Media Controller

This section describes the Cisco DCNM Web Client UI **Media Controller** tab.

Note

- From Cisco DCNM Release 11.1(1), only a user with the network-admin role can configure a host or flow policy, and global configuration settings.
- IPFM maintains the last known monitored state of switches before they stop communicating. If switch doesn't report in 2 minutes, it will be marked as **Out Of Sync**. Check the sync status and the last sync timestamp by clicking **Telemetry Switch Sync Status** link on the respective monitoring page, for example, **Media Controller / Flow / Flow Status**.

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 the POAP Launchpad section.

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 that is 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.

You can use the DCNM media controller deployment for only monitoring purposes and not as a policy manager. For more information, see DCNM Read-Only Mode for Media Controller, on page 42.

NX-OS Streaming Telemetry and DCNM

Using streaming telemetry, NBM process on the switch informs DCNM its state using which DCNM is able to show discovered hosts and flows across the IP fabric. The POAP and `pmn_telemetry_snmp` CLI template, which are packaged in DCNM, generate the necessary telemetry configuration on the switch. An example of the generated configuration is as shown in the following sample:

```
telemetry
  destination-profile
    use-vrf management
  destination-group 200
    ip address <dcnm-ip> port 50051 protocol gRPC encoding GPB
  destination-group 1500
  sensor-group 200
    data-source DME
    path sys/nbm/show/appliedpolicies depth unbounded
    path sys/nbm/show/stats depth unbounded
  sensor-group 201
    data-source DME
    path sys/nbm/show/flows depth 0 query-condition
    rsp-subtree-filter=eq(nbmNbmFlow.bucket,"1")&rsp-subtree=full
  sensor-group 202
    data-source DME
    path sys/nbm/show/flows depth 0 query-condition
    rsp-subtree-filter=eq(nbmNbmFlow.bucket,"2")&rsp-subtree=full
  sensor-group 203
    data-source DME
    path sys/nbm/show/flows depth 0 query-condition
    rsp-subtree-filter=eq(nbmNbmFlow.bucket,"3")&rsp-subtree=full
  sensor-group 204
    data-source DME
    path sys/nbm/show/flows depth 0 query-condition
    rsp-subtree-filter=eq(nbmNbmFlow.bucket,"4")&rsp-subtree=full
  sensor-group 205
    data-source DME
    path sys/nbm/show/endpoints depth unbounded
  sensor-group 300
    data-source NX-API
    path "show ptp brief"
    path "show ptp parent"
  sensor-group 301
    data-source NX-API
    path "show ptp corrections"
  sensor-group 500
    data-source NX-API
    path "show flow rtp details" depth 0
    path "show flow rtp errors active" depth 0
    path "show flow rtp errors history" depth 0
  subscription 201
    dst-grp 200
    snsr-grp 200 sample-interval 60000
    snsr-grp 201 sample-interval 30000
    snsr-grp 205 sample-interval 30000
  subscription 202
    dst-grp 200
    snsr-grp 202 sample-interval 30000
  subscription 203
    dst-grp 200
    snsr-grp 203 sample-interval 30000
  subscription 204
    dst-grp 200
    snsr-grp 204 sample-interval 30000
  subscription 300
    dst-grp 200
    snsr-grp 300 sample-interval 30000
    snsr-grp 301 sample-interval 30000
  subscription 500
    dst-grp 200
    snsr-grp 500 sample-interval 30000
```


- Topology, on page 3

Topology

You can view the Media Controller topology on the **Web UI > Media Controller > Topology** page. This topology is specific to the operations performed by DCNM as a Media Controller.

Note

- If you remove a device from the Inventory, the Policy deployment status for that switch is removed. However, you must clear the policy configuration on the switch also.
- After moving a cable from one port to another port, the old link is retained in the **Topology** window, and it is shown in the red color indicating that the link is down. The port movements are not updated in the **Topology** window. You need to rediscover the switch for the updated ports to be displayed in DCNM.

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 are 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.

Host

The Host menu includes the following submenus:

Discovered Host

You can view all the hosts that are populated through telemetry on this screen. After the switches are discovered, all the switches in the fabric will push data to the DCNM server at regular intervals using telemetry. Cisco DCNM server displays the received Events and Flow statistics for each active flow.

The following table describes the fields that appear on this page. Click the table header to sort the entries in alphabetical order of that parameter.

Table 1: Discovered Host Table Fields and Description

Field	Description
Host Name	Specifies the configured Host Alias for the host IP address. The Host IP is displayed if the Host Alias is not configured.
Role	Specifies the role of the host device. The role of the host can be one of the following: • Sender • External Sender • Dynamic Receiver • External Receiver • Static Receiver
Multicast Group	Specifies the multicast address of the flow in which the host participates.
Source	Specifies the source of the flow which the discovered host participates in.
Switch	Specifies the name of the switch.
Interface	Specifies the interface to which the host is connected to on the sender or receiver switch.
MAC Address	Specifies the MAC address of a physical host, if the switch has ARP entry for that host).
Host Discovered Time	Specifies the date and time at which the switch discovered the host.
Fault Reason	Specifies the failure reason for the flow that the discovered host has participates in.

Host Alias

Cisco DCNM allows you to create host aliases for Media Controller sender and receiver hosts. The active multicast traffic transmitting and receiving devices are termed as hosts. Beginning with Cisco DCNM Release 11.0(1), you can add a host-alias name to your sender and receiver hosts, to help you to identify the hosts by a name. You can also import a large number of Host Alias to Cisco DCNM Media Controller.

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

Table 2: Host Alias Table Field and Description

Field	Description
Host Alias	Specifies the host name that is configured to identify the host.
IP Address	Specifies the IP address of the host connecting to the switch, which you want to refer with an alias name.
Last Updated At	Specifies the date and time at which the host alias was last updated.

This section contains the following:

Add Host Alias

Perform the following task to add new host aliases to devices in the fabric discovered by Cisco DCNM.

Procedure

Step 1 Choose **Media Controller > Host > Host Alias**, click **Add**.

Step 2 In the Add/Edit Host Alias window, enter the following:

- **Host Name**—Enter a fully qualified unified hostname for the identification.
- **IP Address**—Enter the IP address of the host that is the part of a flow.

Note You can also create host alias before a host sends any data to its directly connected sender or receiver leaf .

Step 3 Click **Save** to apply the changes.

Click **Cancel** to discard the host alias.

The new host alias is shown in the table on the **Host Alias** window.

Edit Host Alias

Perform the following task to edit the host alias.

Procedure

Step 1 Choose **Media Controller > Host > Host Alias**, select the check box next to the Host Alias that you need to modify.

Step 2 In the **Add/Edit Host Alias** window, enter the following:

- **Host Name**—Enter a fully qualified unified hostname for the identification.
- **IP Address**—Enter the IP address of the host that is the part of a flow.

Step 3 Click **Save** to apply the changes.

Click **Cancel** to discard the host alias.

The modified host alias is shown in the table on the **Host Alias** window.

Delete Host Alias

Perform the following task to delete the host alias.

Procedure

Step 1 Choose **Media Controller > Host > Host Alias**, select the check box next to the Host Alias that you want to delete.

You can select multiple Host Alias entries to be deleted at the same instance.

Step 2 Click **Delete**.

Step 3 On the confirmation window, click **OK** to delete the Host Alias.

Click **Cancel** to retain the host alias.

Import Host Alias

Perform the following task to import host aliases for devices in the fabric.

Procedure

Step 1 Choose **Media Controller > Host > Host Alias**, click **Import** icon.

Step 2 Browse the directory and select the CSV file, which contains the Host IP address and corresponding unique hostname information.

Step 3 Click **Open**.

The host aliases are imported and displayed on the Host Alias table.

Export Host Alias

Perform the following task to export host aliases for devices in the fabric.

Procedure

Step 1 Choose **Media Controller > Host > Host Alias**, click **Export** icon.

A notification window appears.

Step 2 Select a location on your local system directory to store the Host Aliases configuration from DCNM and click **OK**.

The host alias configuration file is exported to your local directory. The filename is appended with the date and time at which the file was exported. The format of the exported file is `.csv`.

Host Policies

You can add policies to the host devices. Navigate to **Media Controller > Host > Host Policies** to configure the host policies.

Note Switches must be deployed with default host policies. You can edit the default host policies to permit or deny. From the Deployment drop-down list, select **Deploy Selected Policies** to deploy the default policies to the switches.You can also deploy all the default policies to all the managed switches by selecting **Deploy All Default Policies** even without selecting any default policies.

By default, the sequence numbers for policies are auto-generated by DCNM and Multicast mask/prefix is taken as /32. The server property **pmn.hostpolicy.multicast-ranges.enabled** under **Administration > DCNM Server > Server Properties** must be set to '**true**' for the user to be able to provide sequence numbers and multicast mask/prefix. When the server property is set to **True**, the fields to enter the sequence number and the multicast mask/prefix is available in the **Media Controller > Host > Host Policies > Add** and **Media Controller > Host > Host Policies > Edit** pages.

The default host policies must be deployed successfully to the switch before you deploy the custom host policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add, edit, import, or deploy custom policies.

Note When a user logs in to DCNM with a network operator role, all the buttons or options to add, delete, modify, import, export, or deploy policies are disabled. This user can only view policies, and deployment status or history.

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

Table 3: 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.

Field	Description
Delete	Allows you to delete the user-defined host policy. **Note** • Undeploy policies from all switches before deleting them from DCNM. • You can undeploy the default policy, but you cannot delete the default policy. You can delete and undeploy only the custom policies. • When you undeploy the default policies, All Default Policies will be reset to have default permission (Allow).
Delete All	Allows you to delete all custom policies without selecting any policy check box. **Note** • Undeploy policies from all switches before deleting them from DCNM. • You can undeploy the default policy, but you cannot delete the default policy. You can delete and undeploy only the custom policies.
Import	Allows you to import host policies from a CSV file to DCNM. **Note** After import, all policies imported from a CSV file are applied to all managed switches automatically.
Export	Allows you to export host policies from DCNM to a CSV file.

Field	Description
Deployment	

Field	Description

	From the Deployment drop-down list, select an appropriate value.
	• Deploy
	  • Selected Policies—Select this option to deploy selected policies to the switch.
	  • All Default Policies—Select this option to deploy all default policies to the switch.
	  • All Custom Policies—Select this option to deploy all the user-defined policies.
	• Undeploy
	  • Selected Policies—Select this option to undeploy the selected policies.
	  • All Default Policies—Select this option to undeploy the default policies.
	  • All Custom Policies—Select this option to undeploy all the user-defined policies.
	• Redo All Failed Policies—Select this option to deploy all failed policies.
	  All the deployments that failed on switches previously will be deployed again to only those switches. All the undeployments that failed on switches previously will be undeployed again from only those switches.
	• Deployment History—Select one policy from the drop-down list. Select this option to view the deployment history of the selected policy.
	  Deployment History shows the following fields.
	  • Policy Name—Displays the selected policy name.
	  • Switch Name—Specifies the name of the switch that the policy was deployed to.
	  • Deployment Status—Displays the status of deployment. It shows if the deployment was Success or Failed.
	  • Action—Specifies the action that is performed on the switch for that host policy. **Create** implies that the policy has been deployed on the switch. **Delete** implies that the policy has been undeployed from the switch.
	  • Deployment Date/Time—Specifies the date and time at which the host policy was last updated. The format is *Day MMM DD YYYY HH:MM:SS Timezone*.
	  • Failed Reason—Species why the policy was not

Field	Description
	successfully deployed.

Table 4: Host Policies Table Field and Description

Field	Description
Policy Name	Specifies the policy name for the host, as defined by the user.
Host Name	Specifies the host ID.
Receiver IP	Specifies the IP address of the receiving device.
Sender IP	Specifies the IP Address of the transmitting device.
Multicast IP	Specifies the multicast IP address for the host.
Sender IP	Specifies the IP Address of the sender.
Host Role	Specifies the host device role. The host device role is either one of the following: • Sender • Receiver-External • Receiver-Local
Operation	Specifies if the operation of the host policy. The policy has the following operations: • Permit • Deny
Sequence #	Specifies the sequence number of the custom policy when the multicast range is selected.
Deployment Action	Specifies the action performed on the switch for that host policy. • **Create**—The policy is deployed on the switch. • **Delete**—The policy is undeployed from the switch.
Deployment Status	Specifies if the deployment is successful, failed or the policy is not deployed.
Last Updated	Specifies the date and time at which the host policy was last updated. The format is `Day MMM DD YYYY HH:MM:SS Timezone`.

This section contains the following:

Add Host Policy

By default, the sequence number for policies is auto-generated by DCNM, and Multicast mask/prefix is /32 by default. The server property **pmn.hostpolicy.multicast-ranges.enabled** under **Administration > DCNM Server > Server Properties** must be set to '**true**' for the user to be able to provide sequence numbers and multicast mask/prefix. When the server property is set to **true**, the fields to enter the sequence number and the multicast mask/prefix are available in the **Media Controller > Host > Host Policies > Add** and **Media Controller > Host > Host Policies > Edit** windows.

The default host policies must be deployed successfully to the switch before you deploy the custom host policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add custom policies.

To add Host policy from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Host > Host Policies**.

The **Host Policies** window is displayed.

Step 2 Click the **Add** 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 host policy.
- **Host Role**: Specifies the host as a multicast sender or receiver. Select one of the following:
  - Sender
  - Receiver-Local
  - Receiver-External
- **Host Name**: Specifies the host to which the policy is applied. If a destination host is detected, you can choose the hostname from the drop-down list.

  Note Do not select hosts that are discovered as remote receivers to create receiver or sender host policies. However, hosts that are discovered as remote senders can be used for creating sender host policies.
- **Sender IP**: Specifies the IP address of the Sender host. Note that you can specify wildcard for this IP address by specifying the * (asterisk) symbol or 0.0.0.0 in this field.
- **Receiver IP**: Specifies the IP address of the receiver host. This field is visible and is applicable only if the Host Role is set to **Receiver-Local**. Note that you can specify wildcard for this IP address by specifying the * (asterisk) symbol or 0.0.0.0 in this field.

  Note When **Receiver IP** in a receiver host policy is a wildcard (* or 0.0.0.0), **Sender IP** also has to be a wildcard (* or 0.0.0.0).
- **Multicast**: Specifies the multicast IP Address for the host policy. Note that you can specify wildcard for this IP address by specifying the * (asterisk) symbol in this field. This will translate to 224.0.0.0/4. If you specify a wildcard IP address for **Sender IP** and **Receiver IP** fields, the Multicast Group is always required, that is, you cannot specify multicast as * or 0.0.0.0.

- **Allow/Deny**: Click the radio button to choose, if the policy must **Allow** or **Deny** the traffic flow.

Step 4 Click **Save & Deploy** to configure and deploy the Policy.

Click **Cancel** to discard the new policy.

Edit Host Policy

The default host policies must be deployed successfully to the switch before you deploy the custom host policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you edit custom policies.

To edit host policy from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Host > Host Policies**.

The **Host Policies** window is displayed.

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 are applied immediately. If the policy is already applied to any device, the changes may impact the existing flows.

Step 5 Click **Save & Deploy** to configure and deploy the Policy.

Click **Cancel** to discard the changes.

Delete Host Policy

To delete host policy from the Cisco DCNM Web UI, perform the following steps:

Note You can delete only user-defined Host Policies.

Procedure

Step 1 Choose **Media Controller > Host > Host Policies**.

The **Host Policies** window is displayed.

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.

Click **Delete All** to delete all the policies at a single instance.

Step 4 In the delete notification, click **OK** to delete the host policy. Click **Cancel** to return to the Host Policies page.

Note Deleting a host policy from DCNM does not undeploy the policy from the switches on which it is deployed. It is highly recommended to undeploy the policy on the switches before deleting it from DCNM.

A Delete Host policy successful message appears at the bottom of the page.

Import Host Policy

The default host policies must be deployed successfully to the switch before you deploy the custom host policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add custom policies.

To import host policies from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Host > Host Policies**.

The **Host Policies** window is displayed.

Step 2 Click the **Import** host policy icon.

Step 3 Browse the directory and select the `.csv` format file which contains the Host Policy configuration information.

The policy will not be imported if the format in the `.csv` file is incorrect.

Step 4 Click **Open**.

The imported policies are automatically deployed to all the switches in the fabric.

Export Host Policy

To export host policies from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Host > Host Policies**.

The **Host Policies** window is displayed.

Step 2 Click the **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 filename is appended with the date on which the file is exported. The format of the exported file is *.csv*.

Policy Deployment

Policies are automatically deployed to switches whenever they are added, edited, or imported. You can choose to undeploy or redeploy the policies, by choosing the appropriate actions in the **Deployment** drop-down list. The policies will not be deployed correctly if the device is rebooting while the policy was deployed. In such case, the Failed message appears in the Status column in the table below.

The default policies must be deployed successfully to the switch before you deploy the custom policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add custom policies.

Deploy Selected Policies

This option allows you to deploy only selected policies to the devices. You can deploy other policies when required.

Select one or more check boxes next to the policy name. Select this option to deploy selected policies to the switch.

Deploy All Custom Policies

This option allows you to deploy all the custom or user-defined policies to the switch. The policies are deployed even if the switch is rebooting. In such case, the deployment fails and a status message Failed appears in the table below.

Select this option to deploy all the user-defined policies at a single instance.

Undeploy Selected Custom Policies

Select one or more check boxes next to the policy name. Select this option from the drop-down list to undeploy the selected policies.

Undeploy All Custom Policies

This option allows you to undeploy all the custom or user-defined policies in a single instance.

Note From Cisco DCNM Release 11.2(1), you can deploy and undeploy default policies also.

Redo All Failed Custom Policies

The deployment of policies may fail due to various reasons. This option allows you to deploy all failed user-defined policies.

All the deployments that failed previously are deployed again only to those switches. All the undeployments failed previously are redeployed from only those switches.

Deployment History

This option allows you to view the deployment history of the policy.

The policy name is shown in the Policy Name field. From the drop-down list, choose the switch on which this policy was deployed.

The deployment history of the selected policy for the switch appears in the table below.

Deployment History table shows the following fields.

Table 5: Policy Deployment History Table Field and Descriptions

Field	Description
Deployment Status	Displays the deployment status of the policy. It shows if the deployment was Success or Failed.
Deployment Action	Specifies the action that is performed on the switch for that policy. **Create**: The policy is deployed on the switch. **Delete**: The policy is undeployed from the switch.
Deployment Date/Time	Specifies the date and time at which the host policy was last updated. The format is *Day MMM DD YYYY HH:MM:SS Timezone*.
Failed Reason	Species why the policy was not successfully deployed.

Applied Host Polices

Beginning from Cisco DCNM Release 11, you can view the policies that you have applied in the entire network. On the Cisco DCNM Web UI, navigate to **Media Controller > Host > Applied Host Policies** to view the various policies.

The table displays default PIM policy, local receiver policy, and sender policy. Media Controller will not display user-defined PIM Policies or Receiver External Policies.

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

Table 6: Field and Description on the Applied Host Policies

Column Name	Description
Policy Name	Specifies the name of the policy applied.
Host Role	Specifies the role of the host. The host device role is either one of the following: • PIM • Sender • Receiver

Column Name	Description
Switch	Specifies the name of the switch to which the policy is applied.
Interface	Specifies the interface to which the policy is applied.
Active	Specifies if the policy is active or not.
Time Stamp	Specifies the date and time at which the policy was created\deployed. The format is Day, MMM DD YYYY HH:MM:SS (Timezone).

Flow

The Flow menu includes the following submenus:

Flow Status

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

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

Table 7: Active Tab

Field	Description
Show Chart	Click Show Chart icon to view the graphical representation of the Flow Status. **Note** The data refers to the sender leaf when the sender starts broadcasting. Please see the receiver start time in the flow status table to find when the receiver started getting data. Click the **Show** drop-down list to view the flow status information in one of the following formats─Chart, Table, or Chart and Table. Click **Chart Type** icon to view the various chart types. Select a chart type to view the flow status information that is depicted in that chart format. You can choose a chart option to see filled patterns or data markers. Click **Actions** icon to print the report or excel chart information to your local directory.

Field	Description
Multicast IP	Specifies the multicast IP address for the flow. **Note** 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.
Policed	Specifies whether a flow is policed or not policed.
Sender	Specifies the IP Address or the Host alias of the sender for the multicast group.
Receiver	Specifies the IP Address or the Host alias of the receiver joining the group.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.
Sender Switch	Specifies if the Sender switch is a leaf or spine.
Sender Interface	Specifies the interface to which the sender is connected to.
Receiver Switch	Specifies if the Receiver switch is a leaf or spine.
Receiver Interface	Specifies the interface to which the receiver is connected to.
QOS/DSCP	Specifies the Switch-defined QoS Policy.
Flow Link State	Specifies the state of the flow link. Click **active** link to view the network diagram of the Sender and Receiver. The dotted line displays the direction of the flow of traffic. You can hover over the nodes to view information. The table on the right side shows information about the Sender and Receiver.
Policy ID	Specifies the policy ID applied to the multicast IP.
Sender Start Time	Displays the time from when the sender joined.
Receiver Join Time	Specifies the time at which the receiver joined.

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

Table 8: Inactive Tab

Field	Description
Show Chart	Click Show Chart icon to view the graphical representation of the Flow Status. **Note** The data refers to the sender leaf when the sender starts broadcasting. Please see the receiver start time in the flow status table to find when the receiver started getting data. Click the **Show** drop-down list to view the flow status information in one of the following formats—Chart, Table, or Chart and Table. Click **Chart Type** icon to view the various chart types. Select a chart type to view the flow status information that is depicted in that chart format. You can choose a chart option to see filled patterns or data markers. Click icon to print the report or excel chart information to your local directory.
Multicast IP	Specifies the multicast IP address of the flow.
Flow Alias	Specifies the name of the Flow Alias.
Policed	Specifies whether a flow is policed or not policed.
Sender	Specifies the IP Address or the Host alias of the sender for the multicast groups.
Receiver	Specifies the IP Address or the Host alias of the receiver.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.
QoS/DSCP	Specifies the Switch-defined QoS Policy.
Policy ID	Specifies the policy ID applied to the multicast IP.
Sender Start Time	Specifies the time at which the sender joined.
Receiver Join Time	Specifies the time at which the receiver joined.

Field	Description
Fault Reason	Specifies reason for the inactive flow. Cisco DCNM determines the inactive flow if both the sender and receiver mroute exists with any of the following combinations. • Receiver IIF is null • Receiver OIF is null • Sender IIF is null • Sender OIF is null In this scenario, the switch will not have any fault reason. Therefore, there is no fault reason for such inactive flows.

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

Table 9: Sender Only Tab

Field	Description
Multicast IP	Specifies the multicast IP address for the flow.
Flow Alias	Specifies the name of the Flow Alias.
Policed	Specifies whether a flow is policed or not policed.
Sender	Specifies the name of the sender.
Sender Switch	Specifies the IP address of the sender switch.
Sender Ingress Interface	Specifies the name of the sender ingress interface.
Flow Link State	Specifies the flow link state, if it is allow or deny.
Policy ID	Specifies the policy ID applied to the multicast IP.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.
Sender Start Time	Displays the time from when the sender switch is transmitting information.

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

Table 10: Receiver 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 receiver ID. If the multicast receiver is remote, the **Remote** label can be seen next to its name.
Receiver Interface	Specifies the name of the destination switch interface.
Receiver Switch	Specifies the IP address of the receiver switch.
Source Specific Sender	Specifies the IP address of the multicast sender.
Flow Link State	Specifies the flow link state, if it is allow or deny.
Policy ID	Specifies the policy ID applied to the multicast IP.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.
Receiver Join Time	Specifies the time at which the receiver joined.

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

Click 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.

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 a flow alias on **Media Controller > Flow > Flow Alias**.

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

Table 11: 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.

Field	Description
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 from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Alias**.

The **Flow Alias** window is displayed.

Step 2 Click the **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.

Click **Cancel** to discard.

Edit Flow Alias

To edit a flow alias from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Alias**.

The **Flow Alias** window is displayed.

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.

Click **Cancel** to discard the changes.

Delete Flow Alias

To delete flow alias from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Alias**.

The **Flow Alias** window is displayed.

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 from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Alias**.

The **Flow Alias** window is displayed.

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 filename 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 from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Alias**.

The **Flow Alias** window is displayed.

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 the **Media Controller > Flow > Flow Alias** window, on the Cisco DCNM Web Client.

Flow Policies

You can configure the flow policies on **Media Controller > Flow > Flow Policies**.

The default policies are displayed on the Flow policy page. By default, the bandwidth of these policies is 0. You can configure the bandwidth such that any flow that matches the default flow policy will accordingly use the bandwidth and QOS/DSCP parameters. The policy is deployed to all the devices when you save the configuration.

The default flow policies must be deployed successfully to the switch before you deploy the custom flow policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add, edit, import, or deploy custom policies.

Note When you undeploy a default policy, it will be reset to default values, that is, Bandwidth:0gbps, DSCP:Best Effort, and Policer:Enabled.

Note When a user logs in to DCNM with a network operator role, all the buttons or options to add, delete, modify, import, export, or deploy policies are disabled. This user can only view policies, and deployment status or history.

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

Table 12: 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. **Note** • You cannot delete the default flow policies. • Undeploy policies from all switches before deleting them from DCNM.

Field	Description
Delete All	Allows you to delete all the flow policies at a single instance. **Note** Undeploy policies from all switches before deleting them from DCNM.
Import	Allows you to import flow policies from a CSV file. **Note** After import, all policies imported from a CSV file are applied to all managed switches automatically.
Export	Allows you to export flow policies to a CSV file.

Field	Description
Deployment	

Field	Description

	From the Deployment drop-down list, select an appropriate value.
	• Deploy
	  • Selected Policies—Select this option to deploy selected policies to the switch.
	  • All Default Policies—Select this option to deploy all default policies to the switch.
	  • All Custom Policies—Select this option to deploy all the user-defined policies.
	• Undeploy
	  • Selected Policies—Select this option to undeploy the selected policies.
	  • All Default Policies—Select this option to undeploy the default policies.
	  • All Custom Policies—Select this option to undeploy all the user-defined policies.
	• Redo All Failed Policies—Select this option to deploy all failed policies.
	  All the deployments that failed on switches previously will be deployed again to only those switches. All the undeployments that failed on switches previously will be undeployed again from only those switches.
	• Deployment History—Select one policy from the drop-down list. Select this option to view the deployment history of the selected policy.
	  Deployment History shows the following fields.
	  • Policy Name—Displays the selected policy name.
	  • Switch Name—Specifies the name of the switch that the policy was deployed to.
	  • Deployment Status—Displays the status of deployment. It shows if the deployment was Success or Failed.
	  • Specifies the action that is performed on the switch for that flow policy.
	  • **Create**—Implies that the policy has been deployed on the switch.

Field	Description
	• **Delete**—Implies that the policy has been undeployed from the switch. • Deployment Date/Time—Specifies the date and time at which the host policy was last updated. The format is *Day MMM DD YYYY HH:MM:SS Timezone*. • Failed Reason—Species why the policy was not successfully deployed.

Table 13: Flow Policies Table Field and Description

Field	Description
Policy Name	Specifies the flow policy name.
Multicast IP Range	Specifies the multicast IP address for the traffic.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.
QoS/DSCP	Specifies the Switch-defined QoS Policy.
Deployment Status	Specified if the flow policy is deployed successfully or failed.
Deployment Action	Specifies the action that is performed on the switch for that host policy. • **Create**—The policy is deployed on the switch. • **Delete**—The policy is undeployed from the switch.
In Use	Specifies if the flow policy is in use or not.
Policer	Specifies whether the policer for a flow policy is enabled or disabled. **Note** In adding or editing a flow policy, the default policer state is **Enabled**.
Last Updated	Specifies the date and time at which the flow policy was last updated. The format is `Day MMM DD YYYY HH:MM:SS Timezone`.

Note A new flow policy or an edited flow policy is 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

The default host policies must be deployed successfully to the switch before you deploy the custom host policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add custom policies.

To add flow policy from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller** > **Flow** > **Flow Policies**.

The **Flow Policies** window is displayed.

Step 2 Click the **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.
- **Bandwidth**: Specifies the bandwidth that is 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 the **Policer** toggle switch to enable or disable policer for a flow. By default, the poilcer for a new flow policy is enabled.

Step 6 In the Multicast IP Range, enter the beginning IP and ending IP Address for the multicast range.

Click **Plus (+)** icon to add the multicast range to the policy.

Step 7 Click **Deploy** to deploy the new policy.

Click **Cancel** to discard the changes.

Edit Flow Policy

The default flow policies must be deployed successfully to the switch before you deploy the custom flow policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you edit custom policies.

To add flow policy from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Policies**.

The **Flow Policies** window is displayed.

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 the **Policer** toggle switch to enable or disable policer for a flow policy.

Step 6 Click **Deploy** to deploy the new policy.

Click **Cancel** to discard the changes.

Delete Flow Policy

To delete flow policy from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Policies**.

The **Flow Policies** window is displayed.

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.

Note You cannot delete the default policies.

Step 3 Click **Delete** icon to delete the selected flow policy.

Click **Delete All** icon to delete all the flow policies at a single instance.

Import Flow Policy

The default flow policies must be deployed successfully to the switch before you deploy the custom flow policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you import custom policies.

To import flow policies from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Policies**.

The **Flow Policies** window is displayed.

Step 2 Click the **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 the **Media Controller > Flow > Flow Policies** window, on the Cisco DCNM Web Client.

The imported policies are automatically deployed to all the switches in the fabric.

Export Flow Policy

To export host policies from the Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Media Controller > Flow > Flow Policies**.

The **Flow Policies** window is displayed.

Step 2 Click the **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 filename is appended with the date on which the file is exported. The format of the exported file is `.csv`.

Policy Deployment

Policies are automatically deployed to switches whenever they are added, edited, or imported. You can choose to undeploy or redeploy the policies, by choosing the appropriate actions in the **Deployment** drop-down list. The policies will not be deployed correctly if the device is rebooting while the policy was deployed. In such case, the Failed message appears in the Status column in the table below.

The default policies must be deployed successfully to the switch before you deploy the custom policies on that switch. Otherwise, the custom policies will fail to deploy. Ensure that you deploy all default policies successfully to all the switches before you add custom policies.

Deploy Selected Policies

This option allows you to deploy only selected policies to the devices. You can deploy other policies when required.

Select one or more check boxes next to the policy name. Select this option to deploy selected policies to the switch.

Deploy All Custom Policies

This option allows you to deploy all the custom or user-defined policies to the switch. The policies are deployed even if the switch is rebooting. In such case, the deployment fails and a status message Failed appears in the table below.

Select this option to deploy all the user-defined policies at a single instance.

Undeploy Selected Custom Policies

Select one or more check boxes next to the policy name. Select this option from the drop-down list to undeploy the selected policies.

Undeploy All Custom Policies

This option allows you to undeploy all the custom or user-defined policies in a single instance.

Note From Cisco DCNM Release 11.2(1), you can deploy and undeploy default policies also.

Redo All Failed Custom Policies

The deployment of policies may fail due to various reasons. This option allows you to deploy all failed user-defined policies.

All the deployments that failed previously are deployed again only to those switches. All the undeployments failed previously are redeployed from only those switches.

Deployment History

This option allows you to view the deployment history of the policy.

The policy name is shown in the Policy Name field. From the drop-down list, choose the switch on which this policy was deployed.

The deployment history of the selected policy for the switch appears in the table below.

Deployment History table shows the following fields.

Table 14: Policy Deployment History Table Field and Descriptions

Field	Description
Deployment Status	Displays the deployment status of the policy. It shows if the deployment was Success or Failed.
Deployment Action	Specifies the action that is performed on the switch for that policy. **Create**: The policy is deployed on the switch. **Delete**: The policy is undeployed from the switch.

Field	Description
Deployment Date/Time	Specifies the date and time at which the host policy was last updated. The format is *Day MMM DD YYYY HH:MM:SS Timezone*.
Failed Reason	Species why the policy was not successfully deployed.

Global

The Global menu includes the following submenus:

Events

Cisco DCNM allows you to view and purge the various events between the Host and Flow. The Events are recorded on **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 **Administration > DCNM Server > Server Properties** page.

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

Field	Description
Purge	Click to remove the old/unwanted events. **Note** If the DCNM server restarts, by default a maximum of 5000 event entries are retained for 6 hours. Click one of the radio buttons to choose the Purge options. • **Max # of Records**—Enter the maximum number of records to delete. • **# of Days**—Enter the number of days for which you need to delete the events. • **Delete all data from the previous date**—Specifies a date before which all the data is deleted. Click **Purge** to delete/retain PMN events information.
Category	Specifies if the event category.
Severity	Specifies the severity of the event.

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

Config

The Config menu includes the following submenus:

Setting Up the SNMP Server for DCNM

When you add a switch to the DCNM inventory, DCNM automatically configures the switch with the following configuration so that the switch knows where to send SNMP traps: snmp-server host dcnm-host-IP traps version 2c public UDP port - 2162

Follow these steps to establish switch-to-DCNM connectivity if you are planning to use a controller deployment.

Procedure

Step 1 To ensure that DCNM receives SNMP traps from the switches, specify the IP address (or VIP address for native HA) to which the switches send the SNMP traps by configuring DCNM server property `trap.registaddress=dcnm-ip` under **Administrator > Server Properties**.

Step 2 For an Inband environment, use the `pmn_telemetry_snmp` CLI template that is packaged along with the Cisco DCNM Application, to configure more SNMP settings on the switch. For more information, see Switch Global Config, on page 36.

AMQP Notifications

For all DCNM operations (such as Host Alias, Host Policy, and so on), AMQP notifications are sent. For operations triggered by the switch and received through telemetry (such as Flow Status), Cisco DCNM

periodically checks for new events and generate appropriate notifications. This time period can be configured by setting the "AMQP_POLL_TIME" value in the `server.properties`.

To update the `server.properties` file and change AMQP poll interval, perform the following:

1. Locate the `server.properties` file that is located at the following location:

   `/usr/local/cisco/dcm/fm/conf/`
2. Edit the line AMQP_POLL_TIME based on the required poll interval. Poll interval value is in minutes.

   `AMQP_POLL_TIME=5`

   The poll interval is set to 5 minutes. By default, the poll interval is set to 2 minutes.
3. Restart the DCNM server to apply the changes that are made in the `server.properties` file, using the command:

   appmgr restart dcnm—for Standalone deployment

   appmgr restart ha-apps—for Native HA deployment

Note AMQP port 5672 is blocked to ensure AMQP always uses TLS or secure connection.

To open the port, log in to the Cisco DCNM server as a root user, and run the following command: **iptables -t mangle -I BUILTIN-FW-SERVICES -p tcp -m tcp --dport 5672 -j ACCEPT**

AMQP Notification Components

- **Routing Key**

  The routing key is an address that the exchange may use to decide how to route the message. This is similar to a URL in HTTP. Most exchange types use the routing key to implement routing logic, but user may choose to ignore it and filter on some other criteria such as message contents. DCNM PMN additionally includes routing key criteria in message header properties.

- **Routing Key Format**

  The routing key of DCNM PMN AMQP for object notification has following format: `Severity.Operation.ObjectType`

  Example: `info.com.cisco.dcnm.event.pmn.create.host`

Key Identifier	Details
Severity	Message Severity (Info/Warning/Error)
Operation	Create/Update/Delete/Discover/Apply/ Establish/Deploy/SwitchReload/DCNM
Object Type	Object involved in notification includes Host Alias, Host, Host Policy, Flow Policy, Flow, Switch, DCNM.

- **Message Properties**

  Message includes following properties and header which can be used for content parsing.

Property	Value
priority	Message priority. Its default value is 0.
delivery_mode	Delivery mode used for the message. Its default value is 2 (persistent), which means the message is stored both in-memory and on disk.
content_encoding	UTF-8
content_type	MIME type of message content. The default value is application/json.
headers	List of name-value pairs about the message. • Severity—Message Severity (Info/Warning/Error). • Operation Status—Success/Failure. • Operation—Create/Update/Delete/Discover/Apply/Establish/Deploy/SwitchReload/DCNM. • Bulk—True/False indicates bulk operation. • Type—Object involved in notification such as Host Alias, Host, Host Policy, Flow Policy, Flow, Switch, DCNM. • User—Logged-in user who performed the action. • Event—Message sent (for backwards compatibility).
message_id	Message ID

- **Notification Body**

  DCNM notification payload contains necessary information to identify the resources that trigger the notification, as well as link for detailed information retrieval. In case of operation failure, the notification includes the error message with detailed reason.

Switch Global Config

Prior to Release 11, Cisco DCNM Media Controller performed operations such as managing the bandwidth, stitching the flows, host link bandwidth, and so on. Beginning with Release 11, DCNM allows two major operations.

- Monitor the Network
- Configure Host and Flow policies

DCNM monitors the Flow Status, Discovered Host, Applied Host Policies and other operations using Telemetry. For any operations triggered by the switch and received through telemetry (e.g. Flow Established), DCNM periodically checks for new events and generate appropriate notification.

If `pmn.deploy-on-import-reload.enabled` server property is set to true, during a switch reload, when DCNM receives switch coldStartSNMPtrap, it will push Global Config, and Host and Flow policies that are showing 'Deployment Status=Successes' to the switch automatically. The switch telemetry and SNMP configuration can be deployed on demand by using DCNM packaged `pmn_telemetry_snmp` CLI template via **Configure** > **Templates** > **Template Library**.

Navigate to **Cisco DCNM Web UI** > **Media Controller** > **Global** > **Config** to set or modify Switch Global configuration and WAN links.

When Cisco DCNM is installed in Media Controller Deployment mode, you can deploy policies the unicast bandwidth, ASM range, and WAN links through **Web UI** > **Media Controller** > **Global** > **Config**.

After you deploy the DCNM in Media Controller mode, you must configure the bandwidth and ASM. The remaining percentage of the bandwidth is utilized by the multicast traffic. DCNM acts like a Master Controller, and deploy the bandwidth and ASM configurations to all the switches in the fabric.

Navigate to **Cisco DCNM Web UI** > **Media Controller** > **Global** > **Config** > **Switch Global Config** to configure the global parameters.

Note A user with the network operator role in DCNM cannot save, deploy, undeploy, add or delete ASM, or edit the unicast bandwidth reservation percentage.

AMQP Notifications

As Cisco DCNM uses Telemetry to fetch data from the Fabric, the flow status and AMQP notifications may not reflect the current state in real time. It periodically checks new events and generate appropriate notification. Also, flows are no longer limited to a single spine and may take N or W or M shape. Host policies are applied based on the switch interface configuration and not just-in-time (JIT). All these architecture changes influence current AMQP messages and trigger time. By default, poll interval is set to 2 minutes. For more information, see AMQP Notifications, on page 34.

Unicast Bandwidth Reservation

You can configure the server to allot a dedicated percentage of bandwidth to unicast traffic. The remaining percentage is automatically reserved for multicast traffic.

In the Unicast Bandwidth Reservation (%) field, enter a numeric value to configure the bandwidth.

ASM Range

Any Source Multicast (ASM) is a PIM tree building mode that uses shared trees to discover new sources and receivers as well as source trees to form shortest paths from receivers to sources. ASM provides discovery of multicast sources.

You can configure the ASM range by specifying the IP address and the subnet mask.

In the ASM/Mask field, enter the IP address and subnet mask defining the multicast source. Click **Add** icon to add the multicast address to the ASM range. You can add multiple ASM ranges. To delete an ASM range, select the check box next to the ASM/Mask in the table and click **Delete** icon.

After you configure the Unicast Bandwidth Reservation and ASM range, you can perform the following operations to deploy this to the switches.

Table 15: Operations on the Global Config screen

Icon	Description
Save	Click **Save** to save the configurations.
Deploy	After configuring the Unicast Bandwidth and ASM range, you can choose to deploy the configuration. You can choose one of the following from the drop-down list: • **All**—Deploys both ASM and Bandwidth configuration to all switches. • **Bandwidth**—Deploys only the bandwidth configuration. • **ASM**—Deploys only the ASM configuration. • **All Failed**—Deploys all failed deployments. Success or Failed message appears next to each of the ASM range in the table.
Undeploy	You can undeploy the Unicast Bandwidth and ASM range. From the drop-down list, choose one of the following: • **All**—Undeploys both ASM and Bandwidth configuration to all switches. • **Bandwidth**—Undeploys only the bandwidth configuration from the switches. • **ASM**—Undeploys only the ASM configuration.
Status	Unicast Bandwidth Reservation Status specifies if the bandwidth deployment was success, or failed or not deployed. ASM/Mask Status field displays if the ASM and Mask configuration was deployed successfully, or failed or not deployed.
History	Click the respective History link to view the deployment history for Unicast Bandwidth and ASM deployments.

The following table describes the fields that appear on the Deployment History.

Table 16: Deployment History Field and Description

Field	Description
Switch Name	Specifies the switch name in the fabric on which the configuration was deployed.
Action	Specifies the action that is performed on the switch - **Deploy** or **Undeploy**.
Deployment Status	Displays the status of deployment. It shows if the deployment was Success or Failed.
Deployment Date/Time	Displays the date and time when the deployment was initialized.
Failed Reason	Specifies the reason why the deployment failed.
Show	From the drop-down list, choose an appropriate filter. • Quick Filter - A search field appears in every column. You can enter a search string to filter. • Advanced Filter - In the Advanced Filter screen, select the All or Any radio button in the Match field. In the Select Filter field, select the category from the drop-down list. Select an appropriate condition from the drop-down field in the next field. Enter a search string in the next field. Click **Add** icon to add another filter. Click **Remove** icon to delete the filter. Click **Clear** to clear all the filters. Click **Apply** to activate the filters, and view the filtered events. Click **Save** to save the applied filter. Click **Cancel** to discard the advanced filters. • All - This removes all the filters and displays the complete deployment history. • Manage Preset Filters - Select an appropriate filter from the drop-down list. Click Edit to modify the filter parameters. Click **Remove** to delete the filter. Click **Cancel** to discard the changes and revert to Deployment History.
Total	Displays the total number of events on the Deployment History page.

After deploying the global configurations, configure the WAN for each switch in your network.

WAN Links

Beginning with Release 11, Cisco DCNM Web UI allows you to configure WAN links for each switch in your fabric.

The external end devices can connect to the network through a Border Leaf and PIM router. The interface that connects the PIM router to the Border Leaf is called WAN Link.

Note A user with the network operator role in DCNM cannot save, deploy, undeploy, or edit WAN links.

1. From the Select a Switch drop-down list, choose a switch in the fabric for which you want to establish WAN links.

   The list of interfaces on the switch is populated in the following table.

Note The switches that are a part of the fabric appear in the drop-down list.

2. In the WAN Links column, from the drop-down list, choose **Yes** or **No** to designate the interface as a WAN link.
3. Click **View All Deployed WAN Links** to view the Switch Name, Switch IP Address, and Interface Name which is configured as a WAN link. You can choose an appropriate filter to view the WAN links.
4. Click **Save** to save the selection on interfaces as WAN links and other configuration changes.
5. Click **Deploy** to configure the interfaces as WAN links.
6. Click **Undeploy** to remove the WAN links from the switch.

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

Table 17: WAN Links Table Field and Description

Field	Description
Status	Specifies if the WAN links are deployed or undeployed on the selected switch.
History	Click this link to view the deployment history. For description about the fields that appear on this page, see the table below.
Interface Name	Specifies the interface which is connected as a WAN link to the end device.
Admin Status	An up arrow depicts that the status is up. A down arrow implies that the status is down.
Oper Status	An up arrow depicts that the operational state of the interface is up. A down arrow implies that the status is down.

Field	Description
WAN Links	From the drop-down, list you can choose to designate this interface as a WAN link. • Select **Yes** to configure the interface as a WAN link. • Select **No** to remove the interface as a WAN link.
Deployment Status	Specifies if the interface is deployed as a WAN link or not.

The following table describes the fields that appear on the Deployment History.

Table 18: Deployment History Field and Description

Field	Description
Switch Name	Specifies the switch name in the fabric on which the configuration was deployed.
Action	Specifies the action that is performed on the switch - **Deploy** or **Undeploy**.
Deployment Status	Displays the status of deployment. It shows if the deployment was Success or Failed.
Deployment Date/Time	Displays the date and time when the deployment was initialized.
Failed Reason	Specifies the reason why the deployment failed.

Field	Description
Show	From the drop-down list, choose an appropriate filter. • Quick Filter - A search field appears in every column. You can enter a search string to filter. • Advanced Filter - In the Advanced Filter screen, select the All or Any radio button in the Match field. In the Select Filter field, select the category from the drop-down list. Select an appropriate condition from the drop-down field in the next field. Enter a search string in the next field. Click **Add** icon to add another filter. Click **Remove** icon to delete the filter. Click **Clear** to clear all the filters. Click **Apply** to activate the filters, and view the filtered events. Click **Save** to save the applied filter. Click **Cancel** to discard the advanced filters. • All - This removes all the filters and displays the complete deployment history. • Manage Preset Filters - Select an appropriate filter from the drop-down list. Click Edit to modify the filter parameters. Click **Remove** to delete the filter. Click **Cancel** to discard the changes and revert to Deployment History.
Total	Displays the total number of events on the Deployment History page.

DCNM Read-Only Mode for Media Controller

From Cisco DCNM Release 11.1(1), you can use the **pmn.read-only-mode.enabled** server property in DCNM. This property allows you to use the DCNM media controller deployment for only monitoring purposes and not as a policy manager. You can set this property to **true** or **false**. By default, the **pmn.read-only-mode.enabled** server property is set to **false**.

After you modify the **pmn.read-only-mode.enabled** server property, restart DCNM by using the **appmgr restart DCNM** command for the property to take effect.

In a DCNM Native HA setup, you need to follow the standard method of modifying any server property file:

1. Set the server property in the `server.properties` file.
2. Use the **appmgr stop all** command on the secondary appliance and then on the primary appliance.
3. Use the **appmgr start all** command on the primary appliance and then on the secondary appliance for the property to take effect.

When DCNM is in the read-only mode, note the following:

- **Host Policies**, **Flow Policies**, and **Global** menu items in **Media Controller** are hidden.
- Acessing the add, delete, modify, deploy, or undeploy API corresponding to Host or Flow policy, and global configuration will result in an error saying that operation is not allowed in the read-only mode.
- Adding a new device and reloading the switch does not push or repush any configuration from DCNM to the switches.

We recommend that you to take a decision to use DCNM in either the read-only (RO) or read-write (RW) mode when you perform a fresh install of DCNM. After you configure policies or import policies into DCNM, or deploy policies to switches, do not modify DCNM from RO to RW or vice-versa. You can first remove policies configuration in DCNM and switches, and then convert DCNM mode to RO or RW, that is, undeploy (default and custom host-policies, default and custom flow-policies, and global config) and delete all custom policies from DCNM. Similarly, delete any existing policies deployed by DCNM on switches. After DCNM is in the RO mode, you can apply policies on switches directly. In case of DCNM being configured in the RW mode, you can deploy policies from DCNM GUI.

A user is not expected to convert DCNM to the RO or RW mode if any of following cases are true:

- If DCNM already contains policies, that is, host policies, flow policies, and global config.
- If a DCNM instance has deployed policies to switches.
- If switches managed in DCNM are already configured with policies.