn
 ip route 0/0 35.1.1.11
 address-family ipv6 unicast
 route-target both auto
 route-target both auto evpn
 ipv6 route 0::/0 35.1.1.1.2

router bgp 2000
 vrf MyVRF_50016 ## bgp VRF configured
 address-family ipv4 unicast
 advertise l2vpn evpn
 redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
 maximum-paths ibgp 2
 network 0/0
 address-family ipv6 unicast
 advertise l2vpn evpn
 redistribute direct route-map FABRIC-RMAP-REDIST-SUBNET
 maximum-paths ibgp 2
 network 0::/0
 neighbor 35.1.1.11 remote-as 3000
 address-family ipv4 unicast
 send-community both
 route-map EXTCON-RMAP-FILTER out
 neighbor 35.1.1.1.2 remote-as 3000
 address-family ipv6 unicast
 send-community both
 route-map EXTCON-RMAP-FILTER-V6 out

interface Ethernet1/30.3 #sub interface member of VRF deployed
 encapsulation dot1q 3
 vrf member MyVRF_50016
 ip address 35.1.1.10/24
 ipv6 address 35:1:1:1::1/64
 no shutdown

configure terminal
 apply profile 9K-FABRIC-Default_VRF_Extension-50016

```