



CHAPTER 4

Cisco DCNM Web Client

Using Cisco DCNM Web Client, you can monitor Cisco MDS and Nexus family switch events, performance and inventory, and perform minor administrative tasks.

The default user credentials to access Cisco DCNM, Release 10.0.x are as configured during the deployment of the installers.

Cisco DCNM Web Client provides the following features:

- [Navigating DCNM Web Client, page 4-1](#)
- [Downloading Cisco DCNM-SAN Client, page 4-3](#)
- [Downloading Cisco Device Manager Client, page 4-4](#)
- [Viewing Dashboard Information, page 4-4](#)
- [Viewing Topology Information, page 4-4](#)
- [Viewing Inventory Information, page 4-5](#)
- [Viewing Monitor Information, page 4-5](#)
- [Viewing Administration Information, page 4-5](#)
- [Using Cisco DCNM Web Client with SSL, page 4-5](#)
- [Enhancements in Cisco DCNM Release 10.1\(x\), page 4-7](#)

Navigating DCNM Web Client

Cisco Data Center Network Manager (DCNM) is a management system for the Cisco Unified Fabric. It enables you to provision, monitor, and troubleshoot the data center network infrastructure. It provides visibility and control of the unified data center. Cisco DCNM provides a comprehensive feature set that meets the routing, switching, and storage administration needs of data centers. Cisco DCNM streamlines the provisioning for the unified fabric and monitors the SAN and LAN components. Cisco DCNM provides a high level of visibility and control through a single web based management console for Cisco Nexus, Cisco MDS, and Cisco Unified Computing System (UCS) products. During the DCNM installation, you can choose to install applications related to Unified Fabric only for Unified Fabric-mode installations.

The DCNM Web Client has standardized certain navigation conventions.

- [Scope Menu, page 4-2](#)
- [Admin Menu, page 4-2](#)
- [Table and Filtering Navigation, page 4-2](#)

- [Printing, page 4-2](#)
- [Exporting to a File, page 4-2](#)
- [Sorting Columns, page 4-3](#)
- [Cisco DCNM Web Search Engine, page 4-3](#)

Scope Menu

Beginning with Cisco NX-OS Release 6.x, a new drop-down list called Scope is added to Cisco DCNM Web Client that applies to all pages except the Administration and Configure pages.

You can use the scope menu to filter network information by:

- Data Center
- Default_LAN
- Default_SAN
- Individual Fabric Various other custom scopes created by the users.

The features accessible from the tabs are limited to the areas that you choose in the filter tree.

Admin Menu

You can use the admin menu to:

- **DCNM SAN:** Launch the SAN Client.
- **DCNM DM:** Launch the Device Manager Client which is part of the SAN option.
- **Change Password:** Changes the password for the current logged in user.
- **Help Content:** Pops out the online help of the current page.
- **About:** Display the information about Cisco Data Center Network Manager.
- **Logout:** Logout from the DCNM Web Client.

Table and Filtering Navigation

Some tables that can be filtered will have a filter option to view subsets of the information. Either choose the filter menu or click **Filter**. An editable row at the top of the table appears. Enter values into the table cells and click **Return** to display matching rows.

Printing

Click **Print** to view the table in a printer-friendly format. You can then print the page from the browser.

Exporting to a File

An Export icon is in the upper right corner of some tables or top right corner of the window. Click this icon to export the data to Microsoft Excel.

Sorting Columns

Not all columns are sortable but you can click a sortable column head to sort the information for that column.

Cisco DCNM Web Search Engine

The search engine helps you to locate records according to the following search criteria:

- Search by Name.
- Search by IP Address.
- Search by WWN.
- Search by Alias.
- Search by MAC Address.
- Search by Serial Number.

Using the Cisco DCNM Search Engine

-
- Step 1** Click **Search box** on the top right corner of the main window.
You see the search text box.
- Step 2** Use the drop-down to search by:
- Name
 - IP Address
 - WWN
 - Alias
 - MAC Address
 - Serial Number
- Step 3** Enter the value based on the search option and click the arrow to begin the search.
The search results are displayed in a new window.

Downloading Cisco DCNM-SAN Client

You must use Cisco DCNM Web Client to launch Cisco DCNM-SAN Client.

-
- Step 1** On the top right of the DCNM Web Client home screen, click the settings icon next to the login user.
Select **DCNM-SAN** option.
- Step 2** If you have the latest Java version installed, a Warning message is displayed.
- Step 3** Click **Run with the latest version** button.
- Step 4** Enter the user credentials to log on to Cisco DCNM-SAN client. This message appears only the first time you launch Cisco DCNM-SAN Client.

Downloading Cisco Device Manager Client

You must use Cisco DCNM Web Client to Install Cisco Device Manager client.



Note

Device Manager Client is part of the SAN option.

Step 1 On the top right of the DCNM Web Client home screen, click the settings icon next to the login user. Select **DCNM DM** option.

Step 2 If you have the latest Java version installed, a Warning message is displayed.



Note

Cisco DCNM Device Manager supports JRE versions 1.6 and 1.7. Follow the instructions in the Cisco Device Manager installer wizard to proceed with the installation.

Step 3 Once the installation is complete, enter the user credentials to log on to the Cisco Device Manager client.

Viewing Dashboard Information

The Cisco DCNM Web Client dashboard gives you comprehensive information of the following:

- [Summary](#) - You can view the summary dashboard which displays the overall functioning of all the devices connected. It gives you daily statistics of the connected devices. New panels has been introduced in release 10.0.x to simplify the management of LAN and SAN clients.
- [Network](#) - You can view the information of switches including status and license, as well as detailed switch dashboard information for a specific switch.
- [Storage](#) - You can view details about the storage device along with its events and topology.
- [Compute](#) - You can view the details and events for a particular Host along with its events and topology.



Note

Compute is available only with SAN installation

For more information about the Dashboard tab, refer to the [Web Client Online Help](#).

Viewing Topology Information

Topology is a first class menu item in this release with the intention that it is fully functional for providing detailed access to configuration as well as monitoring functionality. The Cisco DCNM topology consolidates functionality in the existing Fabric topology as well as the current Dashboard topology into a new fully featured topology which includes the following features in a single view:

- Optional display of Vinci Balls or device icons.
- Display of Multi-link, Port-channels, VPCs.
- Display of Inter-fabric links.
- VDC and Pod Groupings.

- Device-Scope, Fabric and Datacenter drill-down.
- Automatic VPC Peer and FEX Groupings.
- Ability to select devices and take action consistent with other areas of the product.

For more information about Topology, refer to the [Web Client Online Help](#).

Viewing Inventory Information

Beginning with Cisco 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. In this tab, you can find the discovered LAN switches, SAN switches, Storage devices and Virtual Machine Manager. You can also add a new discovery LAN or SAN switch as well.

For more information about Inventory tab, refer to the [Web Client Online Help](#).

Viewing Monitor Information

You can get the performance statistics of CPU, Memory, Traffic, others, accounting and events information. You can also view performance information about SAN and LAN. You can also create customized reports based on historical performance, events, and inventory information gathered in this tab. You can create aggregate reports with summary and detailed views. You can also view previously saved reports.

For more information about Monitor tab, refer to the [Web Client Online Help](#).

Viewing Configure Information

Allow user to view and configure Zoning, Device Alias, Port Monitoring and Device Credentials.

For more information about Configure tab, refer to the [Web Client Online Help](#).

Viewing Administration Information

You can view and configure DCNM servers, DCNM users, performance setup and event setup.

For more information about Administration tab, refer to the [Web Client Online Help](#).

Using Cisco DCNM Web Client with SSL

From release 10.0.x, Cisco DCNM Web Client uses HTTPs. If you want to install SSL certificates and use Cisco DCNM Web Client over HTTPs (using TCP port 443 or another custom port), you need a certificate for each external IP address that accepts secure connections. You can purchase these certificates from a well-known Certificate Authority (CA).

To enable SSL, you must set up the keystore to use either a self-signed certificate or a certificate from a trusted third-party company such as VeriSign.

This section includes the following topics:

- [Creating a Local Certificate, page 4-6](#)
- [Creating a Certificate Request, page 4-6](#)

Creating a Local Certificate

- Step 1** Set up a keystore to use a self-signed certificate (local certificate). From the command line, enter the following command on windows:
- ```
%JAVA_HOME%\bin/keytool -genkey -alias tomcat -keyalg RSA -keystore "C:\Program Files\Cisco Systems\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks"
```
- Step 2** Enter your name, organization, state, and country. Enter **change it** when prompted for a keystore password. If you prefer to use your own password, do not forget to change the keystorepass attribute in the server.xml file. When prompted for a key password, press **Enter** or use the same password as the keystore password.



**Note** You can now follow the steps in the next section for modifying DCNM Web Client to use SSL.

To obtain a certificate from the Certificate Authority of your choice, you must create a Certificate Signing Request (CSR). The CSR is used by the certificate authority to create a certificate that identifies your website as secure.

## Creating a Certificate Request

- Step 1** Create a local certificate (as described in the previous section).



**Note** You must enter the domain of your website in the fields First and Last name in order to create a working certificate.

- Step 2** Create the CSR with this command on windows:

```
keytool -certreq -keyalg RSA -alias tomcat -file certreq.csr -keystore "C:\Program Files\Cisco Systems\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks"
```

Now you have a file called certreq.csr. The file is encoded in PEM format. You can submit it to the certificate authority. You can find instructions for submitting the file on the Certificate Authority website.

- Step 3** After you have your certificate, you can import it into your local keystore. You must first import a Chain Certificate or Root Certificate into your keystore. You can then import your certificate.

- Step 4** Download a Chain Certificate from the Certificate Authority where you obtained the certificate:

- For Verisign.com commercial certificates, go to this URL:  
<http://www.verisign.com/support/install/intermediate.html>
- For Verisign.com trial certificates, go to this URL:  
[http://www.verisign.com/support/verisign-intermediate-ca/Trial\\_Secure\\_Server\\_Root/index.html](http://www.verisign.com/support/verisign-intermediate-ca/Trial_Secure_Server_Root/index.html)

- For Trustcenter.de, go to this URL:  
<http://www.trustcenter.de/certservices/cacerts/en/en.htm#server>
- For Thawte.com, go to this URL:  
<http://www.thawte.com/certs/trustmap.html>
- Import the Chain Certificate into your keystore by entering the **keytool -import -alias root -keystore " C:\Program Files\Cisco Systems\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -trustcacerts -file filename\_of\_the\_chain\_certificate** command.
- Import the new certificate in X509 format by entering the **keytool -import -alias tomcat -keystore " C:\Program Files\Cisco Systems\dcm\jboss-as-7.2.0.Final\standalone\configuration\fmserver.jks" -trustcacerts -file your\_certificate\_filename** command.

## Enhancements in Cisco DCNM Release 10.1(x)

Beginning from Release 10.1(x), the following are the enhancements in the Cisco DCNM.

### Web-Based Interface and VLAN management

#### Interface Templates

The intent of interface templates is to quickly and reproducibly configure interfaces. Template Instance Associations are maintained in a way consistent with POAP which means that templates are read-only.

Template input is maintained and reloaded on edit. Template input is transitioned during a template change for a given interface. Only a single template may be associated with a single interface. Template output is stored on the filesystem in a way consistent with POAP in order to allow inclusion in a combined POAP definition.

Physical Interface will support the following in this release:

- Ethernet

Logical Interfaces also have template associations, and have the ability to be created and destroyed as well. The following Logical Interface types would be needed:

- VLAN

From **Inventory > Switches** of the web client, you can select a switch and then click on the **Physical Interfaces** tab to configure one or multiple interfaces. You can also shutdown or no shut selected interface(s).

#### Port-Channel Templates

Port-channels (including VPC port channels) require more as there are interface associations must be maintained for parent, as well as member ports. Both associations should be kept and updated so that a user viewing a member port can see the full template definition associated with the parent port-channel.

## LAN Credential Management

For Cisco DCNM-SAN, there are two sets of switch/fabric credentials: discovery and config change credentials. You can provide the discovery credentials when initiating switch or fabric discovery and provide config change credentials when changing any SAN settings.

For Cisco DCNM-LAN, discovery credentials were used for switch config changes as well. In this release, config change credentials management is available for LAN also. DCNM LAN switch credentials management in the web client can be found at **Configure > Credentials Management > LAN Credentials**. You can specify the default credentials or individual switch credentials. Individual device credentials will take precedence over default credentials.

This new feature can facilitate user to enter default credentials and individual device credentials. Instead of entering device credentials one by one for all the switches that you have access to, now you can enter default credentials. Default credentials will apply for all use access switches. You can always override the default credentials, by entering the individual device credentials separately.

For detailed information about this feature, please refer to [Web Client Online Help](#).

## Support for DCNM Connect (DCNM Storage Controller)

DCNM storage controller provides capability for Storage Volume Management, storage volume and host association management in DCNM Web Client. Storage orchestration is enabled by this feature. It allows intelligent auto configuration of SAN fabric connectivity between Hosts and FC storage.

The feature needs to provide a specific set of functionality for usability. They will be limited to the user workflows for:

- Creating - Modifying - Deleting a LUN/Volume
- Creating and Removing Host LUN mapping(s)
- Create Zoning for HLMs

For detailed information about the workflow, please refer to [Web Client Online Help](#).

DCNM Connect allows user to navigate to a specific storage pool/aggregate page and create new volume.

DCNM Connect allows user to associate volumes to hosts. Back-end logic shall provide complete zone and LUN mask configuration if hosts are configured with multiple FC path.

## Operation Administration and Maintenance (OAM) for VxLAN

Virtual Extensible LAN (VxLAN) is an encapsulation protocol for running an overlay network on existing Layer 3 infrastructure. The primary goal of VxLAN is to extend the virtual LAN (VLAN) address space by adding a 24-bit segment ID and thus increasing the number of available segments to 16 million. The extended segment space is needed to enable large multi-tenant environments, where the 4094 LAN segments via IEEE 802.1q VLANs do not provide sufficient number of segments. VxLAN uses IP/UDP encapsulation, and hence can run over existing IP network infrastructure and allows for extending a LAN segment across layer 3 network. Usage of IP also enables L3 ECMP to be used in the network for better link utilization and resiliency.

As VxLAN network provides overlay solution, it requires Operation Administration and Maintenance (OAM) Tools for Fault Detection, verification, Performance, and Diagnostics to troubleshoot and easily manage the network.



In this release, Cisco DCNM integrates with OAM for VxLAN. From the **Topology** of the DCNM Web Client, you can select the **VxLAN OAM** option, and track the Reachability, Actual Path and other details. In this release, we will support Ping, TraceRoute and PathTrace. You can provide the Source host IP, Destination host IP and select the VRF, DCNM will highlight the route.

For more information about this new feature, please refer to [Web Client Online Help](#).

## FCIP Wizard Migration

To enhance the FCIP support in DCNM, the FCIP wizard is migrated to the Web client. You can find the FCIP wizard from **Configuration > SAN > FCIP**. It will take you go through the steps of setting up the FCIP link similar to the SAN client wizard.

For more information about this new feature, please refer to [Web Client Online Help](#).

## FICON RNID support in web client & SAN client

Navigate to **Inventory > View > Switches** of the Cisco DCNM Web Client, and click on a selected switch link, it will direct you to the switch dashboard. Additional FICON RNID for the connected interface is now available in **Interfaces** tab **Connected to** column if FICON applied. The FICON RNID information is retrieved via SNMP from the switch.

In the SAN client, FICON RNID information iss available in the fabric map link tooltip.

## SMART Zoning

This new function enhances the Web Zoning client to show which zones are Smart Zone enabled, and allow user to enable and disable smart zoning per zone. It also allows user to specify the device type when adding a new member to a smart zone.

This enhancement can be find from **Configure > SAN > Zoning** of the Cisco DCNM Web Client. For more information about this new feature, please refer to [Web Client Online Help](#).

## Support for Cisco MDS 9000 24/10-Port SAN Extension Module

Cisco MDS NX-OS Release 7.3(1)DY(1) 24/10-Port SAN Extension Module line card is now supported by Cisco DCNM from this release, which is a 24x2/4/8/10/16G FC and 8x1G/10G or 2x40GE IPS module for the MDS 9700 Series Directors that allows customers to extend their existing FC SANs using IPS ports, including DCNM SAN, DCNM Web Client and the Device Manager.

The Cisco MDS 9000 24/10-Port SAN Extension Module support on DCNM includes the following:

- Discover and manage the line card on Cisco MDS 9700 platforms from Cisco DCNM Web Client.
- Discover and manage the line card from DCNM SAN client and DM.
- Change IPStorage speed by group as port 1-4 or 5-8 from Device Manager.

For more information about this new feature, please refer to [Web Client Online Help](#) and [DCNM SAN Client Online Help](#).

## Slow Drain Enhancement

You are able to schedule daily job for slow drain feature in this release. You can either select **Daily** or **Once** for the **Duration** option under **Monitor > SAN > Slow Drain Analysis**. There will be only one daily job for each fabric. You can choose any intervals (less than 24 hours) for daily job, once the daily job finished, it will generate a report which can be viewed from **Monitor > Report > View**.

For more information about this new feature, please refer to [Web Client Online Help](#).

## FCIP Compression Ratio

In this release, Cisco DCNM shows the RX/TX Compression Ratio for FCIP ports. The FCIP Compression Ratio can be find from **Monitor > SAN ISLs** page. A new column **FCIP Compression Ratio** is added, and it will be empty for non-FCIP ports. With visibility of compression rate, you will have a better understanding of critical FCIP performance statistics.

## Config Archive Enhancements

In this release, Cisco DCNM has made the following enhancements for the **Configure Archive** feature:

- Option to run Archive job once  
Added a new checkbox to enable user to schedule a job once. You can schedule job for **once** and **now**.
- Restore on custom VDC  
Previously custom VDC was not supporting restore functionality. In this release restore is supported for custom VDC.
- Federation Support  
When servers are in federation, only the server which manages the switch could schedule job, copy, view, edit and restore the configuration of the device. In this release the dependency has been removed and tasks are delegated between the federated servers.
- Parallel Execution  
Enabled parallel execution of restore on different devices as well as run the archive job in parallel for multiple devices in one job.
- UI enhancements  
Radio buttons on the **Switch Configuration** main page have been changed to checkboxes to enable multiple selections. Unwanted checkbox from parent row is removed. If you do multiple selections, only **Delete** button will be enabled and Cisco DCNM doesn't allow user to delete **Running**, **Startup** or **Golden** configuration. If you select two configuration, the **Compare** button will also be enabled. For COPY and RESTORE number of steps needed to select the devices has been reduced by one. Selected devices window will be having checkboxes to enable multiple device selection.

Restore drop-down menu has been separated into two push buttons (Restore and Golden backup).

For more information about this enhancement, please refer to [Web Client Online Help](#).

## ISSU/GIR/SMU Enhancements

In this release, Cisco DCNM has made the following enhancements for **ISSU/GIR/SMU**:

- **Bootflash visibility improvements**  
In order to improve the usability, Cisco DCNM has made the enhancement to check the space availability on the bootflash and prompt the user if the disk space is not available when you select image for installation from the server. You are able to delete the files from the bootflash of the device directly from DCNM in order to make space for the installation. You are also able to see the disk space utilization on bootflash.
- **Support for TFTP and FTP enabled file transfers**  
In the prior releases, Cisco DCNM supported SFTP for transferring images from server to devices. Cisco DCNM now provides option to use FTP, TFTP, SFTP and SCP for file transfer.
- **SMU information across devices and scale improvements**  
You are now able to see the information related to the SMU packages installed across the devices in the data center from the SMU Image Management screen of the web client. This will give the complete information related to the packages and help you in deciding on selection of switches and SMU packages for the installation.
- **GIR history and scale improvements**  
You are now able to see the historical tasks for image upgrade and Software maintenance upgrades. The historical tasks for GIR are visible as well.
- **ISSU history for devices**  
You are able to see the history of the ISSU tasks performed at device level. This will help to keep track of the images installed on the devices.
- **Summarized status update at task level**  
In the prior releases, detailed status update is provided only if you select a particular task. This might not be user friendly when there is large number of devices in image upgrade job. Now Cisco DCNM shows the latest status of installation at task level so that you can view all of them in a single screen.
- **Sequencing devices for Image upgrade**  
During image upgrade, you have the option to perform upgrade either sequential or parallel. In case of sequential upgrade, Cisco DCNM are providing the option to sequence the device upgrade from DCNM.
- **Support for Isolate and shutdown modes for GIR on N3K and N9K**  
On most of nexus devices there is only one type of GIR maintenance mode. But in case of N3K and N9K you now have the option to have GIR in either shutdown or isolate mode. In all other platforms only shutdown mode is supported.
- **Pre GIR during Image upgrade**  
Cisco DCNM are now providing the option to move the device to maintenance mode before doing image upgrade from the image upgrade wizard.

For more information about this enhancement, please refer to [Web Client Online Help](#).

## Template Enhancement

In this release, Cisco DCNM has made the following enhancements for Template:

- Bulk Import Support in Configure Template Page

In order to import large number of templates at a time, now you are able to import a zip file which contains many templates from **Configure > Templates > Deploy** of the Cisco DCNM Web Client.

- Enable/Disable fields based on some condition in Config Job creation wizard

You can show or hide particular fields based on some conditions in Configure job creation wizard. You can provide an annotation with the condition in which the field needs to be enabled. In the condition statement users can use following operators: ==, !=, ||, &&.

- Configure Template Tree Structure view based on Meta Data

Cisco DCNM provides tree structure view in Configure Template page.

For more information about this enhancement, please refer to [Web Client Online Help](#).

## vPC Enhancement

In this release, Cisco DCNM has made the following enhancements for vPC:

- Physical Port vPC support

Physical port vPC is now supported in Monitor **vPC Consistency** screen, **vPC Performance** screen from **Monitor > LAN > VPC** and vPC Topology

- vPC+

Cisco Nexus switches support creation of vPC along with fabric patch, its called as vPC+. In case of vPC+ peer-link port-channel will be in fabric patch mode, peer switches will have fabric path switch ID.

Discovery of vPC+ is now supported in Cisco DCNM, and the information is displayed in Topology view and vPC details page. And vPC workflow also supports the creation of vPC+.

- Splitting vPC workflow

vPC workflow helps user to create vPC with Nexus switches (LAN) through a guided workflow. In this release, Cisco DCNM has splitted the workflow into two-step process:

- vPC Peer Creation
- vPC Creation

vPC workflow supports the following additional features:

- Add, Edit, Delete vPC Domain
- Add, Edit vPC's
- vPC+ creation



### Note

For vPC+ creation, wizard will list all Interfaces, irrespective of whether it supports fabric path or not. If you select the interface which does not supports vPC+ configuration, it will fail on the device, and configuration will be rolled back (if device supports rollback).

For more information about this enhancement, please refer to [Web Client Online Help](#).

## Search Enhancement

Enhanced the search feature to allow search for VM tracker and generic setup. You are also able to see which leaf the host is connected to.

For more information about this enhancement, please refer to [Web Client Online Help](#).

## EoL Report for MDS Product Family

Cisco DCNM now provides End of Life report for MDS product family.

To generate up-to-date EoL report, you need to download the updated **cisco\_eol.xls** from Cisco Connection Online (CCO). Follow the below steps to generate the EoL report:

- 
- |               |                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Go to <a href="http://www.cisco.com/go/dcnm">http://www.cisco.com/go/dcnm</a> and download latest <b>cisco_eol.xls</b> file. |
| <b>Step 2</b> | Copy the downloaded <b>cisco_eol.xls</b> file to DCNM server under the directory <b>/usr/local/cisco/dcm/fm/conf/</b> .      |
| <b>Step 3</b> | Run the EoL report from <b>Monitor &gt; Report &gt; Generate</b> .                                                           |
- 

## Media Controller for IP Fabric

Beginning with Cisco DCNM Release 10.1(2), through open APIs, the Cisco DCNM Media Controller seamlessly integrates with the broadcast controller and provides a similar operator workflow with all the benefits of an IP-based infrastructure. The DCNM Media Controller features an intuitive GUI that enables you to configure your IP fabric using pre-defined templates designed for media networks.

The key features are:

- **Topology Visualization**—Cisco DCNM 10.1(2) consists of a new scalable Topology visualization UI which shows the PMN Fabric, end points attached to the fabric along with search based querying based-on Flow ID and related health statistics.
- **Endpoint (Sender and Receiver management)**—Senders and receivers can connect to the Leaf switches of the PMN Fabric. The Sender initiates a multicast flow and the Receiver subscribes to a multicast flow. Cisco DCNM exposes the API for registration of the Sender and Receiver. DCNM also allows the Sender/Receiver to be validated/authenticated by the API user. A table lists all the current registered senders and receivers with information about the flow instances. DCNM UI and REST APIs allow users to add additional metadata to the receiver/sender information, such as Camera-BXB or Camera-SJ, to aid in easy mapping.
- **Bandwidth management for Multicast Flows**—DCNM performs bandwidth management of flows and the error recovery operations.
- **Error recovery and flow reconfigurations**—On link failure, DCNM will receive notifications from the switch and will then perform a best effort to re-route the impacted flows.
- **Flow visualization and monitoring**—You can monitor the End Hosts and perform flow search on topology. On the Topology visualization, you can view, search, and sort flows based on following criteria.
  - Flow id—Unique identifies for each flow.
  - Sender status—All Flows originating from the selected sender.

- Receiver status—All Flows that the receiver is subscribed to.
- All subscribers of a given Flow.
- Any error conditions in the Fabric.
- Packet drop conditions—These should be provided by the switch.
- Flow counters—These should be provided by the switch.
- SNMP based port status monitoring will be shown with historical information.
- Port state changes should be reported by switch and will be displayed on Topology as well.
- High Availability for all Controller operations—There are separate DCNM HA pair setups for Active Network and Standby Networks. Each DCNM HA pair independently performs bandwidth management and controller functions for each Network. The two media networks are independent from the controller perspective.

To enable Media Controller on the Cisco DCNM Web Client, you must install the DCNM in media-controller mode. See *Cisco DCNM Installation Guide, Release 10.1(x)* for more information.

You can monitor the devices from the Cisco DCNM **Web Client > Media Controller**.