

Media Controller

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

Note From Cisco NDFC Release 11.1(1), only a user with the network-admin role can configure a host or flow policy, and global configuration settings.

Note

- From Cisco NDFC 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 NDFC **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 NDFC Software.

If you have configured the Cisco NDFC 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 NDFC 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 NDFC Media Controller API reference on Cisco DevNet.

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

NX-OS Streaming Telemetry and NDFC

Using streaming telemetry, IPFM process on the switch informs NDFC its state using which NDFC is able to show discovered hosts and flows across the IP fabric. The POAP and `pmn_telemetry_snmp` CLI template, which are packaged in NDFC, 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
  sensor-group 400
    data-source DME
    path sys/nbm/show/faults depth unbounded
    path sys/nbm/show/notify depth unbounded
  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
subscription 400
  dst-grp 200
  snsr-grp 400 sample-interval 0
```

Scope in Media Controller

The switch groups that you created in the **Administration > DCNM Server > Switch Groups** window are listed under the **SCOPE** drop-down list.

The **SCOPE** drop-down list is applicable for all the windows under **Media Controller** except the **Events** window.

For example, when you search in the **Topology** window, the search is effective only for the switch group that has been selected in the **SCOPE** drop-down list.

Similarly, the operations for Host, Flow, RTP Flow Monitor, and Global Config windows are effective only for the devices under the switch group selected in the **SCOPE** drop-down list.

The switch groups are separated from one another. For example, you can create a host alias with the same name and IP address for two different switch groups. For more information, see *Managing Switch Groups*.

Note If you select **Data Center** from the **SCOPE** drop-down list, you will see a pop-up window saying that Data Center is not supported.

- Generic Multicast Monitoring, on page 3
- Topology, on page 6
- Host, on page 7
- Flow, on page 21
- RTP, on page 39
- Multicast NAT, on page 41
- Global, on page 53
- Config, on page 55
- NDFC Read-Only Mode for Media Controller, on page 64

Generic Multicast Monitoring

From Cisco NDFC Release 11.4(1), you can use the Generic Multicast feature for monitoring purposes. This feature is applicable for switches with the Cisco NX-OS Release 9.3(5) and later.

Generic Multicast is available with the Media Controller deployment mode. After NDFC installation, decide whether to run NDFC in IP Fabric for Media (IPFM) mode or Generic Multicast mode. You can enable the Generic Multicast mode by using the **pmn.generic-multicast.enabled** server property.

Enabling Generic Multicast Mode

1. Choose **Administration > DCNM Server > Server Properties**.
2. Set the **pmn.generic-multicast.enabled** server property to **true**. By default, this server property is set to **false**.
3. Click **Apply Changes** to save the server settings.
4. A pop-up dialog box appears asking to restart all NDFC services. Click **Ok**.
5. For a standalone NDFC installation, restart NDFC by using the **appmgr restart dcnm** command for the property to take effect.

   For a NDFC HA mode, set the **pmn.generic-multicast.enabled** server property to **true** and click **Failover** in the **Administration / DCNM Server / Native HA** window. The new NDFC active comes up in the generic multicast mode.

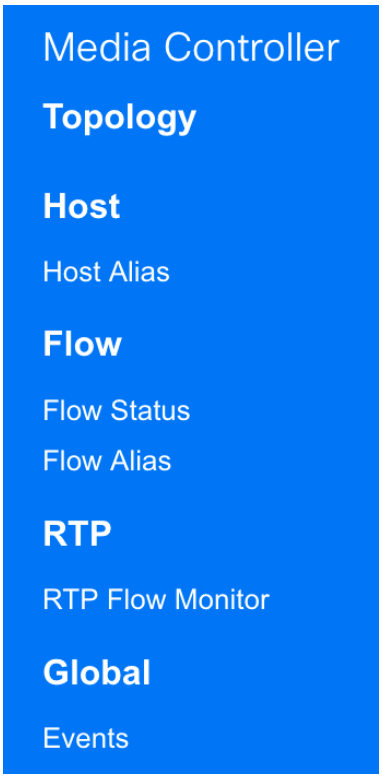


Note

- You can set the **pmn.generic-multicast.enabled** server property to **false** and restart NDFC to enable NDFC in IPFM mode.
- IPFM supports read-only or read/write mode by using a setting in the **Server Properties** window. This property will be not applicable after you set NDFC in the generic multicast mode because IPFM and generic multicast are mutually exclusive features.

Generic Multicast Menu

Cisco NDFC in the generic multicast mode contains a subset of the IPFM features for monitoring.



NX-OS Streaming Telemetry and NDFC (Generic Multicast)

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

```
feature telemetry
 telemetry
  destination-profile
   use-vrf management
  destination-group 600
    ip address <dcnm-ip> port 50051 protocol gRPC encoding GPB.
  sensor-group 600
   data-source DME
   path sys/mca/show/flows depth unbounded
  sensor-group 601
    path sys/mca/show/stats depth unbounded
 subscription 600
  dst-grp 600
  snsr-grp 600 sample-interval 30000
  dst-grp 600
  snsr-grp 600 sample-interval 30000
  snsr-grp 601 sample-interval 60000
 subscription 300
    dst-grp 600
    snsr-grp 300 sample-interval 30000
    snsr-grp 301 sample-interval 60000
 subscription 500
    dst-grp 600
    snsr-grp 500 sample-interval 30000
```

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 NDFC as a Media Controller.

Click a switch and the **Flows** section in the slide out window displays NAT label information, that is, Ingress, Egress, or Ingress and Egress.

Note This section is applicable for both the IPFM and Generic Multicast modes in NDFC.

Generic Multicast isn't limited to the two tier spine or leaf topology. The flow classification and path tracing isn't limited to any specific topology as long as all the involved switches are Cisco Nexus 9000 Series switches with the Cisco NX-OS Release 9.3(5). Generic Multicast is supported for the default VRF.

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

Note

- If you remove a device from the Inventory, the Policy deployment status for that switch is removed. However, 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's shown in the red color indicating that the link is down. The port movements aren't updated in the **Topology** window. Rediscover the switch for the updated ports to be displayed in NDFC.

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**.

In the Generic Multicast mode, also, you can search the receiver-interface name or IP addresses in this window.

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.

Show Panel > Bandwidth

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

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

The display format is *Transmitted-Received*.

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

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

Bandwidth Tracking on Host Facing Link

The senders and receivers can connect to leaf switches of the IPFM Fabric. The sender initiates a multicast flow and the receiver subscribes to a multicast flow. Since multicast is used, there can be multiple receivers subscribing to a flow. The senders are devices such as cameras, microphones, playback devices and so on. The receivers are devices such as video monitors, speakers, multiviewers, and so on.

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

You can track the bandwidth on the host facing link. Using this functionality, NDFC doesn't allow the receiver to request for more flows or sender to send more flows than the available bandwidth on the host facing link.

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 NDFC server at regular intervals using telemetry. Cisco NDFC 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
VRF	Specifies the VRF instance.
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).
NDFC 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.

Starting from Cisco NDFC Release 11.3(1), multiple entries of the same host are grouped together as an expandable row. Click the arrow icon to expand a specific row or collapse multiple rows into a single row.

Host Alias

Note This section is applicable for both the IPFM and Generic Multicast modes in NDFC.

Cisco NDFC 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 NDFC 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 many Host Alias to Cisco NDFC 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 NDFC.

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 NDFC 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 NDFC 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 NDFC 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.
Delete	Allows you to delete the user-defined host policy. **Note** • Undeploy policies from all switches before deleting them from NDFC. • 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 NDFC. • 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 NDFC. **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 NDFC 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 NDFC, 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 NDFC 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 NDFC 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 NDFC 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 NDFC 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 NDFC.

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 NDFC 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 NDFC 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 You cannot undeploy the default configured policies.

Note From Cisco NDFC 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 NDFC Release 11, you can view the policies that you have applied in the entire network. On the Cisco NDFC 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
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

Note This section is applicable for both the IPFM and Generic Multicast modes in NDFC.

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

In the generic multicast mode, switch reports the receiver interface IP address instead of the receiver endpoint IP address. This IP is displayed in the **Flow Status** and **Topology** windows as a host. Also, as there's no policing of the traffic, switch reports only "allowed bytes/packets" and not "denied bytes/packets".

Multicast NAT Visualization

NDFC follows the existing flow classification for multicast flows, that is, active, inactive, sender, or receiver-only. With ingress and egress NAT multiple, input and output addresses can be translated to same group. NDFC aggregates these flows per sender and receiver combination and provides visibility into NAT rules via topology.

Multicast NAT is supported in the IPFM network, and it is not supported for regular or generic multicast.

You can use the **NAT Search** field to search for NAT flows. All pre/post multicast and source IP-Addresses are not visible in the **Flow Status** window. You can view these details for a given flow in a pop-up by clicking the active flow hyperlink. The **NAT Search** feature allows you to enter the IP address of either pre or post source/multicast group and filter relevant entries. Note that searched IP address may not be visible in main table on filtering as it may be part of pre or post entry that can be seen on corresponding pop-up window.

For NAT flow with NAT type containing Ingress, the source and group will be the post NAT source and post NAT group. For NAT type containing Egress, the source and group will be pre-NAT source and pre-NAT group. NAT rules are displayed on the **Sender Only** and **Receiver Only** tabs.

For a NAT flow, the topology graph path tracing shows the **NAT** badge on the switch which has ingress NAT and shows **NAT** label on the link to the receiver for egress NAT.

For NAT flow, there is an extra table shown below the topology graph panel to show all the relevant Ingress NAT or Egress NAT information. The NAT Flow information is also available on the **Topology** window.

The following table provides information about the fields and their descriptions:

Field	Description
NAT	Specifies the NAT mode, that is, Ingress, Egress, or Ingress and Egress. For the Ingress NAT type, the following information is displayed: Ingress (S) – Specifies that ingress NAT is performed on the Sender Switch, also known as First Hop Router (FHR). Ingress (R) - Specifies that ingress NAT is performed on the Receiver Switch (also known as Last Hop Router (LHR). Ingress (S, R) - Specifies that ingress NAT is performed on both the Sender and Receiver Switch.
Pre-Source	Specifies the source IP address before NAT.
Post-Source	Specifies the source IP address after NAT.
Pre-Group	Specifies the multicast group before NAT.
Post-Group	Specifies the multicast group after NAT.
Post S Port	Specifies the source port after NAT.
Post DST Port	Specifies the destination port after NAT.

Fields and Descriptions

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

Table 7: Active Tab

Field	Description
Common Fields for IPFM and Generic Multicast Modes	
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.
NAT	Specifies whether the flow is ingress, Egress, or both Ingress and Egress.
Flow Alias	Specifies the name of the Flow Alias.
Sender	Specifies the IP Address or the Host alias of the sender for the multicast group.
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.
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.
Sender Start Time	Displays the time from when the sender joined.
Receiver Join Time	Specifies the time at which the receiver joined.
Fields Specific for IPFM Mode	
Priority	Specifies the flow priority for flows.
Policed	Specifies whether a flow is policed or not policed.
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.
QOS/DSCP	Specifies the Switch-defined QoS Policy.
Policy ID	Specifies the policy ID applied to the multicast IP.
Field Specific for Generic Multicast Mode	
Receiver Interface IP	Specifies the IP address of the receiver interface joining the group.

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

Table 8: Inactive Tab

Field	Description

Common Fields for IPFM and Generic Multicast Modes	
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.
Sender	Specifies the IP Address or the Host alias of the sender for the multicast group.
Sender Start Time	Displays the time from when the sender joined.
Receiver Join Time	Specifies the time at which the receiver joined.
Fields Specific for IPFM Mode	
Priority	Specifies the flow priority for flows.
Policed	Specifies whether a flow is policed or not policed.
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.
QOS/DSCP	Specifies the Switch-defined QoS Policy.
Policy ID	Specifies the policy ID applied to the multicast IP.
Fault Reason	Specifies reason for the inactive flow. Cisco NDFC 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.
Field Specific for Generic Multicast Mode	
Receiver Interface IP	Specifies the IP address of the receiver interface joining the group.

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

Table 9: Sender Only Tab

Field	Description
Common Fields for IPFM and Generic Multicast Modes	
Multicast IP	Specifies the multicast IP address for the flow.
Flow Alias	Specifies the name of the Flow Alias.

Field	Description
Common Fields for IPFM and Generic Multicast Modes	
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's allow or deny.
Sender Start Time	Displays the time from when the sender switch is transmitting information.
Fields Specific for IPFM Mode	
Policed	Specifies whether a flow is policed or not policed.
Policy ID	Specifies the policy ID applied to the multicast IP.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.

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

Table 10: Receiver Only Tab

Field	Description
Common Fields for IPFM and Generic Multicast Modes	
Multicast IP	Specifies the multicast IP address for the flow.
Flow Alias	Specifies the name of the Flow Alias.
Name	Specifies the receiver ID. If the multicast receiver is remote, the **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's allow or deny.
Receiver Join Time	Specifies the time at which the receiver joined.
Fields Specific for IPFM Mode	
Policy ID	Specifies the policy ID applied to the multicast IP.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.

Note If stats are enabled on switches, only then they can be seen in NDFC.

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 NDFC holds the Flow statistics values in the NDFC server internal memory. Therefore, after a NDFC Restart or HA switch over, the Flow statistics won't 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 NDFC, a message BW_UNAVAIL appears. This is resolved after the uplinks between the switches are detected by NDFC after discovery of the devices.

Flow Alias

Note This section is applicable for both the IPFM and Generic Multicast modes in NDFC.

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.
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 NDFC 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 NDFC 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 NDFC 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 NDFC 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 NDFC 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 NDFC 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 NDFC 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 NDFC.
Delete All	Allows you to delete all the flow policies at a single instance. **Note** Undeploy policies from all switches before deleting them from NDFC.
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 NDFC 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 From the **Flow Priority** drop-down list, choose the priority for the flow. You can choose either **Low** or **Critical**. The default value is **Low**.

The flow priority is used during the following scenarios:

- Error Recovery - Unicast Routing Information Base (URIB) reachability changes on flows, and a re-Reverse-path forwarding (RPF) is being performed. When a set of existing flows is retried, the recovery starts from the flows with **Critical** priority.
- Flow Retry - When pending flows are retried, the **Critical** priority flows are retried first.

Note
The **Flow Priority** drop-down list is applicable only for the switches with the Cisco NX-OS Release 9.3(5) and later.

Step 8 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 NDFC Web UI, perform the following steps:

SUMMARY STEPS

1. Choose **Media Controller > Flow > Flow Policies**.
2. Check the check box next to the flow policy name, that you need to edit.
3. Click **Edit** Flow policy icon.
4. In the Edit Flow Policy window, edit the **Multicast IP**, **Bandwidth**, **QoS/DSCP** fields.
5. Click the **Policer** toggle switch to enable or disable policer for a flow policy.
6. From the **Flow Priority** drop-down list, choose the priority for the flow. You can choose either **Low** or **Critical**. The default value is **Low**.
7. Click **Deploy** to deploy the new policy.

DETAILED 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 From the **Flow Priority** drop-down list, choose the priority for the flow. You can choose either **Low** or **Critical**. The default value is **Low**.

The flow priority is used during the following scenarios:

- Error Recovery - Unicast Routing Information Base (URIB) reachability changes on flows, and a re-Reverse-path forwarding (RPF) is being performed. When a set of existing flows is retried, the recovery starts from the flows with **Critical** priority.
- Flow Retry - When pending flows are retried, the **Critical** priority flows are retried first.

Note
The **Flow Priority** drop-down list is applicable only for the switches with the Cisco NX-OS Release 9.3(5) and later.

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

Click **Cancel** to discard the changes.

Delete Flow Policy

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

SUMMARY STEPS

1. Choose **Media Controller > Flow > Flow Policies**.
2. Click the **Import** flow policy icon.
3. Browse the directory and select the file which contains the Flow Policy configuration information.
4. Click **Open**.

DETAILED 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 NDFC 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 NDFC 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 You cannot undeploy the default configured policies.



Note From Cisco NDFC 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.

Field	Description
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.

Static Flow

You configure a static receiver using the **Static Flow** window.

Table 15: Static Flow Operations

Field	Description
Switch	Allows you to select a switch based on **SCOPE**.
Add	Allows you to add a static flow.
Delete	Allows you to delete a static flow.

Table 16: Static Flow Field and Description

Field	Description
VRF	Specifies the VRF for a static flow.
Group	Specifies the group for a static flow.
Source	Specifies the source IP address for the static flow.
Interface Name	Specifies the interface name for the static flow. If it is not specified while creating the static flow, it is displayed as **N/A**.
Deployment Action	Specifies the action that is performed on the switch for the rule. Create implies that the static flow has been deployed on the switch. Delete implies that the static flow has been undeployed from the switch.
Deployment Status	Specifies if the static flow is deployed or not. If there is a deployment failure, hover over the information icon to view the failure reason.
Last Updated	Specifies the date and time at which the static flow was last updated. The format is Day MMM DD YYYY HH:MM:SS Timezone.

Adding Static Flow

Procedure

Step 1 Navigate to **Media Controller > Flow > Static Flow**.

Step 2 Click the **Add** icon.

Step 3 In the **Add Static Flow** window, specify the following information:

Switch: Specifies the switch name. This field is read-only, and it's based on the switch selected in the **Static Flow** window.

Group: Specifies the multicast group.

Source: Specifies the source IP address.

Interface Name: Specify the interface name for the static flow. This field is optional. If you don't specify an interface name, the host IP 0.0.0.0 is passed to the API and config is created using Null0 interface.

Step 4 Click **Save & Deploy** to save the static flow.

Click **Cancel** to discard it.

Deleting Static Flow

Procedure

Step 1 Navigate to **Media Controller > Flow > Static Flow**.

Step 2 Select a static flow that you need to delete and click the **Delete** icon to delete the selected static flow.

RTP

Note This section is applicable for both the IPFM and Generic Multicast modes in NDFC.

The **RTP** menu includes the **RTP Flow Monitor** submenu.

RTP Flow Monitor

Cisco NDFC provides a view of all the active RTP stream. It also lists out active flows that have RTP drops and historical records for the same. For active media controller flow, NDFC provides RTP topology to pinpoint the loss in network.

Note You need to enable telemetry in the switches to view RTP Flow Monitor. For more information, refer your respective platform documentation.

To view **RTP Flow Monitor**, choose **Media Controller > RTP > RTP Flow Monitor**.

The RTP Flow monitor window has three tabs: **Active**, **Packet Drop**, and **Drop History**.

The description of the fields in these tabs are:

Field	Description
Switch	Specifies the name of the switch.
Interface	Specifies the interface from which the flows are detected.
Source IP	Specifies the source IP address of the flow.
Source Port	Specifies the source port of the flow.
Destination IP	Specifies the destination IP address of the flow.
Destination Port	Specifies the destination port of the flow.
Bit Rate	Specifies the bit rate of the flow, in bps, kbps, mbps, gbps, or tbp.
Packet Count	Specifies the number of packets in the flow.
Packet Loss	Specifies the number of lost packets.
Loss Start	Specifies the time at which the packet loss started.
Loss End	Specifies the time at which the packet loss stopped.
Start Time	Specifies the time at which the flow started.
Protocol	Specifies the protocol that is being used for the flow.

You can click the **Telemetry Switch Sync Status** link to check whether the switches are in sync. The **Sync Status** column displays the status of the switches.

Active

The **Active** tab displays the current active flows. You can also view these flows by navigating to **Media Controller > Flow > Flow Status**.

Click the **Export** icon at the top left of the table to export the Active Flow Status data in a .csv file.

Packet Drop

The **Packet Drop** tab shows the packet drops for active flows.

Click the **Export** icon at the top left of the table to export the Packet Drop data in a .csv file.

Flow Topology

The flow topology is displayed for the active flows that are displayed in the **Media Controller > Flow Status** window.

Click a switch link to display the end-to-end flow topology.

The flow topology displays the direction of the flows, that is, from sender to the receiver. If there are multiple receivers for a given flow, you can choose a receiver from the **Select Receiver** drop-down list.

The switches experiencing packet drops are circled in red.

Hover your cursor over a switch to display the following details:

- Name
- IP address
- Model
- Packet loss, if any

Click the **file** icon next to the links between the switches to view the interface counters errors for the interfaces connecting the two switches.

When you click the file icon, the **show interface <*interface name*> counters errors** command is run for the interface where the flow is participating between these switches, and the results are displayed in a pop-in.

Drop History

When active RTP packet drop is not observed, records from the **Packet Drop** tab are moved to the **Drop History** tab. By default, the RTP drop history is maintained for 7 days. You can customize this setting by updating value for the **pmn.elasticsearch.history.days** property in the **Administration > DCNM Server > Server Properties** window.

Note The **Drop History** tab displays only the last 100,000 records at the maximum.

Click the **Export** icon at the top left of the table to export the Packet Drop History data in a .csv file.

For information about the AMQP based notifications, see Cisco NDFC IP for Media Deployment - AMQP Notifications and for information about REST APIs, see Cisco NDFC API Reference Guide.

Multicast NAT

From Cisco NDFC Release 11.5(1), multicast NAT translation of UDP stream is supported on the NDFC IPFM mode. You can apply NAT for the incoming traffic (ingress), or on the egress link or interface. The scope of ingress NAT is entire switch, whereas egress NAT is for a specific interface. The same switch can have both ingress and egress NAT. However, it can’t be on the same flow for a given switch. Egress NAT has capability to replicate the same flow up to 40 times. To achieve this function, the service-reflect interface is defined on the switch. It serves for multiple or single egress port.

Note Ingress and/or Egress NAT translation is supported only on the sender switch, also known as First Hop Router (FHR), and receiver switch, also known as Last Hop Router (LHR). It is not supported on intermediates nodes such as spine switches.

For more information about NAT, see Cisco Nexus 9000 Series NX-OS IP Fabric for Media Solution Guide, Release 9.3(x).

Prerequisites

- Set up loopback interface with PIM sparse mode. When flow is translated, post-translated source needs to be secondary IP address on this loopback to make sure RPF check won't fail. This loopback is configured as service reflect interface for NAT purpose. You need to set up lookback per VRF.

  Here is an example to configure the loopback interface:

```
interface loopback10
ip router ospf 1 area 0
ip pim sparse-mode
ip address 192.168.1.1/32
ip address 172.16.1.10/32 secondary

ip service-reflect source-interface loopback10
```

- TCAM memory carving must be completed.

  The command to configure the TCAM for Multicast NAT is as follows:

```
hardware access-list tcam region mcast-nat tcam-size
```

  For information about switch models that support multicast NAT, see Configuring Multicast Service Reflection with IPFM in Cisco Nexus 9000 Series NX-OS IP Fabric for Media Solution Guide.

NAT Modes

NAT Mode objects are created per switch and VRF. The switches are populated in the drop-down based on the scope. You should select the switch to list and operate on the corresponding NAT Mode objects.

Table 17: NAT Modes Operations

Field	Description
Switch	Allows you to select a switch based on **SCOPE**.
Add	Allows you to add a new NAT mode.
Delete	Allows you to delete a NAT mode.
Import	Allows you to import NAT modes from a CSV file to NDFC.
Export	Allows you to export NAT modes from NDFC to a CSV file.

Deployment	From the **Deployment** drop-down list, select an appropriate value.
	• Deploy
	  • Selected Modes—Select this option to deploy selected modes to the switch.
	  • All Modes—Select this option to deploy all modes to the switch.
	• Undeploy
	  • Selected Modes—Select this option to undeploy the selected modes.
	  • All Modes—Select this option to undeploy all the modes.
	• Redo All Failed Modes—Select this option to deploy all failed modes.
	All the deployments that failed previously on the selected switch will be deployed again and all the undeployments that failed previously will be undeployed again from the switch.
	• Deployment History— Select this option to view the deployment history of the selected mode.
	Deployment History shows the following fields.
	• Switch Name—Specifies the name of the switch that the mode was deployed to.
	• VRF-Specifies the name of the VRF that mode was deployed to.
	• Group-Specifies the multicast group of the NAT mode.
	• Mode-Specifies the NAT mode, that is, ingress or egress.
	• 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 mode. Create implies that the mode has been deployed on the switch. Delete implies that the mode has been undeployed from the switch.
	• Deployment Date/Time—Specifies the date and time at which the mode was last updated. The format is Day MMM DD YYYY HH:MM:SS Timezone.
	• Failed Reason — Specifies why the mode wasn't successfully deployed.

Table 18: NAT Mode Field and Description

Field	Description
VRF	Specifies the VRF in which the NAT mode is deployed.
Group	Specifies the multicast address of the NAT mode.
Mode	Specifies the multicast NAT mode, that is, ingress or egress.
Deployment Action	Specifies the action that is performed on the switch for that mode. Create implies that the mode has been deployed on the switch. Delete implies that the mode has been undeployed from the switch.

Deployment Status	Specifies if the mode is deployed or not. If there's deployment failure, hover over the information icon to view the failure reason.
Last Updated	Specifies the date and time at which the mode was last updated. The format is Day MMM DD YYYY HH:MM:SS Timezone.

Adding a NAT Mode

Procedure

Step 1 Navigate to **Media Controller > Multicast NAT > NAT Modes**.

Step 2 Click the **Add** icon.

Step 3 In the **Add NAT Mode** window, specify the following information:

Mode: Select the multicast NAT mode, that is, **Ingress** or **Egress**.

Switch: Specifies the switch name. This field is read-only, and it's based on the switch selected in the **NAT Modes** window.

VRF: Select the VRF to which the NAT mode should belong to. For the **Egress** NAT mode, the default VRF is selected and it's non-editable.

Group / Mask: Specify the multicast group with the mask. The same group can't be ingress as well as egress NAT on a given switch. You need to identify whether particular group or mask would be ingress or egress.

Step 4 Click **Save & Deploy** to save the NAT mode and deploy it.

Click **Cancel** to discard the NAT mode.

Deleting a NAT Mode

Deleting a NAT mode doesn't undeploy the NAT Mode from the switch. Therefore, make sure to undeploy the NAT mode from the switch before deleting it from NDFC.

Procedure

Step 1 Navigate to **Media Controller > Multicast NAT > NAT Modes**.

Step 2 Select the NAT mode that you need to delete and select **Deployment > Undeploy > Selected Modes**.

If the NAT mode isn't deployed or failed, you can skip this step.

Step 3 Click the **Delete** icon to delete the selected NAT mode.

Egress Interface Mappings

Table 19: Egress Interface Mappings Operations

Field	Description
Switch	Allows you to select a switch based on **SCOPE**.
Add	Allows you to add an egress interface mapping.
Edit	Allows you to add an egress interface mapping.
Delete	Allows you to delete an egress interface mapping.
Import	Allows you to import egress interface mappings from a CSV file to NDFC.
Export	Allows you to export egress interface mappings from NDFC to a CSV file.

Deployment	From the Deployment drop-down list, select an appropriate value.
	• Deploy
	  • Selected Egress Interface Mappings ─Select this option to deploy selected egress interface mappings to the switch.
	  • All Egress Interface Mappings─Select this option to deploy all egress interface mappings to the switch.
	• Undeploy
	  • Selected Egress Interface Mappings ─Select this option to undeploy the selected egress interface mappings.
	  • All Egress Interface Mappings ─Select this option to undeploy all the egress interface mappings.
	• Redo All Failed Egress Interface Mappings ─Select this option to deploy all failed egress interface mappings.
	All the deployments that failed previously on the selected switch will be deployed again and all the undeployments that failed previously will be undeployed again from the switch.
	• Deployment History─ Select this option to view the deployment history of the selected egress interface mapping.
	Deployment History shows the following fields.
	• Switch Name─Specifies the name of the switch that the egress interface mappings were deployed to.
	• Egress Interface-Specifies the name of the egress interface that the mapping is deployed to.
	• Map Interface-Specifies the map interface for the egress interface mappings.
	• Max Replications-Specifies the maximum replications for the egress interface mappings.
	• 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 egress interface mapping. Create implies that the mapping has been deployed on the switch. Delete implies that the mapping has been undeployed from the switch.
	• Deployment Date/Time─Specifies the date and time at which the mapping was last updated. The format is Day MMM DD YYYY HH:MM:SS Timezone.
	• Failed Reason ─ Specifies why the mapping was not successfully deployed.

Table 20: Egress Interface Mappings Field and Description

Field	Description
Egress Interfaces	Specifies the egress interfaces for the mapping.

Map Interface	Specifies the map interface. Egress interfaces and map interface have Many to One relationship. When there are more than one Egress Interfaces for a mapping, it is shown as a hyperlink. You can click on the hyperlink to see the complete list of interfaces.
Max Replications	Specifies the max replications for the map interface.
Deployment Action	Specifies the action that is performed on the switch for that egress interface mapping. Create implies that the egress interface mapping has been deployed on the switch. Delete implies that the egress interface mapping has been undeployed from the switch.
Deployment Status	Specifies if the egress interface mapping is deployed or not. If there's deployment failure, hover over the information icon to view the failure reason.
Last Updated	Specifies the date and time at which the egress interface mapping was last updated. The format is Day MMM DD YYYY HH:MM:SS Timezone.

Adding Egress Interface Mapping

Procedure

Step 1 Navigate to **Media Controller > Multicast NAT > Egress Interface Mappings**.

Step 2 Click the **Add** icon.

Step 3 In the **Add/Edit Egress Interface Mapping** window, specify the following information:

Switch: Specifies the switch name. This field is read-only, and it's based on the switch selected in the **Egress Interface Mappings** window.

Egress Interface(s): Specifies the egress interface. You can select one or more egress interfaces. Egress Interfaces and Map interface are pre-populated based on the switch selected.

You can select multiple Egress Interfaces by checking the checkboxes and selected interfaces are shown in the box on the right side. Both fields only show the interfaces that are available selection, that is, the interfaces that are already defined in other mappings are filtered out. To select all the interfaces, you can select **All**. When **All** is selected, the list box to select individual egress interfaces is disabled.

Map Interface: Specifies the map interface. An interface can either be an Egress Interface or a Map Interface and can't be both. An error is displayed if you select a map interface that is already selected as an Egress Interface.

Max Replications: Specifies the maximum replications for the map interface. The range for this field is 1–40. The default value is 40.

Step 4 Click **Save & Deploy** to save the egress interface mapping and deploy it.

Click **Cancel** to discard it.

Editing Egress Interface Mapping

Procedure

Step 1 Navigate to **Media Controller > Multicast NAT > Egress Interface Mappings**.

Step 2 Select an egress interface mapping and click **Edit**.

In the **Add/Edit Egress Interface Mapping** window, you can edit egress interfaces and **Max Replications** field. Specify the new value in **Max Replications** that should be within 1–40.

Step 3 Click **Save & Deploy** to save the egress interface mapping and deploy it.

Click **Cancel** to discard it.

Deleting Egress Interface Mapping

Deleting an egress interface mapping doesn't undeploy the egress interface mapping from the switch. Therefore, make sure to undeploy the egress interface mapping from the switch before deleting it from NDFC.

Procedure

Step 1 Navigate to **Media Controller > Multicast NAT > Egress Interface Mappings**.

Step 2 Select an egress interface mapping that you need to delete and select **Deployment > Undeploy > Selected Egress Interface Mappings**.

If the egress interface mapping is not deployed or failed, you can skip this step.

Step 3 Click the **Delete** icon to delete the selected egress interface mapping.

NAT Rules

NAT rules are identical for ingress and egress NAT except you need to also specify receiver OIF for egress NAT.

Table 21: NAT Rules Operations

Field	Description
Switch	Allows you to select a switch based on **SCOPE**.
Add	Allows you to add a NAT rule.
Delete	Allows you to delete a NAT rule.
Import	Allows you to import NAT rules from a CSV file to NDFC.
Export	Allows you to export NAT rules from NDFC to a CSV file.

Deployment	From the Deployment drop-down list, select an appropriate value.
	• Deploy
	  • Selected Rules ─ Select this option to deploy selected NAT rules to the switch.
	  • All Rules ─ Select this option to deploy all NAT rules to the switch.
	• Undeploy
	  • Selected Rules ─Select this option to undeploy the selected NAT rules.
	  • All Rules ─Select this option to undeploy all the NAT rules.
	• Redo All Failed Rules─Select this option to deploy all failed rules.
	All the deployments that failed previously on the selected switch will be deployed again and all the undeployments that failed previously will be undeployed again from the switch.
	• Deployment History─ Select this option to view the deployment history of the selected rule.
	Deployment History shows the following fields.
	• Switch Name─Specifies the name of the switch that the rule was deployed to.
	• VRF-Specifies the VRF that the mapping belongs 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 rule. Create implies that the rule has been deployed on the switch. Delete implies that the rule has been undeployed from the switch.
	• Deployment Date/Time─Specifies the date and time at which the rule was last updated. The format is Day MMM DD YYYY HH:MM:SS Timezone.
	• Failed Reason ─ Specifies why the rule wasn't successfully deployed.

Table 22: NAT Rules Field and Description

Field	Description
VRF	Specifies the VRF for the NAT rule.
Mode	Specifies the NAT mode, that is, ingress or egress.
Pre-Translation Group	Specifies the multicast group before NAT.
Post-Translation Group	Specifies the multicast group after NAT.
Group Mask	Specifies the group mask.
Pre-Translation Source	Specifies the source IP address before NAT.
Post-Translation Source	Specifies the source IP address after NAT.
Source Mask	Specifies the source mask.

Post-Translation Source Port	Specifies the source port after NAT. The range is 0–65535. The value 0 means that there's no translation of UDP source port.
Post-Translation Destination Port	Specifies the destination port after NAT. The value 0 means that there's no translation of UDP destination port.
Static Oif	Specifies the static outgoing interface to bind the Egress NAT rule to. This dropdown is populated with Egress Interfaces defined in the **Egress Interface Mappings** window. This field is disabled for Ingress mode.
Deployment Action	Specifies the action that is performed on the switch for the rule. Create implies that the rule has been deployed on the switch. Delete implies that the rule has been undeployed from the switch.
Deployment Status	Specifies if the rule is deployed or not. If there's a deployment failure, hover over the information icon to view the failure reason.
Last Updated	Specifies the date and time at which the rule was last updated. The format is Day MMM DD YYYY HH:MM:SS Timezone.

Adding NAT Rule

Procedure

Step 1 Navigate to **Media Controller > Multicast NAT > NAT Rules**.

Step 2 Click the **Add** icon.

Step 3 In the **Add NAT Rules** window, specify the following information:

Switch: Specifies the switch name. This field is read-only, and it's based on the switch selected in the **NAT Rules** window.

Mode: Select the NAT mode, that is, ingress or egress.

VRF: Select the VRF for the NAT rule. By default, it's the **default** VRF.

Pre-Translation Group: Specifies the multicast group before NAT.

Post-Translation Group: Specifies the multicast group after NAT.

Group Mask: Specifies the mask value for the NAT rule. By default, it's 32.

Pre-Translation Source: Specifies the source IP address before NAT.

Post-Translation Source: Specifies the source IP address after NAT.

Note
The Post-Translation Source IP needs to be the secondary IP address on the loopback interface to make sure RPF check won't fail.

Source Mask: Specifies the source mask value for the NAT rule. By default, it's 32.

Post-Translation Source Port: Source Port is 0 by default. The value 0 means no translation.

Post-Translation Destination Port: Destination Port is 0 by default. The value 0 means no translation.

Statis Oif: This field is disabled for the **Ingress** mode. In the **Egress** mode, it populates the interfaces based on the Egress Interface Mappings defined.

Step 4 Click **Save & Deploy** to save the NAT rule.

Click **Cancel** to discard it.

Only one Ingress rule can be created for an SG combination, whereas for an Egress rule, the number of rules created for an SG is based on max replication value defined in the Egress Interface Mappings.

Deleting NAT Rule

Deleting a NAT rule doesn't undeploy the NAT rule from the switch. Therefore, make sure to undeploy the NAT rule from the switch before deleting it from NDFC.

Procedure

Step 1 Navigate to **Media Controller > Multicast NAT > NAT Rules**.

Step 2 Select a NAT rule that you need to delete and select **Deployment > Undeploy > Selected NAT Rules**.

If the NAT rule isn't deployed or failed, you can skip this step.

Step 3 Click the **Delete** icon to delete the selected NAT rule.

Border Router Config

You can designate ports as border ports for multi-fabric interconnect in the **Border Router Config** window.

Table 23: Border Router Config Operations

Field	Description
Switch	Allows you to select a switch based on **SCOPE**.
VRF	Allows you to select a VRF.
Status	Displays the status of the border router config. It also displays the deployment date and time, and failed reason.

History	Displays the deployment history for the border router config. Deployment History shows the following fields. • Switch Name—Specifies the name of the switch that the config was deployed to. • VRF-Specifies the name of the VRF that config 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 config. Deploy implies that the config has been deployed on the switch. Undeploy implies that the config has been undeployed from the switch. • Deployment Date/Time—Specifies the date and time at which the config was last updated. The format is Day MMM DD YYYY HH:MM:SS Timezone. • Failed Reason — Specifies why the config was not successfully deployed.
View All Deployed Border Routers	Allows you to view all the deployed border routers.
Save	Allows you to save the border router config on interfaces.
Deploy	Allows you to deploy border router config on interfaces.
Undeploy	Allows you to undeploy border router config on interfaces.

Table 24: Border Router Config Field and Description

Field	Description
Interface Name	Specifies the interface name in the switch.
Admin Status	Specifies the admin status of the interface.
Oper Status	Specifies the operational status of the interface.
Border Router	Specifies whether the interface contains border router config.
Deployment Status	Specifies if the border router config is deployed or not. If there is a deployment failure, hover over the information icon to view the failure reason.

Deploying Border Router Config

Procedure

Step 1 Navigate to **Media Controller > Multicast NAT > Border Router Config**.

Step 2 Select the Switch and VRF from their corresponding drop-down lists.

Step 3 In the **Border Router Config** table, under the **Border Router** column, select **Yes** for an interface to which the border router config must be deployed.

Step 4 Click **Save**, and then **Deploy**.

To remove the border port designation for an already designated port, select **No** from the drop-down, click **Save**, and then click **Deploy**. To remove all the border port designations, click **Undeploy**.

Global

The Global menu includes the following submenus:

Events



Note This section is applicable for both the IPFM and Generic Multicast modes in NDFC.

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

The IPFM Events table is updated real-time.

The maximum stored IPFM 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 NDFC 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 IPFM 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`.

Copying Switch Running Configuration to Start-up Configuration

Whenever there's any deployment to the switch via NDFC, the switch running configuration is automatically saved to the start-up configuration. In other words, NDFC invokes the **copy r s** command on a switch immediately after a deployment to make sure that the configuration is preserved between the switch reloads. An event with the category 'CopyRS' is logged in **Media Controller > Events** when the **copy r s** command is invoked as well as when it's completed either successfully or with an error.

For success, the description of the event is logged as:

`copy r s command successfully completed on switch <switch IP>`

For failure, the description of the event is logged as:

`execution of copy r s command failed for switch <switch IP>, Error: <error message>`

Realtime Notifications

NDFC provides fault notifications via events and AMQP notifications. A key fault notification is when a flow cannot be established end to end in the fabric because of resource unavailability. The realtime fault notification is deleted when the fault is resolved, that is:

- When the flow is established.
- When the request to establish the flow is complete.

From NDFC release 11.5(1), realtime notification is sent on successful flow creation and deletion. If the flow is not established end to end for any reason, this event-based notification is not generated. Instead, a fault notification is generated.

When a switch receives an IGMP Join, it checks for system resources like bandwidth, policer availability, host-policy configuration, and so on, before provisioning the flow. If any resource isn't available, the flow isn't established end to end. Through telemetry, NDFC registers for event-based notifications. NDFC further generates AMQP messages corresponding to the notifications.

For AMQP, you should create a queue to get the event. You should bind this queue to an exchange. In this case, it's **DCNMExchange**. Use this routing key to get real-time notifications: **error.com.cisco.dcnm.event.pmn.realtime.switch**. To get real-time notifications for create or delete flow events, use the routing key: **information.com.cisco.dcnm.event.pmn.realtime.switch**.

These notifications are also available in the Cisco NDFC Web UI in the **Media Controller > Global > Events** window. Whenever a fault is generated, it's displayed as an **Error**. Whenever the fault is removed or cleared, it's displayed as an **Information**. The **Description** column entry contains the fabric or scope name, switch ID, and the unique fault identifier. The **Last Update Time** column provides the time when the event was generated.

Threshold Notifications

NDFC generates threshold notifications in the following scenarios:

- An interface utilization reaches a certain threshold.
- A flow under/over utilizes the allocated bandwidth.

The notification is deleted when the condition is resolved.

As you provision flows on the switch, NDFC checks the interface usage and raises alerts based on the following utilization:

- 60%-74% - WARNING
- 75%-89% - SEVERE
- 90% and over - CRITICAL

For the flow bandwidth notification, switch checks for flow statistics every 1 minute, and by comparing the statistics, rate is calculated. Here are the scenarios:

- If the rate is less than 60 % of the configured flow policy bandwidth, notification is generated.
- If the rate is more than the configured bandwidth, that is, above 100 %, notification is generated.
- When the rate falls back in the range between 60 % and 100 %, notification is removed.

Config

The Config menu includes the following submenus:

Setting Up the SNMP Server for NDFC

When you add a switch to the NDFC inventory, NDFC 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-NDFC connectivity if you are planning to use a controller deployment.

Procedure

Step 1 To ensure that NDFC 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 NDFC 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 NDFC Application, to configure more SNMP settings on the switch. For more information, see Switch Global Config, on page 58.

AMQP Notifications

For all NDFC 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 NDFC 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 NDFC 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 Prior to NDFC 11.5(1), the unsecure AMQP broker port 5672 was open by default and stored in the iptables.save file on NDFC so that the AMQP client can access with HTTP. From NDFC 11.5(1), the port 5672 is closed by default, and AMQP client can access with HTTPs.

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. NDFC IPFM additionally includes routing key criteria in message header properties.

- **Routing Key Format**

The routing key of NDFC IPFM 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/NDFC
Object Type	Object involved in notification includes Host Alias, Host, Host Policy, Flow Policy, Flow, Switch, NDFC.

- **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/NDFC. • Bulk—True/False indicates bulk operation. • Type—Object involved in notification such as Host Alias, Host, Host Policy, Flow Policy, Flow, Switch, NDFC. • User—Logged-in user who performed the action. • Event—Message sent (for backwards compatibility).

Property	Value
message_id	Message ID

- **Notification Body**

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

- Monitor the network.
- Configure host and flow policies.

NDFC 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), NDFC 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 NDFC 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 NDFC 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 NDFC is installed in Media Controller Deployment mode, you can deploy policies the unicast bandwidth, Any Source Multicast (ASM) range, and WAN links through **Web UI > Media Controller > Global > Config**.

After you deploy the NDFC in Media Controller mode, configure the bandwidth and ASM. The remaining percentage of the bandwidth is utilized by the multicast traffic. NDFC 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 NDFC cannot save, deploy, undeploy, add or delete ASM, or edit the unicast bandwidth reservation percentage.

AMQP Notifications

As Cisco NDFC 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 56.

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.

Reserve Bandwidth to Receiver Only

In previous NDFC releases, switch always used to pull ASM traffic to spine to cut down flow set up time. However, this unnecessarily occupies spine bandwidth if there are no active receivers. From Cisco NDFC Release 11.4(1), you can check the **Reserve Bandwidth to Receiver Only** check box to push the ASM traffic to spine only if there is a receiver. This feature is applicable for switches with the Cisco NX-OS Release 9.3(5) and later.

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 these configurations to the switches.

Table 25: Operations on the Global Config screen

Icon	Description
Save	Click **Save** to save the configurations.

Icon	Description
Deploy	To deploy the configuration, you can choose one of the following from the drop-down list: • **All**—Deploys ASM, unicast bandwidth, and reserved bandwidth configuration to all switches. • **Unicast BW**—Deploys only unicast bandwidth configuration. • **Reserve BW**—Deploys only the reserve 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	To undeploy the configuration, you can choose one of the following from the drop-down list: • **All**—Undeploys ASM, unicast bandwidth, and reserved bandwidth configuration to all switches. • **Unicast BW**—Undeploys only unicast bandwidth configuration. • **Reserve BW**—Undeploys only the reserve bandwidth configuration. • **ASM**—Undeploys only the ASM configuration.
Status	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 26: Deployment History Field and Description

Field	Description
Switch Name	Specifies the switch name in the fabric on which the configuration was deployed.

Field	Description
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.

Interface Configs

Beginning with Release 11, Cisco NDFC 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 NDFC cannot save, deploy, undeploy, or edit interface configs.

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

   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 Interfaces** to view the Switch Name, Switch IP Address, and Interface Name which is configured as a WAN link or reserved the bandwidth. You can choose an appropriate filter to view the deployed interfaces.
4. In the **Unicast BW %** column, you can configure the interface to allot a dedicated percentage of bandwidth to unicast traffic. The remaining percentage is automatically reserved for multicast traffic. Enter a numeric value or the default **n/a** value in this column for an interface.

   If you set the unicast bandwidth per interface, then it will take precedence over the global unicast bandwidth reservation.
5. Click **Save** to save the selection on interfaces as WAN links and other configuration changes.
6. Click **Deploy** to configure the interfaces as WAN links.
7. Click **Undeploy** to remove the WAN Links or unconfigure the unicast bandwidth from the switch.

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

Table 27: WAN Links Table Field and Description

Field	Description
Status	Specifies if the WAN links or unicast bandwidths 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 and this interface will be in Layer 3.

Field	Description
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.
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.
Unicast BW %	Specifies the dedicated percentage of bandwidth to the unicast traffic. The remaining percentage is automatically reserved for the multicast traffic. The default value is **n/a**.
Deployment Status	Specifies if the interface is deployed or not.

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

Table 28: 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.

NDFC Read-Only Mode for Media Controller

From Cisco NDFC Release 11.1(1), you can use the **pmn.read-only-mode.enabled** server property in NDFC. This property allows you to use the NDFC 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 NDFC by using the **appmgr restart DCNM** command for the property to take effect.

In a NDFC 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.

Starting from Cisco NDFC Release 11.3(1), Host Policies, Flow Policies, and Global menu items are displayed in the Media Controller deployment in NDFC Read-only mode. NDFC retrieves information about the host policies, flow policies, and global configuration from each switch in the fabric and displays the retrieved information. The information that is displayed is specific to each switch.

Static receiver in read-only mode will not read the static receiver configuration from the device and populate the database. To check the static receivers configured on the switch, you can use the existing GET static receiver API or use the new REST API GET **/pmn/switches/static-receiver-discovery/{switchIp}** to get static receiver from a given switch IP address.

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

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

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

Host Policies - NDFC Read-Only Mode

Navigate to **Media Controller > Host > Host Policies** in NDFC Read-only mode to display the host policies for a switch. By default, information is displayed for the first switch in the **Select Switch** drop-down list. You can select another switch for which you want the information to be displayed from this drop-down list.

Table 29: Host Policies Table Field and Description

Field	Description
VRF	Specifies the VRF instance on the switch where the policy is defined.
Sequence #	Specifies the sequence number of the policy. This field displays 20000000 for default host policies.
Host Name	Specifies the host ID.
Receiver	Specifies the IP address of the receiving device.
Multicast IP / Mask	Specifies the multicast IP address and mask for the host.
Sender	Specifies the IP Address of the sender.

Field	Description
Host Role	Specifies the host device role. The host device role is 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
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*.

Flow Policies - NDFC Read-Only Mode

Navigate to **Media Controller > Flow > Flow Policies** in NDFC Read-only mode to display the flow policies for a switch. By default, information is displayed for the first switch in the **Select Switch** drop-down list. You can select another switch for which you want the information to be displayed from this drop-down list.

Table 30: 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.
Policer	Specifies whether the policer for a flow policy is enabled or disabled.
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*.

Switch Global Config - Read-Only Mode

Navigate to **Media Controller > Global > Config** to display the Switch Global configuration in NDFC Read-Only mode. You can select a switch from the **Select a Switch** drop-down list to display the switch global configuration that is currently deployed on that switch. You can also select a specific VRF from the **Select a VRF** drop-down list.

WAN Links - Read-Only Mode

Navigate to **Media Controller > Global > Config** to and click **WAN Links** to display the WAN links in NDFC Read-Only mode. You can select a switch from the **Select a Switch** drop-down list to display the WAN links that are currently deployed on that switch.

The following table describes the fields that appear on the WAN Links tab.

Table 31: WAN Links Table Field and Description

Field	Description
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.
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.