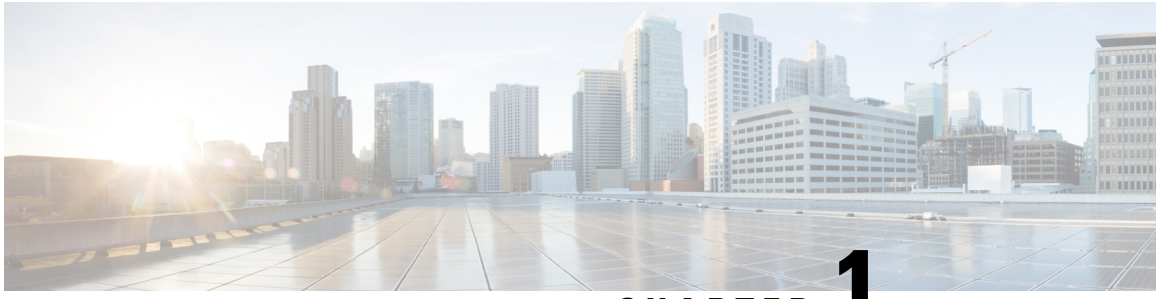
Cisco Nexus 9000 Series NX-OS IP Fabric for Media Solution Guide, Release 9.2(x)

First Published: 2018-07-16

Last Modified: 2019-02-17

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

CONTENTS



CHAPTER 1

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the *Cisco Nexus 9000 Series NX-OS IP Fabric for Media Solution Guide, Release 9.2(x)*.

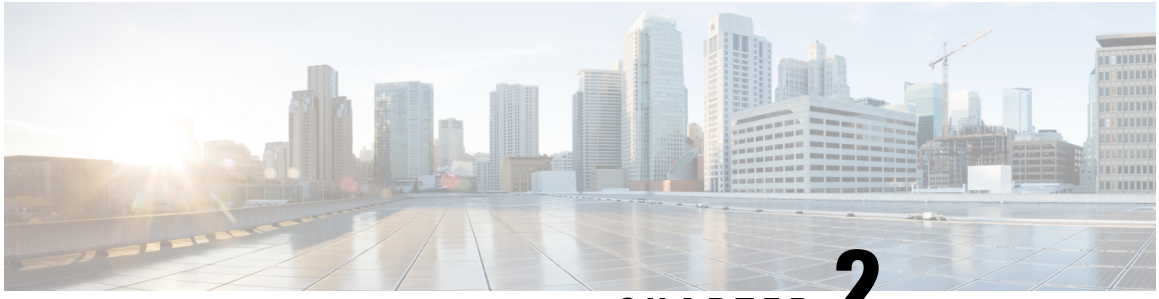
New and Changed Information

This table summarizes the new and changed features for the *Cisco Nexus 9000 Series NX-OS IP Fabric for Media Solution Guide, Release 9.2(x)* and tells you where they are documented.

Table 1: New and Changed Features

Feature	Description	Changed in Release	Where Documented
Host policies	Added the ability to enter a wildcard (0.0.0.0) for the host IP address for sender and local receiver host policies.	9.2(3)	Configuring NBM for a Spine-Leaf Topology, on page 19
NBM	Added the ability to establish flows by creating an NBM flow definition.	9.2(3)	Creating an NBM Flow Definition, on page 37
NBM	Added the ability to disable the policer for NBM flow policies.	9.2(3)	Configuring NBM for a Spine-Leaf Topology, on page 19 Configuring NBM for a Single Modular Switch, on page 34
PIM	Removed the requirement to prebuild the shortest path tree (SPT) for known (S,G) routes using the **ip pim pre-build-spt force** command.	9.2(3)	Configuring PIM on Spine and Leaf Switches, on page 24

Feature	Description	Changed in Release	Where Documented
IP fabric for media	Added support for the Cisco Nexus 9336C-FX2 and 93240YC-FX2 as leaf or spine switches.	9.2(1)	Cisco Nexus 9000 Series Switches, on page 5
Flow bandwidth	Added the ability to configure the flow bandwidth and flow policy bandwidth in Kbps, Mbps, or Gbps and changed the default value to 0.	9.2(1)	Configuring NBM for a Spine-Leaf Topology, on page 19 Configuring NBM for a Single Modular Switch, on page 34
Host policies	Added the ability to configure host policies within NBM for senders, local receivers, and external receivers.	9.2(1)	Configuring NBM for a Spine-Leaf Topology, on page 19
Multisite	Introduced this feature for all IP fabric for media supported platforms.	9.2(1)	Configuring Multisite, on page 40
NBM	Deprecated the **nbm mode controller** command in Cisco NX-OS 9.x releases.	9.2(1)	



CHAPTER 2

Overview of Cisco's IP Fabric for Media Solution

This chapter contains information about Cisco's IP fabric for media solution.

Licensing Requirements

For a complete explanation of Cisco NX-OS licensing recommendations and how to obtain and apply licenses, see the *Cisco NX-OS Licensing Guide*.

About the IP Fabric for Media Solution

Today, the broadcast industry uses a serial digital interface (SDI) router and SDI cables to transport video and audio traffic. The SDI cables can carry only a single unidirectional signal. As a result, many cables, frequently stretched over long distances, are required, making it difficult and time-consuming to expand or change an SDI-based infrastructure.

Cisco's IP fabric for media solution helps transition from an SDI router to an IP-based infrastructure. In an IP-based infrastructure, a single cable can carry multiple bidirectional traffic flows and can support different flow sizes without requiring changes to the physical infrastructure.

The IP fabric for media solution consists of a flexible spine and leaf architecture or a single modular switch topology. The solution uses Cisco Nexus 9000 Series switches with the Cisco non-blocking multicast (NBM) algorithm (an intelligent traffic management algorithm) and with or without the Cisco Data Center Network Manager (DCNM) Media Controller. Using open APIs, the Cisco DCNM Media Controller can integrate with various broadcast controllers. The solution provides a highly reliable (zero drop multicast), highly visible, highly secure, and highly available network.

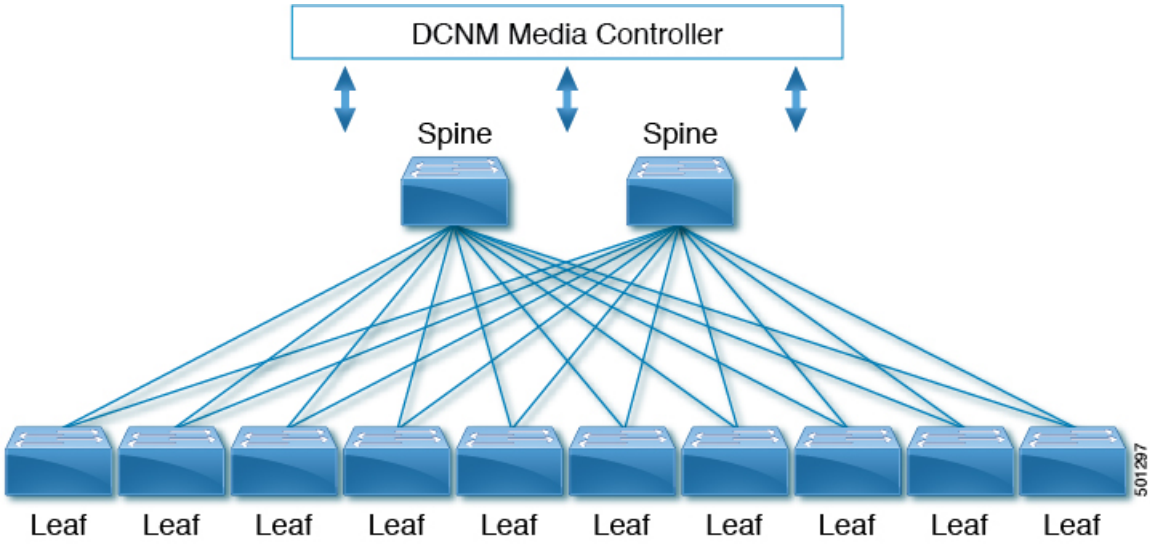
Deployment Types

Cisco's IP fabric for media solution supports the following types of deployments:

- Spine-leaf topology—Flexible architecture for large-scale deployments that are typically seen in an IP studio.
- Single modular switch—Architecture suitable for fixed deployments, with the controller providing features such as flow visibility, security, and monitoring.

Spine-Leaf Topology

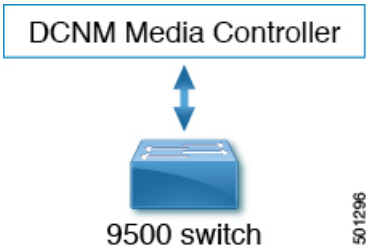
Cisco's IP fabric for media solution supports a spine-leaf topology that consists of multiple spine and leaf switches. The topology supports any combination of leaf switches, including using just one type of leaf switch.



Media sources and receivers connect to the leaf switches, and receivers initiate IGMP join requests to the leaf switches in order to receive the media traffic.

Single Modular Switch Topology

Cisco's IP fabric for media solution supports a single modular switch topology that consists of one Cisco Nexus 9500 Series switch.



IP Fabric for Media Solution Components

Cisco Nexus 9000 Series Switches

The following Cisco Nexus 9000 Series switches are used to transport video and audio traffic through the IP fabric:

Cisco Nexus 9000 Series Switch	Number and Size of Ports	Role in Topology
Cisco Nexus 9236C switch	36 x 40/100-Gbps ports	Spine or leaf in spine-leaf topology
Cisco Nexus 9272Q switch	72 x 40-Gbps ports	Spine or leaf in spine-leaf topology
Cisco Nexus 92160YC-X switch	48 x 1/10/25-Gbps ports	Leaf in spine-leaf topology
Cisco Nexus 9336C-FX2 switch	36 x 40/100-Gbps ports	Spine or leaf in spine-leaf topology
Cisco Nexus 9348GC-FXP switch	48 x 100-Mbps/1-Gbps ports	Leaf in spine-leaf topology
Cisco Nexus 9364C switch	64 x 40/100-Gbps ports	Spine in spine-leaf topology
Cisco Nexus 93108TC-EX switch	48 x 1/10-Gbps ports	Leaf in spine-leaf topology
Cisco Nexus 93108TC-FX switch	48 x 10-Gbps ports	Leaf in spine-leaf topology
Cisco Nexus 93180LC-EX switch	32 x 40/100-Gbps ports	Leaf in spine-leaf topology
Cisco Nexus 93180YC-EX switch	48 x 1/10/25-Gbps ports	Leaf in spine-leaf topology
Cisco Nexus 93180YC-FX switch	48 x 10/25-Gbps ports	Leaf in spine-leaf topology
Cisco Nexus 93240YC-FX2 switch	12 x 40/100-Gbps ports	Spine or leaf in spine-leaf topology
Cisco Nexus 9504 or 9508 switch with the following line cards: • N9K-X9636C-R • N9K-X9636C-RX • N9K-X9636Q-R **Note** The N9K-X96136YC-R line card is not supported.	36 x 40/100-Gbps ports (for N9K-X9636C-R line cards) 32 x 40/100-Gbps ports (for N9K-X9636C-RX line cards) 36 x 40-Gbps ports (for N9K-X9636Q-R line cards)	Spine in spine-leaf topology or single modular switch

*For the latest breakout and optics support, see https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html.

DCNM Media Controller

Through open APIs, the Cisco DCNM Media Controller seamlessly integrates with the broadcast controller and provides a similar operator workflow with all the benefits of an IP-based infrastructure. The DCNM Media Controller features an intuitive GUI that enables you to configure your IP fabric using predefined templates that are designed for media networks.

The DCNM Media Controller enables you to do the following:

- Configure secure generic or multicast-specific policies for individual hosts and allow or deny hosts based on their role.
- Configure secure multicast-specific policies for multiple hosts and flows.
- View the traffic flow and bandwidth utilization to identify problem areas (such as link failures or oversubscriptions) in your fabric.
- Use flow analytics to measure and store bit rates and to display the details for individual traffic flows.
- View an audit log of actions that are performed on the fabric.

Failure Handling

Cisco's IP fabric for media solution supports deterministic failure handling.

During a link or switch failure, the affected flows are moved to alternate links, provided sufficient bandwidth is available. With SMPTE 2022-7, redundancy is built on the endpoints, which ensures that the link or switch failure does not affect production traffic.

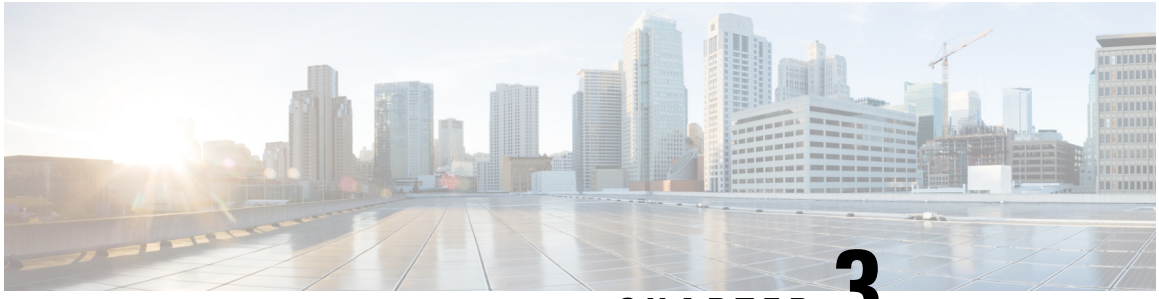
Benefits of the IP Fabric for Media Solution

Cisco's IP fabric for media solution provides the following benefits:

- Replaces specialized hardware (SDI routers) with a general-purpose switching infrastructure.
- Supports various types and sizes of broadcasting equipment endpoints with port speeds up to 100 Gbps.
- Supports the latest video technologies, including 4K and 8K ultra HD.
- Scales horizontally. When you need more capacity, you can add a leaf switch to support more endpoints.
- Provides a deterministic network with zero packet loss, ultra low latency, and minimal jitter.
- Capable of synchronizing all media sources and receivers.
- Provides deterministic failure handling that sends traffic to the receiver when a link fails between a leaf and the spine.
- Supports the coexistence of live and file-based traffic flows for postproduction work.
- Offers increased network security.
- Provides a non-blocking network design to prevent the oversubscription of links.
- Requires no changes to the existing operator workflow.

Related Documentation

Related Topic	Document Title
Cisco DCNM Media Controller	Cisco DCNM Installation Guide for Media Controller Deployment, Release 11.0(1) Cisco DCNM online help
Cisco NX-OS release information	Cisco Nexus 9000 Series NX-OS IP Fabric for Media Release Notes
Cisco NX-OS software upgrades	Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide
IGMP snooping and PIM	Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide
IP fabric for media scalability numbers	Cisco Nexus 9000 Series NX-OS Verified Scalability Guide
NX-API REST	Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference
OSPF	Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide
PTP	Cisco Nexus 9000 Series NX-OS System Management Configuration Guide
QoS	Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide
TCAM carving	Cisco Nexus 9000 Series NX-OS Security Configuration Guide
VLANs	Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide



CHAPTER 3

Setting Up the IP Fabric for Media

This chapter describes how to set up an IP fabric for media network.

Determining the Number and Types of Leaf Switches Required in the IP Fabric

The number and types of leaf switches required in your IP fabric depend on the number and types of endpoints in your broadcasting center.

Follow these steps to help determine how many leaf switches you need:

1. Count the number of endpoints (cameras, microphones, and so on) in your broadcasting center (for example, 360 10-Gbps endpoints and 50 40-Gbps endpoints).
2. Determine the type of leaf switches required based on the type of endpoints in your broadcasting center.
   - For 1-Gbps endpoints, use the Cisco Nexus 9348GC-FXP leaf switch.
   - For 10-Gbps endpoints, use the Cisco Nexus 92160YC-X, 93108TC-EX, 93108TC-FX, 93180YC-FX, or 93180YC-EX leaf switches.
   - For 40-Gbps endpoints, use the Cisco Nexus 9236C, 9272Q, 93240YC-FX2, 9336C-FX2, 9364C, or 93180LC-EX leaf switches.
3. Determine the number of leaf switches required based on the number of endpoints and uplinks that each leaf switch supports.

Note The uplink and downlink numbers in the following table are a recommendation. There are no technical limitations to use certain ports as uplinks or host-facing links.

Table 2: Endpoints and Uplinks Supported Per Leaf Switch

Leaf Switch	Endpoint Capacity	Uplink Capacity
Cisco Nexus 9236C switch	25 x 40-Gbps endpoints	10 x 100-Gbps (1000-Gbps) uplinks
Cisco Nexus 9272Q switch	36 x 40-Gbps endpoints	36 x 40-Gbps (1440-Gbps) uplinks
Cisco Nexus 92160YC-X switch	40 x 10-Gbps endpoints	4 x 100-Gbps (400-Gbps) uplinks
Cisco Nexus 9336C-FX2 switch	25 x 40-Gbps endpoints	10 x 100-Gbps (1000-Gbps) uplinks
Cisco Nexus 9348GC-FXP switch	48 x 1-Gbps/100-Mbps endpoints	2 x 100-Gbps (200-Gbps) uplinks
Cisco Nexus 9364C switch[1]	Not applicable	64 x 100-Gbps (6400-Gbps) uplinks
Cisco Nexus 93108TC-EX switch	48 x 10-Gbps endpoints	6 x 100-Gbps (600-Gbps) uplinks
Cisco Nexus 93108TC-FX switch	48 x 1/10-Gbps endpoints	6 x 100-Gbps (600-Gbps) uplinks
Cisco Nexus 93180LC-EX switch	32 x 40-Gbps endpoints	4 x 100-Gbps (400-Gbps) uplinks
Cisco Nexus 93180YC-EX switch	48 x 10-Gbps endpoints	6 x 100-Gbps (600-Gbps) uplinks
Cisco Nexus 93180YC-FX switch	48 x 10/25-Gbps endpoints	6 x 100-Gbps (600-Gbps) uplinks
Cisco Nexus 93240YC-FX2 switch	48 x 10/25-Gbps endpoints	12 x 100-Gbps (1200-Gbps) uplinks

[1] The Cisco Nexus 9364C switch does not support breakout.

For example:

- For 360 10-Gbps endpoints, you need eight Cisco Nexus 93180YC-EX leaf switches because each switch can support up to 48 10-Gbps endpoints.
- For 50 40-Gbps endpoints, you need two Cisco Nexus 9236C leaf switches because each switch can support up to 25 40-Gbps endpoints.

4. Make sure that the uplink bandwidth (toward the spine switch) is greater than or equal to the downstream bandwidth (toward the endpoints).

   a. Use this equation to determine the uplink bandwidth:

```
Uplink Capacity per Leaf Switch x Number of Leaf Switches = Uplink Bandwidth
```

For example:

600 Gbps (uplink capacity for each Cisco Nexus 93180YC-EX switch) x eight Cisco Nexus 93180YC-EX leaf switches = 4800-Gbps uplink bandwidth

1000 Gbps (uplink capacity for each Cisco Nexus 9236C switch) x two Cisco Nexus 9236C leaf switches = 2000-Gbps uplink bandwidth

4800-Gbps uplink bandwidth (for eight Cisco Nexus 93180YC-EX leaf switches) + 2000-Gbps uplink bandwidth (for two Cisco Nexus 9236C leaf switches) = 6800-Gbps total uplink bandwidth

b. Use this equation to determine the downstream bandwidth:

```
Endpoint Capacity per Leaf Switch x Number of Leaf Switches = Downstream Bandwidth
```

For example:

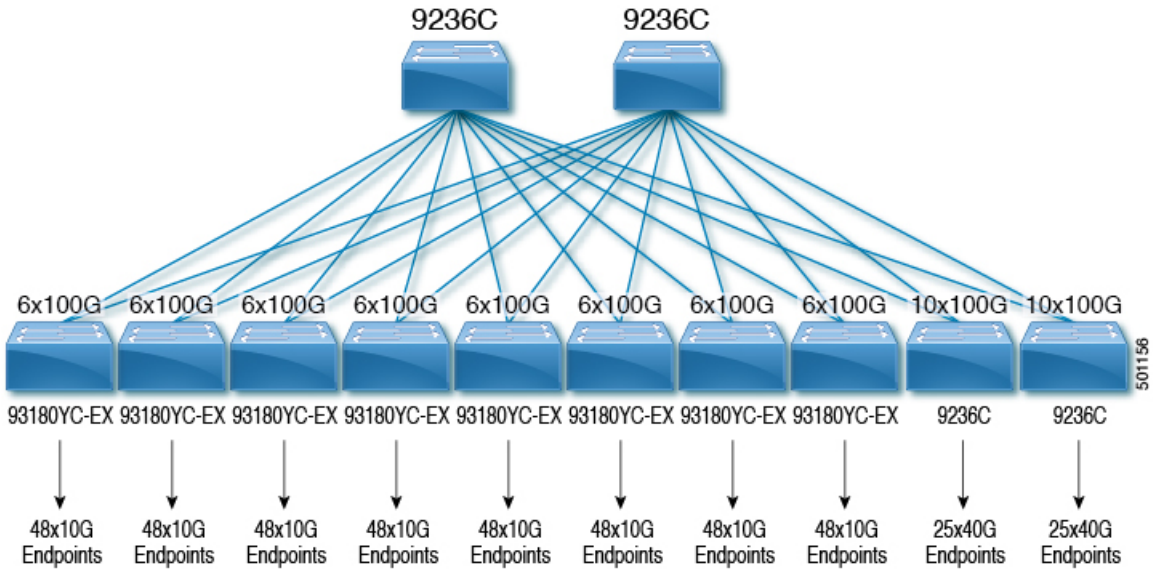
48 x 10 Gbps (480-Gbps endpoint capacity) for each Cisco Nexus 93180YC-EX leaf switch x eight leaf switches = 3840-Gbps downstream bandwidth

25 x 40 Gbps (1000-Gbps endpoint capacity) for each Cisco Nexus 9236C leaf switch x two leaf switches = 2000-Gbps downstream bandwidth

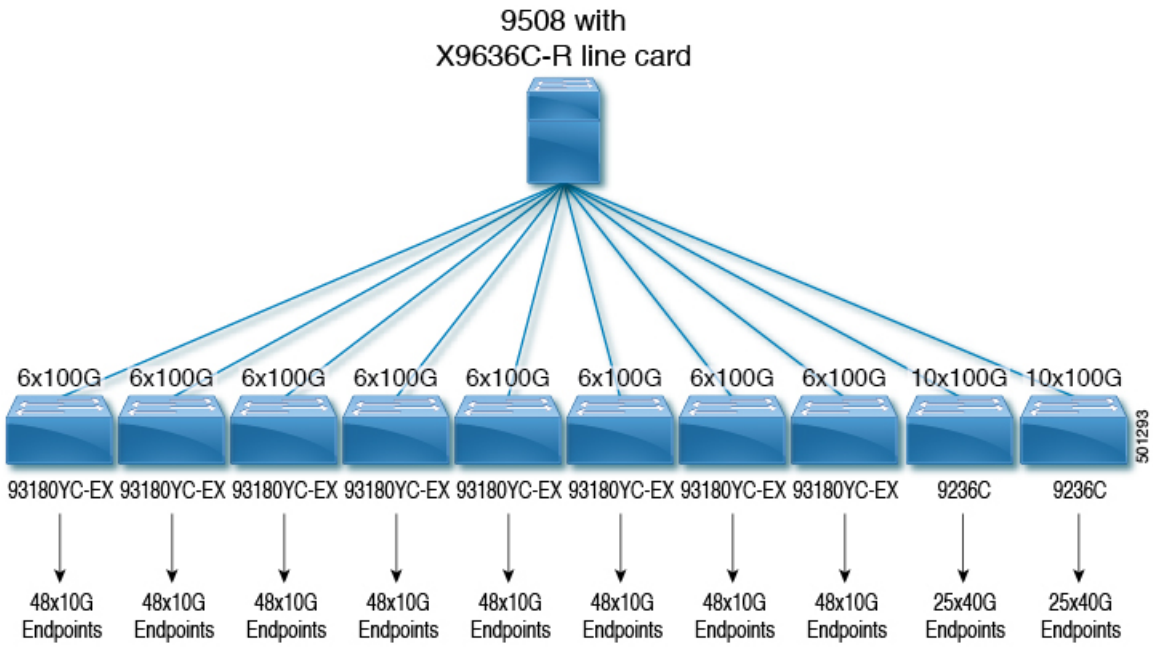
3840-Gbps downstream bandwidth (for eight Cisco Nexus 93180YC-EX leaf switches) + 2000-Gbps downstream bandwidth (for two Cisco Nexus 9236C leaf switches) = 5840-Gbps total downstream bandwidth

5. If the total uplink bandwidth is greater than or equal to the total downstream bandwidth, your topology is valid. You can now determine the number of achievable flows. If the uplink bandwidth is less than the downstream bandwidth, rework your topology until the upstream bandwidth is equal to or greater than the downstream bandwidth.

The following topology uses the examples in this section:



The following diagram shows an example topology with a Cisco Nexus 9508 spine switch and an N9K-X9636C-R line card:



Determining the Number of Achievable Flows in the IP Fabric

Use this equation to determine the number of possible flows in your IP fabric:

```
Total Bandwidth ÷ Flow Size = Number of Achievable Flows
```

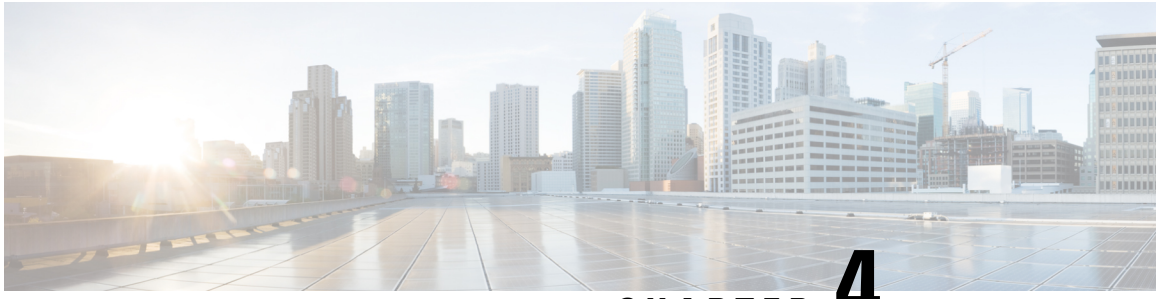
The flow size is configurable and is typically based on the type of video technology that is used in your broadcasting center.

Table 3: Flow Sizes Per Video Technology

Technology	Flow Size
HD video	1.5 Gbps (1500 Mbps)
3G HD video	3 Gbps (3000 Mbps)
4K ultra HD video	12 Gbps (12,000 Mbps)
8K ultra HD video	48 Gbps (48,000 Mbps)

For example:

7200-Gbps total bandwidth ÷ 1.5-Gbps flow size (for HD video) = 4800 possible flows



CHAPTER 4

Configuring IP Fabric for Media

This chapter describes how to configure the Cisco Nexus 9000 Series switches for Cisco's IP fabric for media solution.

Prerequisites

Cisco IP fabric for media solution has the following prerequisites:

- Configure these TCAM carving commands in the following order for all switches (excluding the Cisco Nexus 9504 and 9508 switches with -R line cards) and then reload the switch:

```
hardware access-list tcam region ing-racl 256
hardware access-list tcam region ing-l3-vlan-qos 256
hardware access-list tcam region ing-nbm 1536
```

- Install compatible Cisco NX-OS and DCNM releases. For DCNM installation instructions, see the Cisco DCNM Installation Guide for your DCNM release.

Cisco NX-OS Release	Cisco DCNM Release
9.2(3)	11.1(1)
9.2(2) or 9.2(1)	11.0(1)

Guidelines and Limitations

Cisco's IP fabric for media solution has the following guidelines and limitations:

- The number of leaf switches depends on the number of uplinks that are used and the number of ports available on the spine switch.
- Before you enable NBM, make sure that no flows are active on the switch. If there are active flows, either turn off the flows or reload the switch after configuring NBM.
- NBM is supported only on the default VRF.
- Cisco Nexus 9504 and 9508 switches with the -R line cards do not support policing, DSCP remarking, and flow statistics.
- We recommend using a Layer 3 routed port to an endpoint.
- In a single modular switch deployment using -R line cards with SVIs and endpoints that are connected through a Layer 2 port, the maximum number of flows is 2000.
- For Cisco Nexus 9504 and 9508 switches with -R line cards, six fabric modules are needed for NBM.
- To ensure non-blocking performance, the uplink bandwidth from each leaf switch must be greater than or equal to the bandwidth provided to the endpoints.
- When possible, spread the endpoints across different leaf switches so that there is an equal distribution of sources and receivers on all leaf switches.
- If possible, we recommend overprovisioning uplinks to account for failures.
- As a best practice, use Layer 3 ports that go to the endpoints with a /30 mask. Assign one IP address to the endpoint and another to the switch interface.
- The solution supports IGMPv2 and IGMPv3 joins and PIM Any Source Multicast (ASM) and PIM Source-Specific Multicast (SSM). If multiple sources are sending traffic to the same multicast group in the ASM range, the bandwidth in the fabric is accounted for only one flow. Oversubscription could occur, so take care to avoid multiple senders sending traffic to the same multicast group in the ASM range. In the SSM range, different sources can transmit to the same group, and the bandwidth in the fabric is accounted on a per flow basis.
- Statistics are available only on the switch where senders are connected.
- NBM is not supported with enhanced ISSU. Do not use the [**no**] **boot mode lxc** command in IP fabric for media setups.
- To conserve resources, we recommend disabling statistics when using the **service-policy type qos** command.
- The IP fabric for media solution supports receiver-side bandwidth management, where the IGMP and PIM endpoints on the external link are bandwidth managed.
- The IP fabric for media solution supports dynamic flow policy changes for DSCP and flow bandwidth.
- All supported IP fabric for media platforms allow the sender or receiver end hosts to be connected to the spine.
- The IP fabric for media solution supports multiple border leafs per fabric.
- If you change the unicast bandwidth percentage, you must flap the fabric links for the new value to take effect.
- Only Layer 3 interfaces can be configured as NBM external links. If a Layer 3 interface is changed to a switch port, the NBM external link configuration is removed.

- When you configure a Layer 3 interface as an NBM external link, the interface flaps.
- If an RPF or any of the OIF interfaces cannot accommodate a bandwidth change, the flow is torn down. The next IGMP or PIM join will initiate flow stitching.
- When you change the flow policy (bandwidth) for groups with existing flows in the fabric, make the changes in the following order to reduce the impact on existing flows. Otherwise, oversubscription could occur, depending on the available bandwidth for the interfaces in use.
  1. Change from a lower to higher bandwidth: Modify the policy first on all last hop routers for the existing flows, then on all spine switches, and then on the rest of the switches.
  2. Change from a higher to lower bandwidth: Modify the policy first on all first hop routers for the existing flows, then on all spine switches, and then on the rest of the switches.
- Statistics are not available if you disable the NBM flow policer.
- NBM running on a VXLAN enabled switch is not supported. Feature NBM may disrupt VXLAN underlay multicast forwarding.

Guidelines and Limitations for Host Policies

The following guidelines and limitations apply to host policies:

- Default host policies are configured automatically and are allowed by default.
- By default, all external receiver (PIM) and sender host policies are applied on the external links.
- Delete any custom NBM host policies before updating a default policy.
- All receiver policies are per interface for a given (S,G). Once the policy is applied on an interface for a given (S,G), it is applied to all the reporters in that subnet.
- Host policies are implemented in the software and are not applied to any physical interfaces, such as ACLs and route maps.
- An interface's operational up and down events do not determine if a host policy is applied to the interface.
- Any valid interface with an assigned IP address has host policies that are associated with it based on the subnet IP address.
- Host policies are consulted for the senders and receivers on an interface only when the interface is in the operational up state.
- For PIM and local receiver host policies, the source or the group must be defined and should not be 0.0.0.0 (any). To allow a receiver to subscribe to all groups, use the following example:

```
10 host 192.168.1.1 source 0.0.0.0 group 224.0.0.0/4 {permit | deny}
```

Note If you enter a wild card (0.0.0.0) for the host IP address for a local receiver host policy, which is supported beginning with Cisco NX-OS Release 9.2(3), the source IP address is also a wild card, but a valid group is required.

- If you configure sender host policies with the same host IP address and the same multicast group prefix but with a different action, the latest configuration is rejected.

```
nbm host-policy
sender
10 host 101.1.1.3 group 229.1.1.1/32 deny
20 host 101.1.1.3 group 229.1.1.1/32 permit ←This policy is rejected.
```

- If you configure external receiver (PIM) host policies with the same source IP address and the same multicast group prefix but with a different action, the latest configuration is rejected.

```
nbm host-policy
pim
30 source 111.1.1.3 group 239.1.1.1/32 deny
40 source 111.1.1.3 group 239.1.1.1/32 permit ←This policy is rejected.
```

- If you configure local receiver host policies with the same source IP address and multicast group prefix but with a different host IP address and a different action, the policy with the lowest sequence number (10) takes precedence. If you delete the policy with the lowest sequence number (10), the policy with the next lowest sequence number (20) becomes active.

```
nbm host-policy
receiver
10 host 100.1.1.1 source 145.1.1.1 group 234.1.1.1/32 deny ←This policy takes precedence.
20 host 100.1.1.2 source 145.1.1.1 group 234.1.1.1/32 permit
```

Guidelines and Limitations for Unicast PTP

The following guidelines and limitations apply to unicast PTP:

- Configure every unicast PTP interface with a unique PTP unicast source address.
- The global PTP source and the unicast interface PTP source should not be the same.
- Unicast and multicast are not supported on the same interface.
- We recommend that you modify the default CoPP profile and increase the Committed Information Rate (CIR) of PTP from 280 kbps to 1024 kbps.
- Unicast PTP is supported only for the following platforms:
  - Cisco Nexus 9236C, 9272Q, and 92160YC-X switches
  - Cisco Nexus 93108TC-FX, 93180YC-FX, 93240YC-FX2, 9336C-FX2, 9348GC-FXP, and 9364C switches
  - Cisco Nexus 9504 and 9508 switches with -R line cards

Guidelines and Limitations for the DCNM Media Controller

The following guidelines and limitations apply to DCNM in general:

- Make sure that there is always connectivity to the controller by ensuring redundant paths.

- Do not use CLI commands to modify any policy that is pushed from DCNM. Make any modifications using DCNM.
- When you change any IP fabric for media-related server properties using **DCNM Administration** > **DCNM Server** > **Server Properties**, you must restart DCNM. For installation instructions, see the Installing Cisco DCNM for Media Controller Deployment.
- DCNM leverages the telemetry feature on the switch to stream out IP fabric for media data and uses ElasticSearch for persistence. By default, DCNM stores the historical telemetry data for up to seven days. You can adjust the data retention period using DCNM server property **pmn.elasticsearch.history.days**.
- When a switch is imported into DCNM, DCNM deletes all the host policies, flow policies, WAN links, ASM range, and reserved unicast bandwidth that are configured on that switch. It also resets the host policy as permit, the flow policy as 0 Kbps, and the reserved unicast bandwidth as 0%. If other switches in the same fabric already have policies and configurations that are deployed by DCNM, DCNM deploys the same set of policies and configurations (except WAN link configurations) to the newly imported switch so that the policies and configurations on all switches in the fabric are in sync.
- DCNM listens for a switch's SNMP reload trap. When DCNM detects that a switch has been reloaded, it deletes all the host policies, flow policies, and WAN links configured on that switch. It also resets the host policy as permit, the flow policy as 0 Kbps, and the reserved unicast bandwidth as 0% and redeploys the policies and configurations that have been deployed to that switch.
- If you choose to keep the existing configurations on the switch intact during a switch import and reload, you can set DCNM server property **pmn.deploy-on-import-reload.enabled** to **'false'** and then restart DCNM to make the change effective.

The following guidelines and limitations apply to the flow setup:

- DCNM notifies the broadcast controller or user if an API call is unsuccessful, which requires the broadcast controller or user to retry.
- Static receiver API is not supported with SVIs.
- VM snapshot is not supported. You cannot roll back to a previous DCNM snapshot.

The following guidelines and limitations apply to the flow policy:

- Make default policy changes before any flows are active on the fabric.
- Account for 5% more than the flow bit rate to accommodate a certain amount of burst without the flow being policed. For example, provision a 3G flow as 3.15 Gbps.
- Flow policies can be modified, but flows using those policies are impacted during the modification.

The following guidelines and limitations apply to the host policy:

- When a receiver host policy is applied to a host connected via a Layer 2 port and an SVI, the policy applies to all joins sent by all hosts on that VLAN and cannot be applied to a single receiver.
- Default host policies can be modified only when no custom host policies are defined. In order to modify the default policy, you have to undeploy and then delete any custom policies.
- DCNM supports a multicast range for host policies. By default, DCNM does not allow you to specify the netmask or prefix, but it automatically generates the sequence number for the host policy. If you want to specify the multicast range and manually input the sequence number for the host policy, you can set DCNM server property **pmn.hostpolicy.multicast-ranges.enabled** to **'true'** and restart DCNM.

The following guidelines and limitations apply to network and DCNM connections:

- The DCNM HA pair must be on the same VLAN.
- Connectivity between DCNM and the switch can be done over the out-of-band management port or using in-band management.

Licensing Requirements for DCNM Media Controller

Product	License Requirement
Cisco DCNM	The Cisco DCNM Media Controller requires the Advanced Server DCNM license. For more information on this license, see the Cisco DCNM Installation Guide.

Upgrading to a Cisco NX-OS 9.x Release

Upgrading from a Cisco NX-OS 9.x Release

Follow these steps to upgrade from a Cisco NX-OS 9.x release to a later 9.x release in an IP fabric for media deployment.

Step 1 Upgrade the switch software to a later 9.x release using the **install all** command.

Step 2 Configure TCAM carving for NBM and reload the switch.

Step 3 Upgrade DCNM.

Upgrading from a Cisco NX-OS 7.x Release

Follow these steps to upgrade from a Cisco NX-OS 7.x release to a 9.x release in an IP fabric for media deployment.

Note For Cisco Nexus 9504 and 9508 switches with -R line cards, you must upgrade from Cisco NX-OS Release 7.0(3)F3(4) to a 9.x release.

Step 1 Shut down the endpoint-facing ports on the switches.

Step 2 Disable NBM (using the **no feature nbm** command).

Step 3 If you are upgrading to Cisco NX-OS Release 9.2(3) or a later release, disable the **ip pim pre-build-spt force** command on the spine switches in your fabric.

Step 4 Disable PIM passive mode (using the **no ip pim passive** command).

Step 5 Upgrade the switch software to a 9.x release.

Step 6 Configure TCAM carving for NBM and reload the switch.

Step 7 Upgrade DCNM.

Step 8 Configure PIM and MSDP, if applicable.

Step 9 Enable NBM (using the **feature nbm** command).

Step 10 Configure NBM policies using the CLI or DCNM.

Step 11 If you are upgrading to Cisco NX-OS Release 9.2(3) or a later release and you are not using DCNM, disable IGMP static OIF and create an NBM flow definition to establish a flow.

Step 12 Enable all ports facing the endpoints.

Setting Up the SNMP Server for DCNM

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

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

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

Step 2 For an inband environment, you can use the DCNM-packaged **`pmn_telemetry_snmp`** CLI template to configure more SNMP settings (such as the source interface) on the switch. For more information, see #unique_35.

Step 3 Save the configuration and restart DCNM.

Configuring NBM

The procedure for configuring non-blocking multicast (NBM) varies depending on which deployment method you are using for your IP fabric for media solution.

- Spine-leaf topology
- Single modular switch

Configuring NBM for a Spine-Leaf Topology

Follow this procedure to configure NBM for switches in a spine-leaf deployment. In this mode, you can enable PIM active mode on spine and leaf switches. This feature provides multicast flow setup intelligence within the fabric. It supports multiple spines and variable flow size.

The spine-leaf topology utilizes NBM along with Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP) for provisioning flows within the fabric. The fabric must be configured with Configuring PIM on Spine and Leaf Switches and Configuring MSDP on Spine Switches.

Before you begin

Enable the PIM feature (using the **feature pim** command).

Enable the OSPF feature (using the **feature ospf** command), if you are using the OSPF unicast routing protocol.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **feature nbm**
3. (Optional) [**no**] **nbm host-policy**
4. (Optional) {**sender** | **receiver** | **pim**}
5. (Optional) **default** {**permit** | **deny**}
6. (Optional) Enter one of the following commands:
   - For sender host policies: *sequence-number* **host** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
   - For local receiver host policies: *sequence-number* **host** *ip-address* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
   - For external receiver (PIM) host policies: *sequence-number* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
7. (Optional) [**no**] **nbm reserve unicast fabric bandwidth** *value*
8. [**no**] **nbm flow asm range** [*group-range-prefixes*]
9. [**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**}
10. [**no**] **nbm flow dscp** *value*
11. (Optional) [**no**] **nbm flow policer**
12. [**no**] **nbm flow-policy**
13. [**no**] **policy** *policy-name*
14. (Optional) [**no**] **policer**
15. [**no**] **bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**}
16. [**no**] **dscp** *value*
17. [**no**] **ip group-range** *ip-address* **to** *ip-address*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **feature nbm** **Example:** `switch(config)# feature nbm`	Enables the NBM feature and PIM active mode, which allows the NBM fabric to form a multicast flow without assistance from an external controller.

	Command or Action	Purpose
		When you enter the **feature nbm** command, the following commands are also enabled automatically: • **nbm mode pim-active** • **ip multicast multipath nbm** • **ip pim prune-on-expiry** • **cdp enable** The **no** form of this command disables the following commands: **feature nbm**, **nbm mode pim-active**, **ip multicast multipath nbm**, and **ip pim prune-on-expiry**.

Step 3	(Optional) [**no**] **nbm host-policy**
	Example:
	`switch(config)# nbm host-policy`
	`switch(config-nbm-host-pol)#`
		Configures an NBM host policy for the switch.

Step 4	(Optional) {**sender** | **receiver** | **pim**}
	Example:
	`switch(config-nbm-host-pol)# sender`
	`switch(config-nbm-host-pol-sender)#`
		Configures the NBM host policy for a sender, local receiver, or external receiver (PIM).
		Note Before you update the default NBM host policy, you must first delete any custom host policies.

Step 5	(Optional) **default** {**permit** | **deny**} **Example:** `switch(config-nbm-host-pol-sender)# default permit`	Specifies the default action for the NBM host policy. All three types of host policies are allowed by default.

Step 6	(Optional) Enter one of the following commands:
	• For sender host policies: *sequence-number* **host** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
	• For local receiver host policies: *sequence-number* **host** *ip-address* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
	• For external receiver (PIM) host policies: *sequence-number* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
	Example:
	`switch(config-nbm-host-pol-sender)# 10 host 101.1.1.3 group 229.1.1.1/32 deny`
	Example:
	`switch(config-nbm-host-pol-rcvr)# 40 host 100.1.1.1 source 145.1.1.1 group 234.1.1.1/32 deny`
	Example:
	`switch(config-nbm-host-pol-pim)# 50 source 101.1.1.1 group 235.1.1.1/32 deny`
		Specifies if the sender or receiver flows are to be permitted or denied.
		Beginning with Cisco NX-OS Release 9.2(3), you can enter a wildcard (0.0.0.0) for the host IP address for sender and local receiver host policies. In previous releases, the host IP address is required so that the host policy can be associated with the interface on the switch. Using a wildcard allows you to detect all hosts that are sending or receiving multicast traffic on a particular group or mask using a single configuration. When the host IP address is a wildcard for local receiver host policies, the source IP address is also a wildcard. See the wildcard configuration example at the end of this procedure.

	Command or Action	Purpose
Step 7	(Optional) [**no**] **nbm reserve unicast fabric bandwidth** *value* **Example:** `switch(config)# nbm reserve unicast fabric bandwidth 2`	Reserves a percentage of bandwidth on fabric ports for unicast flows. NBM flow management does not use this bandwidth for flow setup and reserves it on all fabric interfaces for the unicast traffic. The range is from 0 to 100 percent, and the default value is 0.
Step 8	[**no**] **nbm flow asm range** [*group-range-prefixes*] **Example:** `switch(config)# nbm flow asm range 224.0.0.0/8 225.0.0.0/8 226.0.0.0/8 227.0.0.0/8`	Programs the NBM ASM group range for *,G joins. The IGMP joins in this group range are expected to be V2 joins or (*, G) joins. You can configure up to 20 group ranges. The default is no configured group range. **Note** This command is needed only in a multispine deployment.
Step 9	[**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} **Example:** `switch(config)# nbm flow bandwidth 3000 mbps`	Configures the global NBM flow bandwidth in Kbps, Mbps, or Gbps. The minimum supported flow bandwidth is 200 Kbps. **Range** / **Default Value**: 1 to 25,000,000 Kbps — 0 Kbps 1 to 25,000 Mbps — 0 Mbps 1 to 25 Gbps — 0 Gbps
Step 10	[**no**] **nbm flow dscp** *value* **Example:** `switch(config)# nbm flow dscp 10`	Configures the global NBM flow DSCP value. The range is from 0 to 63. If any of the flows do not match the NBM flow group range, the default flow DSCP is used for bandwidth management and flow setup.
Step 11	(Optional) [**no**] **nbm flow policer** **Example:** `switch(config)# no nbm flow policer`	Enables or disables the policer for all NBM flow policies. The policer is enabled by default. **Note** This command is available beginning with Cisco NX-OS Release 9.2(3).

Step 12	[**no**] **nbm flow-policy**
	Example:
	`switch(config)# nbm flow-policy`
	`switch(config-nbm-flow-pol)#`
		Configures the flow bandwidth per flow.

Step 13	[**no**] **policy** *policy-name*
	Example:
	`switch(config-nbm-flow-pol)# policy nbmflow10`
	`switch(config-nbm-flow-pol-attr)#`
		Configures the NBM flow policy. You can specify a maximum of 63 alphanumeric characters for the policy name.

Step 14	(Optional) [**no**] **policer** **Example:**	Enables or disables the policer for the specified NBM flow policy.

	Command or Action	Purpose
	`switch(config-nbm-flow-pol-attr)# no policer`	By default, each source flow uses a policer on the source leaf (the first hop router). In a scenario where the number of multicast source flows exceeds the number of policers, the flow is not accepted by the source leaf. To override this behavior, you can disable the policer under the flow policy. For flows that match the flow policy where the policer is disabled, no policer resource is consumed. **Note** Use this command with caution as it could lead to an unprotected network, where a misbehaving endpoint could transmit more than what it is allowed. Use another method, such as an aggregate policer, to rate limit flows that have no policer programmed by NBM. For information on configuring an aggregate policer, see Configuring Shared Policers. **Note** This command is available beginning with Cisco NX-OS Release 9.2(3).
Step 15	[**no**] **bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} **Example:** `switch(config-nbm-flow-pol-attr)# bandwidth 10 mbps`	Configures the flow bandwidth in Kbps, Mbps, or Gbps for multicast groups matching this policy. The minimum supported flow bandwidth is 200 Kbps. **Range** / **Default Value** 1 to 25,000,000 Kbps / 0 Kbps 1 to 25,000 Mbps / 0 Mbps 1 to 25 Gbps / 0 Gbps
Step 16	[**no**] **dscp** *value* **Example:** `switch(config-nbm-flow-pol-attr)# dscp 10`	Configures the differentiated services code point (DSCP) value on the first-hop redundancy for flows matching the specified group range.

Step 17	[**no**] **ip group-range** *ip-address* **to** *ip-address*
	Example:
	`switch(config-nbm-flow-pol-attr)# ip group-range 224.19.10.1 to 224.19.255.1`
	`switch(config-nbm-flow-pol-attr)# ip group-range 224.20.10.1 to 224.20.255.1`
		Specifies the IP address range for multicast groups that are associated to this policy.

Example

The following example shows a sample configuration for a wildcard host policy:

```
switch(config)# nbm host-policy
  sender
    default permit
```

```
    1100 host 0.0.0.0 group 224.1.1.1/32 permit  << Sender wildcard
  receiver
    default permit
    1100 host 0.0.0.0 source 0.0.0.0 group 231.1.1.1/32 permit  << Receiver wildcards

switch(config)# show nbm host-policy applied sender all
Default Sender Policy: Allow
Applied WildCard host policies
Seq Num    Source     Group       Group Mask  Action
1100       0.0.0.0    224.1.1.1   32          Allow
Total Policies Found = 1

switch(config)# show nbm host-policy applied receiver local all
Default Local Receiver Policy: Allow
Interface  Seq Num  Source   Group      Group Mask  Action  Deny counter  WILDCARD
           1100     0.0.0.0  231.1.1.1  32          Allow   0
Total Policies Found = 1
```

What to do next

Establishing a Flow (Optional)

Configuring PIM on Spine and Leaf Switches

Configuring MSDP on Spine Switches

Configuring PIM on Spine and Leaf Switches

Follow these steps to configure PIM for spine and leaf switches in a spine-leaf topology. The configuration should be the same on all nodes.

Before you begin

Configure NBM for a spine-leaf topology.

SUMMARY STEPS

1. **configure terminal**
2. **ip pim rp-address** *rp-address* **group-list** *ip-prefix*
3. **ip pim ssm range none**
4. **ip pim spt-threshold infinity group-list** *route-map-name*
5. **route-map** *policy-name* **permit** *sequence-number*
6. **match ip multicast group** *policy-name* **permit** *sequence-number*
7. **interface** *interface-type slot/port*
8. **mtu** *mtu-size*
9. **ip address** *ip-prefix*
10. **ip ospf passive-interface**
11. **ip router ospf** *instance-tag* **area** *area-id*
12. **ip pim sparse-mode**
13. **ip igmp version** *number*
14. **ip igmp immediate-leave**
15. **ip pim pre-build-spt force**
16. Configure an RP interface.

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip pim rp-address** *rp-address* **group-list** *ip-prefix* **Example:** `switch(config)# ip pim rp-address 1.2.1.1 group-list 224.0.0.0/4`	Configures a PIM static RP address for a multicast group range. The spine must be configured as the RP. In a multi-spine deployment, all spines must be configured as the RP with the same IP address configured on a loopback interface.
Step 3	**ip pim ssm range none** **Example:** `switch(config)# ip pim ssm range none`	Forces sender traffic to the spine layer, which reduces flow setup latency. **Note** SSM is still supported in the fabric, and this command does not disable SSM.
Step 4	**ip pim spt-threshold infinity group-list** *route-map-name* **Example:** `switch(config)# ip pim spt-threshold infinity group-list mcast-all`	Creates the IPv4 PIM (*, G) state only, for the group prefixes defined in the specified route map.

Step 5	**route-map** *policy-name* **permit** *sequence-number*
	Example:
	`switch(config)# route-map mcast-all permit 10`
	`switch(config-route-map)#`
		Enters route-map configuration mode.

Step 6	**match ip multicast group** *policy-name* **permit** *sequence-number* **Example:** `switch(config-route-map)# match ip multicast group 224.0.0.0/4`	Matches the specified group. Make sure that the route-map group address matches the NBM flow ASM range group address.

Step 7	**interface** *interface-type slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Specifies an interface to configure and enters the interface configuration mode.

Step 8	**mtu** *mtu-size* **Example:** `switch(config-if)# mtu 9216`	Configures an MTU size to support jumbo traffic. It should be configured on all host and fabric interfaces.
Step 9	**ip address** *ip-prefix* **Example:** `switch(config-if)# ip address 10.3.10.1/24`	Configures an IP address for this interface.

	Command or Action	Purpose
Step 10	**ip ospf passive-interface** **Example:** `switch(config-if)# ip ospf passive-interface`	Suppresses routing updates on the interface. This command overrides the router or VRF command mode configuration. OSPF runs passive on host-facing interfaces only. This configuration is needed only on endpoint interfaces and is not needed on fabric interfaces.
Step 11	**ip router ospf** *instance-tag* **area** *area-id* **Example:** `switch(config-if)# ip router ospf p1 area 0.0.0.0`	Enables OSPF on the interface.
Step 12	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on the interface.
Step 13	**ip igmp version** *number* **Example:** `switch(config-if)# ip igmp version 3`	Enables IGMPv3 packet support on endpoint interfaces only.
Step 14	**ip igmp immediate-leave** **Example:** `switch(config-if)# ip igmp immediate-leave`	Configures IGMP immediate leave on endpoint interfaces only.
Step 15	**ip pim pre-build-spt force** **Example:** `switch(config)# ip pim pre-build-spt force`	Prebuilds the shortest path tree (SPT) for all known (S,G) routes in the routing table by triggering PIM joins upstream. **Note** Enter this command only on spine switches. **Note** For Cisco NX-OS Releases 9.2(1) and 9.2(2), this command is needed so the PIM rendezvous point (RP) can pull traffic from the source leaf. Beginning with Cisco NX-OS Release 9.2(3), this command is not needed because the functionality is implemented using another internal mechanism.

Step 16	Configure an RP interface.
	Example:
	`switch(config)# interface loopback0`
	`  ip address 1.2.1.1/32`
	`  ip router ospf p1 area 0.0.0.0`
	`  ip pim sparse-mode`
		Make sure that the RP interface IP address is the same on each spine switch.
		Note Enter this configuration only on spine switches.

Configuring MSDP on Spine Switches

Follow these steps to configure MSDP for spine switches in a spine-leaf topology.

Note MSDP is only needed in a multi-spine deployment that uses an ASM range. In a single-spine deployment, MSDP is not needed.

Before you begin

Enable the MSDP feature (using the **feature msdp** command).

SUMMARY STEPS

1. **configure terminal**
2. Configure a loopback interface to establish an MSDP session between the spine switches.
3. **ip msdp originator-id** *interface*
4. **ip msdp peer** *peer-ip-address* **connect-source** *interface*
5. **ip msdp sa-policy** *peer-ip-address policy-name* **out**
6. **route-map** *policy-name* **permit** *sequence-number*
7. **match ip multicast group** *policy-name* **permit** *sequence-number*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	Configure a loopback interface to establish an MSDP session between the spine switches.
	Example:
	`interface loopback1`
	`  ip address 2.2.3.3/32`
	`  ip router ospf p1 area 0.0.0.0`
	`  ip pim sparse-mode`
		Establishes an MSDP session between the spine switches.

Step 3	**ip msdp originator-id** *interface* **Example:** `switch(config)# ip msdp originator-id loopback1`	Configures the IP address used in the RP field of a Source-Active (SA) message entry.
Step 4	**ip msdp peer** *peer-ip-address* **connect-source** *interface* **Example:** `switch(config)# ip msdp peer 2.2.1.1 connect-source loopback1`	Configures an MSDP peer with the specified peer IP address.
Step 5	**ip msdp sa-policy** *peer-ip-address policy-name* **out** **Example:** `switch(config)# ip msdp sa-policy 2.2.1.1 msdp-mcast-all out`	Enables a route-map policy for outgoing SA messages. By default, all registered sources are sent in SA messages.

	Command or Action	Purpose

Step 6	**route-map** *policy-name* **permit** *sequence-number*
	Example:
	`switch(config)# route-map msdp-mcast-all permit 10`
	`switch(config-route-map)#`
		Enters route-map configuration mode.

Step 7	**match ip multicast group** *policy-name* **permit** *sequence-number* **Example:** `switch(config-route-map)# match ip multicast group 224.0.0.0/8`	Matches the group specified. Make sure that the route-map group address matches the NBM flow ASM range group address.

Configuring Fabric and Host Interfaces

You can configure the fabric and host interfaces using the CLI commands in this section or use the DCNM Media Controller to autoprovision these configurations.

Note We recommend using a Layer 3 routed port to an endpoint.

Configuring a Fabric Interface

You must configure the fabric interface on each leaf switch. This interface goes from the leaf switch to the spine switch.

Note If you want to be able to exchange media flows between an IP fabric for media and external systems make sure to configure the **ip pim sparse-mode** command on the WAN links.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. **ip address** *ip-prefix*/*length*
4. **ip router ospf** *instance-tag* **area** *area-id*
5. **ip pim sparse-mode**
6. **no shutdown**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 1/49`
	`switch(config-if)#`
		Specifies the fabric interface and enters interface configuration mode.

Step 3	**ip address** *ip-prefix/length* **Example:** `switch(config-if)# ip address 1.1.1.0/31`	Assigns an IP address and subnet mask to this interface.
Step 4	**ip router ospf** *instance-tag* **area** *area-id* **Example:** `switch(config-if)# ip router ospf 100 area 0.0.0.0`	Adds the interface to the OSPFv2 instance and area.
Step 5	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on this interface.
Step 6	**no shutdown** **Example:** `switch(config-if)# no shutdown`	Enables the interface.

Configuring a Layer 3 Host Interface

You must configure the Layer 3 routed host interface on each leaf switch. This interface goes from the leaf switch to an endpoint.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **ip igmp version 3**
4. **ip address** *ip-prefix/length*
5. **ip router ospf** *instance-tag* **area** *area-id*
6. **ip pim sparse-mode**
7. **ip ospf passive-interface**
8. **ip igmp immediate-leave**
9. **no shutdown**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		Specifies the host interface and enters interface configuration mode.

Step 3	**ip igmp version 3** **Example:** `switch(config-if)# ip igmp version 3`	Sets the IGMP version to 3.
Step 4	**ip address** *ip-prefix/length* **Example:** `switch(config-if)# ip address 100.1.1.1/24`	Assigns an IP address and subnet mask to this interface.
Step 5	**ip router ospf** *instance-tag* **area** *area-id* **Example:** `switch(config-if)# ip router ospf 100 area 0.0.0.0`	Adds the interface to the OSPFv2 instance and area.
Step 6	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on this interface.
Step 7	**ip ospf passive-interface** **Example:** `switch(config-if)# ip ospf passive-interface`	Suppresses routing updates on the interface. This command overrides the router or VRF command mode configuration. OSPF runs passive on host-facing interfaces only. This configuration is needed only on endpoint interfaces and is not needed on fabric interfaces.
Step 8	**ip igmp immediate-leave** **Example:** `switch(config-if)# ip igmp immediate-leave`	Enables the switch to remove the group entry from the multicast routing table immediately upon receiving a leave message for the group.
Step 9	**no shutdown** **Example:** `switch(config-if)# no shutdown`	Enables the interface.

Configuring a Layer 2 with SVI Host Interface

You must configure the Layer 2 with SVI host interface on each leaf switch. This interface goes from the leaf switch to an endpoint.

SUMMARY STEPS

1. **configure terminal**
2. **feature interface-vlan**
3. **vlan** *vlan-id*
4. **exit**

5. **vlan configuration** *vlan-id*
6. **ip igmp snooping**
7. **ip igmp snooping fast-leave**
8. **exit**
9. **interface vlan** *vlan-id*
10. (Optional) **ip igmp version 3**
11. **ip router ospf** *instance-tag* **area** *area-id*
12. **ip address** *ip-address*
13. **ip pim sparse-mode**
14. **ip pim passive**
15. **ip igmp suppress v3-gsq**
16. **no shutdown**
17. **exit**
18. **interface ethernet** *port/slot*
19. **switchport**
20. **switchport mode** {**access** | **trunk**}
21. **switchport** {**access** | **trunk allowed**} **vlan** *vlan-id*
22. **no shutdown**
23. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**feature interface-vlan** **Example:** `switch(config)# feature interface-vlan`	Enables the creation of VLAN interfaces.

Step 3	**vlan** *vlan-id*
	Example:
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
		Creates a VLAN. The range is from 2 to 3967. VLAN 1 is the default VLAN and cannot be created or deleted. For more information on VLANs, see the Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide.

Step 4	**exit**
	Example:
	`switch(config-vlan)# exit`
	`switch(config)#`
		Exits the VLAN mode.

Step 5	**vlan configuration** *vlan-id*
	Example:
	`switch(config)# vlan configuration 5`
	`switch(config-vlan-config)#`
		Allows you to configure VLANs without actually creating them.

	Command or Action	Purpose
Step 6	**ip igmp snooping** **Example:** `switch(config-vlan-config)# ip igmp snooping`	Enables IGMP snooping on the device for the specific VLAN. For more information on IGMP snooping, see the Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide.
Step 7	**ip igmp snooping fast-leave** **Example:** `switch(config-vlan-config)# ip igmp snooping fast-leave`	Supports IGMPv2 hosts that cannot be explicitly tracked because of the host report suppression mechanism of the IGMPv2 protocol. When you enable fast leave, the IGMP software assumes that not more than one host is present on each VLAN port. The default is disabled for all VLANs.

Step 8	**exit**
	Example:
	`switch(config-vlan-config)# exit`
	`switch(config)#`
		Exits VLAN configuration mode.

Step 9	**interface vlan** *vlan-id*
	Example:
	`switch(config)# interface vlan 5`
	`switch(config-if)#`
		Creates a VLAN interface and enters interface configuration mode. The range is from 2 and 3967.

Step 10	(Optional) **ip igmp version 3** **Example:** `switch(config-if)# ip igmp version 3`	Sets the IGMP version to 3. Enter this command if you are using IGMP version 3.
Step 11	**ip router ospf** *instance-tag* **area** *area-id* **Example:** `switch(config-if)# ip router ospf 201 area 0.0.0.15`	Adds the interface to the OSPFv2 instance and area.
Step 12	**ip address** *ip-address* **Example:** `switch(config-if)# ip address 192.0.2.1/8`	Configures an IP address for this interface.
Step 13	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on this interface. For more information on PIM, see the Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide.
Step 14	**ip pim passive** **Example:** `switch(config-if)# ip pim passive`	Prevents the device from sending PIM messages on the interface or accepting PIM messages from other devices across this interface. The device instead considers that it is the only PIM device on the network and acts as the designated router and designated forwarder for all Bidir PIM group ranges.
Step 15	**ip igmp suppress v3-gsq** **Example:**	Prevents the router from generating a query when it receives an IGMPv3 leave report.

	Command or Action	Purpose
	`switch(config-if)# ip igmp suppress v3-gsq`	
Step 16	**no shutdown** **Example:** `switch(config-if)# no shutdown`	Clears the errors on the interfaces and VLANs where policies correspond with hardware policies. This command allows policy programming to continue and the port to come up. **Note** Apply this command only after you have entered the previous multicast commands.

Step 17	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits the VLAN interface configuration mode.

Step 18	**interface ethernet** *port/slot* **Example:** `switch(config-if)# interface ethernet 2/1`	Configures an Ethernet interface.
Step 19	**switchport** **Example:** `switch(config-if)# switchport`	Sets the interface as a Layer 2 interface.
Step 20	**switchport mode** {**access** | **trunk**} **Example:** `switch(config-if)# switchport mode trunk`	Configures one of the following options: **access**—Sets the interface as a nontrunking, nontagged, single-VLAN Layer 2 interface. An access port can carry traffic in one VLAN only. By default, an access port carries traffic for VLAN 1. **trunk**—Sets the interface as a Layer 2 trunk port. A trunk port can carry traffic in one or more VLANs on the same physical link. (VLANs are based on the trunk-allowed VLANs list.) By default, a trunk interface can carry traffic for all VLANs.
Step 21	**switchport** {**access** | **trunk allowed**} **vlan** *vlan-id* **Example:** `switch(config-if)# switchport trunk allowed vlan 5`	Configures one of the following options: **access**—Specifies the VLAN for which this access port will carry traffic. If you do not enter this command, the access port carries traffic on VLAN 1 only. **trunk allowed**—Specifies the allowed VLANs for the trunk interface. The default is to allow all VLANs on the trunk interface: 1 to 3967 and 4048 to 4094. VLANs 3968 to 4047 are the default VLANs reserved for internal use by default.
Step 22	**no shutdown** **Example:** `switch(config-if)# no shutdown`	Clears the errors on the interfaces and VLANs where policies correspond with hardware policies. This command allows policy programming to continue and the port to come up.

	Command or Action	Purpose

Step 23	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		Exits the interface configuration mode.

Configuring NBM for a Single Modular Switch

After you have set up the IP fabric, you must enable the NBM feature on the switch. The NBM feature ensures that the bandwidth that is coming into the fabric is exactly the same as the bandwidth that is going out.

Follow this procedure to configure NBM for a single modular switch.

Before you begin

Enable the PIM feature (using the **feature pim** command).

Enable the OSPF feature (using the **feature ospf** command), if you are using the OSPF unicast routing protocol.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **feature nbm**
3. [**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**}
4. (Optional) [**no**] **nbm flow policer**
5. [**no**] **nbm flow-policy**
6. [**no**] **policy** *policy-name*
7. (Optional) [**no**] **policer**
8. [**no**] **bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**}
9. [**no**] **ip group** *ip-address*
10. [**no**] **ip group-range** *ip-address* **to** *ip-address*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **feature nbm** **Example:** `switch(config)# feature nbm`	Enables the NBM feature. The **no** form of this command disables this feature.
Step 3	[**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} **Example:**	Configures the global NBM flow bandwidth in Kbps, Mbps, or Gbps. The minimum supported flow bandwidth is 200 Kbps.

	Command or Action	Purpose
	`switch(config)# nbm flow bandwidth 150 mbps`	<table><tr><th>Range</th><th>Default Value</th></tr><tr><td>1 to 25,000,000 Kbps</td><td>0 Kbps</td></tr><tr><td>1 to 25,000 Mbps</td><td>0 Mbps</td></tr><tr><td>1 to 25 Gbps</td><td>0 Gbps</td></tr></table>
Step 4	(Optional) [**no**] **nbm flow policer** **Example:** `switch(config)# no nbm flow policer`	Enables or disables the policer for all NBM flow policies. The policer is enabled by default. **Note** This command is available beginning with Cisco NX-OS Release 9.2(3).

Step 5	[**no**] **nbm flow-policy**
	Example:
	`switch(config)# nbm flow-policy`
	`switch(config-nbm-flow-pol)#`
		Configures the flow bandwidth per flow.

Step 6	[**no**] **policy** *policy-name*
	Example:
	`switch(config-nbm-flow-pol)# policy 1.5gbps`
	`switch(config-nbm-flow-pol-attr)#`
		Configures the NBM flow policy. You can specify a maximum of 63 alphanumeric characters for the policy name.

Step 7	(Optional) [**no**] **policer** **Example:** `switch(config-nbm-flow-pol-attr)# no policer`	Enables or disables the policer for the specified NBM flow policy. By default, each source flow uses a policer on the source leaf (the first hop router). In a scenario where the number of multicast source flows exceeds the number of policers, the flow is not accepted by the source leaf. To override this behavior, you can disable the policer under the flow policy. For flows that match the flow policy where the policer is disabled, no policer resource is consumed. **Note** Use this command with caution as it could lead to an unprotected network, where a misbehaving endpoint could transmit more than what it is allowed. Use another method, such as an aggregate policer, to rate limit flows that have no policer programmed by NBM. For information on configuring an aggregate policer, see Configuring Shared Policers. **Note** This command is available beginning with Cisco NX-OS Release 9.2(3).

	Command or Action	Purpose
Step 8	[**no**] **bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} **Example:** `switch(config-nbm-flow-pol-attr)# bandwidth 1500 mbps`	Configures the flow bandwidth in Kbps, Mbps, or Gbps for multicast groups matching this policy. The minimum supported flow bandwidth is 200 Kbps. **Range** / **Default Value**: 1 to 25,000,000 Kbps / 0 Kbps 1 to 25,000 Mbps / 0 Mbps 1 to 25 Gbps / 0 Gbps

Step 9	[**no**] **ip group** *ip-address*
	Example:
	`switch(config-nbm-flow-pol-attr)# ip group 228.0.0.15`
	`switch(config-nbm-flow-pol-attr)# ip group 228.0.255.15`
		Specifies the IP address for /32 multicast groups.

Step 10	[**no**] **ip group-range** *ip-address* **to** *ip-address*
	Example:
	`switch(config-nbm-flow-pol-attr)# ip group-range 239.255.255.121 to 239.255.255.130`
	`switch(config-nbm-flow-pol-attr)# ip group-range 239.255.255.131 to 239.255.255.140`
	`switch(config-nbm-flow-pol-attr)# ip group-range 239.255.255.141 to 239.255.255.150`
	`switch(config-nbm-flow-pol-attr)# ip group-range 239.255.255.151 to 239.255.255.160`
		Specifies the IP address range for multicast groups associated to this policy.

Example

The following example shows a sample configuration:

```
nbm flow-policy
  policy Audio
    bandwidth 2 mbps
    ip group-range 225.3.5.2 to 225.3.5.255
  policy Video
    bandwidth 3000 mbps
    ip group-range 228.255.255.1 to 228.255.255.255
```

What to do next

Establishing a Flow (Optional)

Establishing a Flow (Optional)

You can establish a flow by creating an NBM flow definition or configuring IGMP static OIF. We recommend configuring an NBM flow definition for Cisco NX-OS Release 9.2(3) and later releases.

Creating an NBM Flow Definition

Beginning with Cisco NX-OS Release 9.2(3), you can establish an NBM flow by creating an NBM flow definition.

NBM exposes a CLI and an API to provision flows to receivers when they do not use IGMP to signal their interest in joining or leaving a flow. As shown in the following diagrams, you can program a flow to go all the way to the receiver leaf, in order to pre-reserve the network bandwidth, or direct the leaf switch to send the traffic to the receiver by specifying the egress interface.

Figure 1: Traffic from a Source to a Leaf

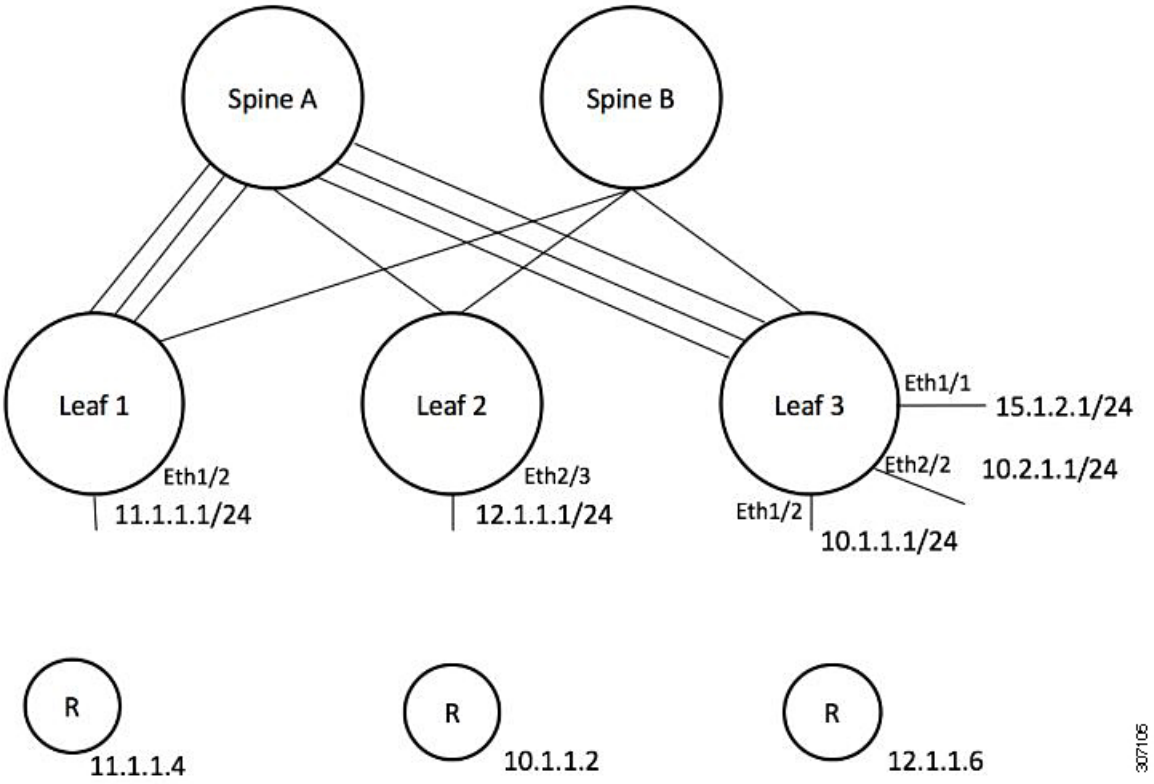
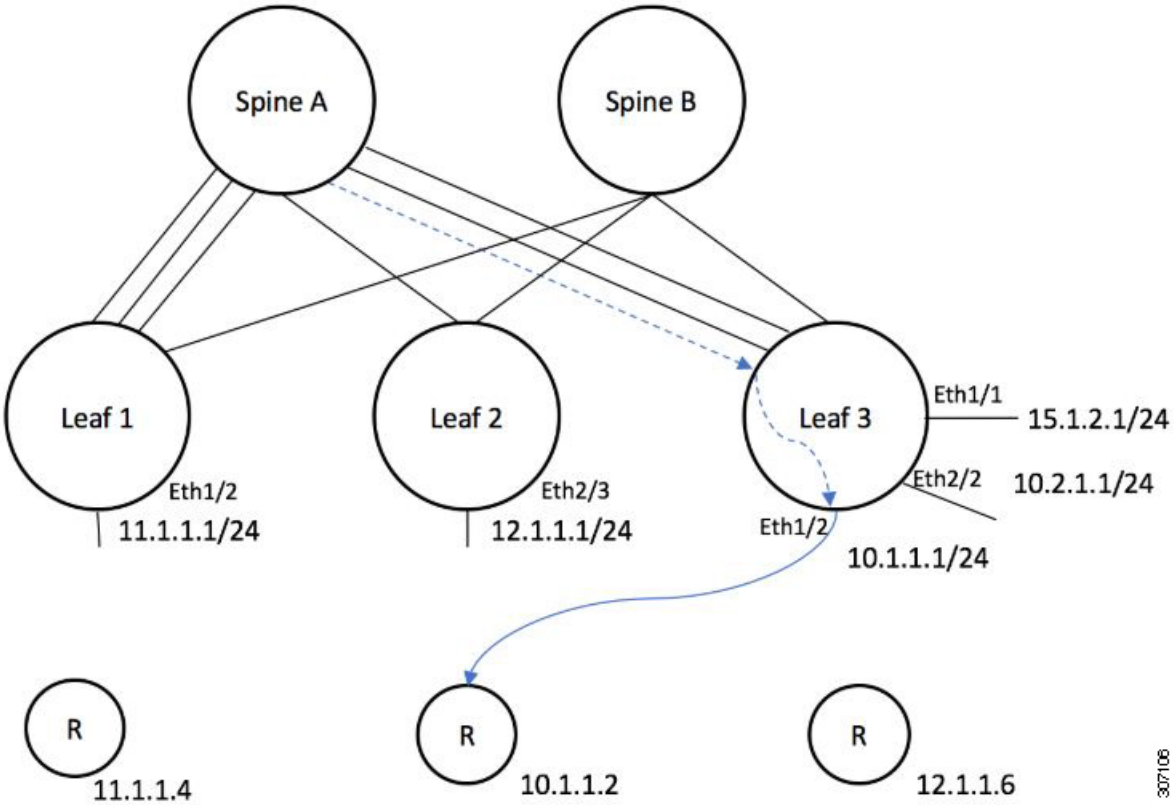


Figure 2: Traffic from the Leaf to a Receiver



Before you begin

Enable NBM.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **nbm flow-definition** *group* [*source*]
3. (Optional) [**no**] **stage-flow**
4. (Optional) [**no**] **egress-interface** *interface*
5. (Optional) [**no**] **egress-host** *reporter-ip-address*

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

	Command or Action	Purpose

Step 2	[**no**] **nbm flow-definition** *group* [*source*]
	Example:
	`switch(config)# nbm flow-definition 235.1.1.13 100.1.1.40`
	`switch(config-nbm-flow-def)#`
	Example:
	`switch(config)# nbm flow-definition 235.1.1.10 0.0.0.0`
	`switch(config-nbm-flow-def)#`
		Configures the NBM flow definition.

Step 3	(Optional) [**no**] **stage-flow** **Example:** `switch(config-nbm-flow-def)# stage-flow`	Brings the flow all the way from the source to the switch.
Step 4	(Optional) [**no**] **egress-interface** *interface* **Example:** `switch(config-nbm-flow-def)# egress-interface ethernet 1/3`	Forwards the flow out of the specified interface.
Step 5	(Optional) [**no**] **egress-host** *reporter-ip-address* **Example:** `switch(config-nbm-flow-def)# egress-host 10.10.10.1`	Forwards the flow to the specified receiver.

Example

The following example shows a sample configuration:

```
nbm flow-definition 225.0.0.16 11.1.1.40
  stage-flow
  egress-interface ethernet 1/3
  egress-host 145.1.1.23
  egress-host 145.1.1.22
  egress-host 145.1.1.24
  egress-host 145.1.1.25
  egress-host 145.1.1.26
  egress-host 145.1.1.27
  egress-host 145.1.1.28
  egress-host 145.1.1.29
nbm flow-definition 225.0.0.11 100.1.1.40
  stage-flow
  egress-interface ethernet 1/4
  egress-host 100.1.1.21
nbm flow-definition 235.1.1.13 100.1.1.40
  stage-flow
  egress-interface vlan 12
  egress-host 101.1.1.11
  egress-host 101.1.1.12
  egress-host 101.1.1.13
  egress-host 101.1.1.14
```

Configuring IGMP Static OIF

For Cisco NX-OS Releases 9.2(1) and 9.2(2), you can establish a flow only by configuring a static IGMP OIF. For Cisco NX-OS Release 9.2(3), we recommend that you create an NBM flow definition rather than configuring static IGMP OIF.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. [**no**] **ip igmp static-oif** *group* [**source** *source*]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface** *interface-type slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Specifies an interface to configure and enters interface configuration mode.

Step 3	[**no**] **ip igmp static-oif** *group* [**source** *source*] **Example:** `switch(config-if)# ip igmp static-oif 230.0.0.0`	Establishes a flow for the specified multicast group. **Note** This command does not support the **route-map** option. **Note** If the switch is running Cisco NX-OS Release 9.2(1) and the flow setup fails due to insufficient bandwidth in the fabric, you must remove and re-add this command once bandwidth is available to re-establish the flow. For later releases, you do not need to remove and re-add this command as the switch automatically tries again to set up the flow.

Configuring Multisite

IP fabric for media provides a reliable channel of communication between multiple sites, where the sender is in one site and receivers are in another site. You can configure some external (or host-side) interfaces as external links and attach external devices to those links to create a multisite solution. By configuring some interfaces as external links, the solution can perform bandwidth management on those interfaces. Switches running in PIM active mode manage the fabric bandwidth through a distributed bandwidth management algorithm running on all switches.

Before you begin

Configure NBM for a spine-leaf topology or a single modular switch.

To support ASM flows across the sites, full mesh MSDP must be enabled between the RPs between the sites. For configuration information, see Configuring MSDP on Spine Switches.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **feature nbm**
3. **ip pim sparse mode**
4. **interface** *interface-type slot/port*
5. **nbm external-link**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **feature nbm** **Example:** `switch(config)# feature nbm`	Enables the NBM feature. The **no** form of this command disables this feature.
Step 3	**ip pim sparse mode** **Example:** `switch(config)# ip pim sparse mode`	Configures PIM on the NBM external link.

Step 4	**interface** *interface-type slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Specifies an interface to configure and enters interface configuration mode.

Step 5	**nbm external-link** **Example:** `switch(config-if)# nbm external-link`	Configures the NBM interface as an external link in order to connect multiple fabrics together in a multisite solution.

Enabling Multicast and Unicast Flows (Optional)

IP fabric for media can be used for multicast as well as unicast flows. You can assign multicast traffic to a priority queue (7) and unicast traffic to the default queue (0). This configuration ensures that unicast traffic does not congest multicast traffic.

Note For spine switches, traffic classification is based on access control list (ACL) and Differentiated Services Code Point (DSCP) values. For sender leaf switches, classification and marking are based on flow programming (S,G) from the DCNM Media Controller.

Before you begin

Configure TCAM carving on all switches (excluding the Cisco Nexus 9504 and 9508 switches with -R line cards) using the following commands, save the configuration, and reload the switch:

- **hardware access-list tcam region ing-racl 256**
- **hardware access-list tcam region ing-l3-vlan-qos 256**
- **hardware access-list tcam region ing-nbm 1536**

Note We recommend the TCAM sizes shown above, but you can adjust the values to meet your network requirements. For more information on ACL TCAM regions, see the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

SUMMARY STEPS

1. **configure terminal**
2. **ip access-list** *acl-name*
3. *sequence-number* **permit** *protocol source destination*
4. **exit**
5. **ip access-list** *acl-name*
6. *sequence-number* **permit** *protocol source destination*
7. **exit**
8. **class-map type qos match-all** *unicast-class-name*
9. **match access-group name** *acl-name*
10. **exit**
11. **class-map type qos match-any** *multicast-class-name*
12. **match access-group name** *acl-name*
13. **exit**
14. **policy-map type qos** *policy-map-name*
15. **class** *unicast-class-map-name*
16. **set qos-group 0**
17. **exit**
18. **class** *multicast-class-map-name*
19. **set qos-group 7**
20. **exit**
21. **exit**
22. **interface ethernet** *slot/port*
23. **service-policy type qos input** *policy-map-name*

24. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**ip access-list** *acl-name*
	Example:
	`switch(config)# ip access-list pmn-ucast`
	`switch(config-acl)#`
		Creates an IP ACL and enters IP ACL configuration mode.

Step 3	*sequence-number* **permit** *protocol source destination*
	Example:
	`switch(config-acl)# 10 permit ip any 0.0.0.0/1`
	`switch(config-acl)# 20 permit ip any 128.0.0.0/2`
	`switch(config-acl)# 30 permit ip any 192.0.0.0/3`
		Creates a rule in the IP ACL to match all unicast IP addresses (Class A, B, and C).

Step 4	**exit**
	Example:
	`switch(config-acl)# exit`
	`switch(config)#`
		Exits IP ACL configuration mode.

Step 5	**ip access-list** *acl-name*
	Example:
	`switch(config)# ip access-list pmn-mcast`
	`switch(config-acl)#`
		Creates an IP ACL and enters IP ACL configuration mode.

Step 6	*sequence-number* **permit** *protocol source destination* **Example:** `switch(config-acl)# 2 permit ip any 224.0.0.0/4`	Creates a rule to match all multicast flows.

Step 7	**exit**
	Example:
	`switch(config-acl)# exit`
	`switch(config)#`
		Exits IP ACL configuration mode.

Step 8	**class-map type qos match-all** *unicast-class-name*
	Example:
	`switch(config)# class-map type qos match-all pmn-ucast`
	`switch(config-cmap-qos)#`
		Creates a class map for unicast traffic and enters class-map configuration mode.

Step 9	**match access-group name** *acl-name* **Example:**	Configures the traffic class by matching packets based on the ACL for unicast traffic.

	Command or Action	Purpose
	`switch(config-cmap-qos)# match access-group name pmn-ucast`	

Step 10	**exit**
	Example:
	`switch(config-cmap-qos)# exit`
	`switch(config)#`
		Exits class-map configuration mode.

Step 11	**class-map type qos match-any** *multicast-class-name*
	Example:
	`switch(config)# class-map type qos match-any pmn-mcast`
	`switch(config-cmap-qos)#`
		Creates a class map for multicast traffic and enters class-map configuration mode.

Step 12	**match access-group name** *acl-name* **Example:** `switch(config-cmap-qos)# match access-group name pmn-mcast`	Configures the traffic class by matching packets based on the ACL for multicast traffic.

Step 13	**exit**
	Example:
	`switch(config-cmap-qos)# exit`
	`switch(config)#`
		Exits class-map configuration mode.

Step 14	**policy-map type qos** *policy-map-name*
	Example:
	`switch(config)# policy-map type qos pmn-qos`
	`switch(config-pmap-qos)#`
		Creates a policy map and enters policy-map configuration mode.

Step 15	**class** *unicast-class-map-name*
	Example:
	`switch(config-pmap-qos)# class pmn-ucast`
	`switch(config-pmap-c-qos)#`
		Creates a class for unicast traffic and enters policy-map class configuration mode.

Step 16	**set qos-group 0** **Example:** `switch(config-pmap-c-qos)# set qos-group 0`	Configures the QoS group value to match on for classification of traffic into the PMN unicast class map.

Step 17	**exit**
	Example:
	`switch(config-pmap-c-qos)# exit`
	`switch(config-pmap-qos)#`
		Exits policy-map class configuration mode.

Step 18	**class** *multicast-class-map-name*
	Example:
	`switch(config-pmap-qos)# class pmn-mcast`
	`switch(config-pmap-c-qos)#`
		Creates a class for multicast traffic and enters policy-map class configuration mode.

	Command or Action	Purpose
Step 19	**set qos-group 7** **Example:** `switch(config-pmap-c-qos)# set qos-group 7`	Configures the QoS group value to match on for classification of traffic into the PMN multicast class map.

Step 20	**exit**
	Example:
	`switch(config-pmap-c-qos)# exit`
	`switch(config-pmap-qos)#`
		Exits policy-map class configuration mode.

Step 21	**exit**
	Example:
	`switch(config-pmap-qos)# exit`
	`switch(config)#`
		Exits policy-map configuration mode.

Step 22	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 1/49`
	`switch(config-if)#`
		Creates an interface and enters interface configuration mode. This command should be used only for fabric interfaces.

Step 23	**service-policy type qos input** *policy-map-name* **Example:** `switch(config-if)# service-policy type qos input pmn-qos`	Adds the policy-map name to the input packets of the interface.
Step 24	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Example

Configuration example:

```
ip access-list pmn-ucast
  10 permit ip any 0.0.0.0 31.255.255.255
  20 permit ip any 128.0.0.0 31.255.255.255
  30 permit ip any 192.0.0.0 31.255.255.255

ip access-list pmn-mcast
  10 permit ip any 224.0.0.0/4

class-map type qos match-all pmn-ucast
  match access-group name pmn-ucast
class-map type qos match-any pmn-mcast
  match access-group name pmn-ucast

policy-map type qos pmn-qos
  class pmn-ucast
    set qos-group 0
  class pmn-mcast
    set qos-group 7
```

```
interface ethernet 1/49
  service-policy type qos input pmn-qos
```

Verifying the NBM Configuration

To display the NBM configuration information, perform one of the following tasks.

show nbm defaults	Displays the NBM default flow policy, host policies, and unicast fabric bandwidth.
show nbm flow-policy [*policy-name*]	Displays the multicast range, bandwidth, DSCP, and QoS for all configured custom flow policies or for a specific custom flow policy.
show nbm flows [**active** [**interface** *type slot/port*] | **all** [**interface** *type slot/port*] | **detail** [**interface** *type slot/port*] | **group** *multicast-group* | **group-based** [**interface** *type slot/port*] | **inactive** [**interface** *type slot/port*] | **interface** *type slot/port* | **no-receiver** [**interface** *type slot/port*] |**source** *ip-address*]	Displays the active flows on the switch for all default and custom flow policies. Optional keywords can be added to narrow the output.
show nbm flows static	Displays the static flows for an NBM flow definition.
show nbm flows statistics	Displays the NBM flow statistics. This command is valid on the first hop router where the senders are connected or on the switch where flows enter the fabric. **Note** This command is not supported for spine switches in a spine-leaf topology and for single modular switches with -R line cards.
show nbm host-policy {**all** {**receiver external** | **receiver local** | **sender**} | **applied** {**receiver external** | **receiver local** {**all** | **interface** *type slot/port*} | **sender** {**all** | **interface** *type slot/port*}}}	Displays all NBM host policies or applied NBM host policies for external receivers (PIM), local receivers, or senders.
show nbm interface bandwidth	Displays the NBM interface bandwidth.
show running-config nbm	Displays the running configuration information for NBM.

The following example shows sample output for the **show nbm flows static** command:

```
switch# show nbm flows static
+-----------------------------------------------------------------------+
|   Stitched Flows                                                      |
+-----------------------------------------------------------------------+
| Source          | Group           | Egress Intf     | Host IP         |
+-----------------------------------------------------------------------+
| 10.102.13.11    | 225.0.0.11      |                 |                 |
|                 |                 | Ethernet1/35    |                 |
+-----------------------------------------------------------------------+
+-----------------------------------------------------------------------+
|   Unstitched Flows                                                    |
+-----------------------------------------------------------------------+
| Source          | Group           | Egress Intf     | Host IP         |
+-----------------------------------------------------------------------+
| 10.102.13.11    | 225.0.0.11      |                 |                 |
|                 |                 | eth1/3          |                 |
|                 |                 |                 | 101.1.1.15      |
| 10.102.13.12    | 225.0.0.11      |                 |                 |
|                 |                 | eth1/3          |                 |
|                 |                 |                 | 10.10.10.10     |
+-----------------------------------------------------------------------+
+-----------------------------------------------------------------------+
```

Sample Output for Show Commands

This section provides output examples for single modular switches without the DCNM Media Controller. In controller-based deployments, statistics are available in the DCNM Media Controller GUI.

Sample Show Command Output

This example shows sample output for the **show nbm defaults** command:

```
switch# show nbm defaults
Default Flow Policy:
Bandwidth : 1000 Kbps
DSCP      : 0
QID       : 0

Default Host Policies:
Sender    : Permit
Receiver  : Permit
PIM       : Permit

Default Unicast Fabric Bandwidth : 1
```

This example shows sample output for the **show nbm flows** command:

```
switch# show nbm flows
NBM Active Source-Group-Based Flows :
Mcast-Group Src-IP Start-Time Src-Intf L4-S L4-D LID Status Num Rx Bw Mbps CFG Bw Mbps
Src-slot Unit Slice DSCP QOS
228.2.10.3 10.12.85.10 08/21 18:45:27.429 Vlan1000 0 0 0 ACTIVE 7 66.000 66.000 1 0 0 48 7

228.1.3.3 10.10.85.10 08/21 18:45:27.324 Vlan1000 0 0 0 ACTIVE 8 18.000 18.000 1 0 0 24 7
228.1.4.1 10.10.85.10 08/21 18:45:27.068 Vlan1000 0 0 0 ACTIVE 8 19.000 19.000 1 0 0 32 7
228.1.9.1 10.10.85.10 08/21 18:45:26.732 Vlan1000 0 0 0 ACTIVE 8 31.000 31.000 1 0 0 32 7
```

This example shows sample output for the **show nbm flows group** *multicast-group* command:

```
switch# show nbm flows group 228.2.10.3
NBM Active Source-Group-Based Flows :
```

```
Mcast-Group Src-IP Start-Time Src-Intf L4-S L4-D LID Status Num Rx Bw Mbps CFG Bw Mbps
Src-slot Unit Slice DSCP QOS
228.2.10.3 10.12.85.10 08/21 18:45:27.429 Vlan1000 0 0 0 ACTIVE 7 66.000 66.000 1 0 0 48 7
```

This example shows sample output for the **show ip igmp groups** command:

```
switch# show ip igmp groups
IGMP Connected Group Membership for VRF "default" - 61520 total entries
Type: S - Static, D - Dynamic, L - Local, T - SSM Translated
Group Address      Type Interface           Uptime    Expires   Last Reporter
225.3.5.1          D    Ethernet3/5         11:48:07  00:03:36  3.5.1.6
225.3.5.2          D    Ethernet3/5         11:48:07  00:03:36  3.5.1.6
225.3.5.3          D    Ethernet3/5         11:48:07  00:03:36  3.5.1.6
225.3.5.4          D    Ethernet3/5         11:48:07  00:03:36  3.5.1.6
```

This example shows sample output for the **show ip igmp groups** *interface* command:

```
switch# show ip igmp groups eth3/5
IGMP Connected Group Membership for Interface "Eth3/5" - 1165 total entries
Type: S - Static, D - Dynamic, L - Local, T - SSM Translated
Group Address      Type Interface      Uptime    Expires   Last Reporter
225.3.5.1          D    Ethernet3/5    11:51:22  00:02:24  3.5.1.6
225.3.5.2          D    Ethernet3/5    11:51:22  00:02:24  3.5.1.6
225.3.5.3          D    Ethernet3/5    11:51:22  00:02:24  3.5.1.6
225.3.5.4          D    Ethernet3/5    11:51:22  00:02:24  3.5.1.6
```

This example shows sample output for the **show ip igmp groups** *multicast-group* command:

```
switch# show ip igmp groups 225.3.5.1
IGMP Connected Group Membership for VRF "default" - matching Group "225.3.5.1"
Type: S - Static, D - Dynamic, L - Local, T - SSM Translated
Group Address  Type  Interface    Uptime    Expires   Last Reporter
225.3.5.1      D     Ethernet3/5  00:05:20  00:10:10  3.5.1.6
```

This example shows sample output for the **show running-config nbm** command:

```
switch# show running-config nbm
!Command: show running-config nbm
!Running configuration last done at: Thu May 10 08:53:37 2018
!Time: Thu May 10 09:33:23 2018

version 9.2(1) Bios:version 07.50
feature nbm

nbm mode pim-active
nbm host-policy
  sender
    default deny
  receiver
    default deny
    5 host 1.0.0.5 source 1.2.3.4 group 232.1.2.0/24 permit
    6 host 1.0.3.5 source 1.2.3.77 group 224.1.2.0/24 permit
    7 host 1.0.0.5 source 1.2.3.88 group 224.1.2.0/24 permit
  pim
    default deny
nbm reserve unicast fabric bandwidth 10
nbm flow asm range 237.1.1.0/24
nbm flow bandwidth 123 kbps
nbm flow-policy
  policy BLAH
  policy POL
  policy POL_1
```

```
    bandwidth 123 kbps
    dscp 10
    ip group-range 237.1.1.0 to 238.1.1.0
  policy POL_A
  policy flow
  policy nbm1_1
    bandwidth 1000000 kbps
    dscp 11
    ip group-range 224.1.0.1 to 224.1.255.255
    ip group-range 225.1.0.1 to 225.1.255.255
```

Configuring PTP for Media (Optional)

Cisco's IP fabric for media solution supports the following IEEE 1588 PTP profiles:

- Audio Engineering Society 67 profile (AES67) - For high-performance streaming audio over IP
- Professional Broadcast Environment profile (SMPTE-2059-2) - For high-performance streaming video over IP

The solution also introduces mixed mode PTP support with multicast sync and announce messages as well as unicast delay request and response messages.

To configure PTP for media, you should use one of these profiles.

Note The PTP configuration for media is different from the PTP configuration for a non-media network. However, you can refer to the Cisco Nexus 9000 Series NX-OS System Management Configuration Guide for more information on PTP.

Before you begin

Enable PTP boundary mode functionality on the switch. PTP packets cannot be routed as regular multicast packets within the fabric.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **feature ptp**
3. [**no**] **ptp source** *ip-address* [**vrf** *vrf*]
4. (Optional) [**no**] **ptp offload**
5. **interface ethernet** *slot/port*
6. [**no**] **ptp**
7. (Optional) [**no**] **ptp announce interval** [**aes67** | **smpte-2059**] *log-seconds*
8. (Optional) [**no**] **ptp announce timeout** [**aes67** | **smpte-2059**] *count*
9. (Optional) [**no**] **ptp delay-request minimum interval** [**aes67** | **smpte-2059**] *log-seconds*
10. (Optional) [**no**] **ptp sync interval** [**aes67** | **smpte-2059**] *log-seconds*
11. (Optional) [**no**] **ptp vlan** *vlan-id*
12. (Optional) **show ptp brief**

13. (Optional) **show ptp port interface** *interface slot/port*
14. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[**no**] **feature ptp** **Example:** `switch(config)# feature ptp`	Enables or disables PTP on the device. **Note** Enabling PTP on the switch does not enable PTP on each interface.
Step 3	[**no**] **ptp source** *ip-address* [**vrf** *vrf*] **Example:** `switch(config)# ptp source 10.10.10.1`	Configures the source IPv4 address for all PTP packets. We recommend that the source IP address be a valid IP address for any interface on the switch.
Step 4	(Optional) [**no**] **ptp offload** **Example:** `switch(config)# ptp offload`	Increases the number of PTP sessions by offloading some timers to the line card.

Step 5	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		Specifies the interface on which you are enabling PTP and enters the interface configuration mode.

Step 6	[**no**] **ptp** **Example:** `switch(config-if)# ptp`	Enables or disables PTP on an interface.
Step 7	(Optional) [**no**] **ptp announce interval** [**aes67** | **smpte-2059**] *log-seconds* **Example:** `switch(config-if)# ptp announce interval aes67 3`	Configures the interval between PTP announce messages on an interface. ***Table 4: PTP Announcement Interval Range and Default Values*** **Option** / **Range** / **Default Value** **aes67** / 0 to 4 log seconds / 1 log second **smpte-2059** / –3 to 1 log seconds / 1 log second Without the **aes67** or **smpte-2059** option / 0 to 4 log seconds / 1 log second

	Command or Action	Purpose
Step 8	(Optional) [**no**] **ptp announce timeout** [**aes67** | **smpte-2059**] *count* **Example:** `switch(config-if)# ptp announce timeout aes67 2`	Configures the number of PTP intervals before a timeout occurs on an interface. ***Table 5: PTP Announcement Timeout Range and Default Values*** **Option** / **Range** / **Default Value** **aes67** / 2 to 10 intervals / 3 intervals **smpte-2059** / 2 to 10 intervals / 3 intervals Without the **aes67** or **smpte-2059** option / 2 to 4 intervals / 3 intervals
Step 9	(Optional) [**no**] **ptp delay-request minimum interval** [**aes67** | **smpte-2059**] *log-seconds* **Example:** `switch(config-if)# ptp delay-request minimum interval aes67 -1`	Configures the minimum interval allowed between PTP delay messages when the port is in the primary state. ***Table 6: PTP Delay-Request Minimum Interval Range and Default Values*** **Option** / **Range** / **Default Value** **aes67** / –4 to 5 log seconds / 0 log seconds **smpte-2059** / –4 to 5 log seconds / 0 log seconds Without the **aes67** or **smpte-2059** option / –1 to 6 log seconds (where –1 = 1 frame per second) / 0 log seconds
Step 10	(Optional) [**no**] **ptp sync interval** [**aes67** | **smpte-2059**] *log-seconds* **Example:** `switch(config-if)# ptp sync interval aes67 1`	Configures the interval between PTP synchronization messages on an interface. ***Table 7: PTP Synchronization Interval Range and Default Values*** **Option** / **Range** / **Default Value** **aes67** / –4 to 1 log seconds / –2 log seconds **smpte-2059** / –4 to –1 log seconds / –2 log seconds Without the **aes67** or **smpte-2059** option / –3 to 1 log seconds / –2 log seconds

	Command or Action	Purpose
Step 11	(Optional) [**no**] **ptp vlan** *vlan-id* **Example:** `switch(config-if)# ptp vlan 1`	Specifies the VLAN for the interface where PTP is being enabled. You can enable PTP only on one VLAN on an interface. The range is from 1 to 4094.
Step 12	(Optional) **show ptp brief** **Example:** `switch(config-if)# show ptp brief`	Displays the PTP status.
Step 13	(Optional) **show ptp port interface** *interface slot/port* **Example:** `switch(config-if)# show ptp port interface ethernet 2/1`	Displays the status of the PTP port.
Step 14	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Configuring Unicast PTP Peers

You must configure both master and slave unicast PTP peers.

SUMMARY STEPS

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **ptp transport ipv4 ucast** {**master** | **slave**}
4. {**master** | **slave**} **ipv4** *ip-address*
5. **ptp ucast-source** *ip-address*
6. (Optional) **show ptp brief**
7. (Optional) **show ptp counters interface ethernet** *slot/port* **ipv4** *ip-address*
8. (Optional) **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**interface ethernet** *slot/port* **Example:**	Specifies the interface on which you are enabling unicast PTP and enters the interface configuration mode.

	Command or Action	Purpose
	`switch(config)# interface ethernet 1/1` `switch(config-if)#`	
Step 3	**ptp transport ipv4 ucast** {**master** | **slave**} **Example:** `switch(config-if)# ptp transport ipv4 ucast master`	Configures the master or slave unicast PTP peer.
Step 4	{**master** | **slave**} **ipv4** *ip-address* **Example:** `switch(config-if)# slave ipv4 81.0.0.2`	Specifies the IP address of the master or slave unicast PTP peer.
Step 5	**ptp ucast-source** *ip-address* **Example:** `switch(config-if)# ptp ucast-source 81.0.0.1`	Specifies the IP address of the PTP unicast source.
Step 6	(Optional) **show ptp brief** **Example:** `switch(config-if)# show ptp brief`	Displays the PTP status.
Step 7	(Optional) **show ptp counters interface ethernet** *slot/port* **ipv4** *ip-address* **Example:** `switch(config-if)# show ptp counters interface ethernet 1/1 ipv4 81.0.0.2`	Displays the unicast PTP counters.
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Example

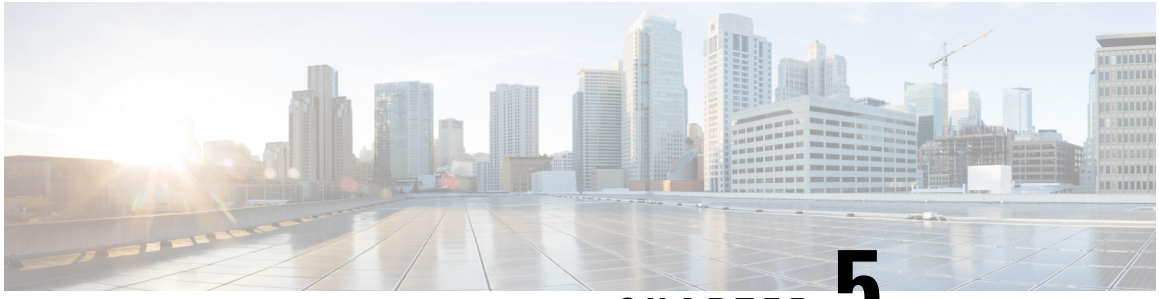
The following example shows how to configure master and slave unicast PTP peers:

```
interface Ethernet1/1
  ptp transport ipv4 ucast master
    slave ipv4 81.0.0.2
  ptp ucast-source 81.0.0.1
  ip address 81.0.0.1/24
  ip router ospf 1 area 0.0.0.2
  no shutdown

interface Ethernet1/2
  ptp transport ipv4 ucast slave
    master ipv4 83.0.0.2
  ptp ucast-source 83.0.0.1
  ip address 83.0.0.1/24
  no shutdown

show ptp counters interface eth1/1 ipv4 81.0.0.2
PTP Packet Counters of IP 81.0.0.2:
```

```
-----------------------------------------------------------------
Packet Type                  TX                      RX
----------------    --------------------    --------------------
Announce                     9                       0
Sync                         70                      0
FollowUp                     70                      0
Delay Request                0                       18
Delay Response               18                      0
PDelay Request               0                       0
PDelay Response              0                       0
PDelay Followup              0                       0
Management                   0                       0
-----------------------------------------------------------------
```



CHAPTER 5

Media Controller

This section describes the DCNM Media Controller.

To bring up the devices from the basic configuration using POAP, you must define the templates and publish the POAP definition through Cisco DCNM **Web Client** > **Configure** > **Deploy** > **POAP Definitions**.

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

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

For information about the Media Controller APIs, see the Cisco DCNM Media Controller API reference on Cisco DevNet.

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

NX-OS Streaming Telemetry and DCNM

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

```
telemetry
  destination-profile
    use-vrf management
  destination-group 200
    ip address <dcnm-ip> port 50051 protocol gRPC encoding GPB
  destination-group 1500
  sensor-group 200
    data-source DME
    path sys/nbm/show/appliedpolicies depth unbounded
    path sys/nbm/show/stats depth unbounded
  sensor-group 201
    data-source DME
    path sys/nbm/show/flows depth 0 query-condition
    rsp-subtree-filter=eq(nbmNbmFlow.bucket,"1")&rsp-subtree=full
  sensor-group 202
```

```
  data-source DME
  path sys/nbm/show/flows depth 0 query-condition
  rsp-subtree-filter=eq(nbmNbmFlow.bucket,"2")&rsp-subtree=full
sensor-group 203
  data-source DME
  path sys/nbm/show/flows depth 0 query-condition
  rsp-subtree-filter=eq(nbmNbmFlow.bucket,"3")&rsp-subtree=full
sensor-group 204
  data-source DME
  path sys/nbm/show/flows depth 0 query-condition
  rsp-subtree-filter=eq(nbmNbmFlow.bucket,"4")&rsp-subtree=full
sensor-group 205
  data-source DME
  path sys/nbm/show/endpoints depth unbounded
sensor-group 300
  data-source NX-API
  path "show ptp brief"
  path "show ptp parent"
sensor-group 301
  data-source NX-API
  path "show ptp corrections"
sensor-group 500
  data-source NX-API
  path "show flow rtp details" depth 0
  path "show flow rtp errors active" depth 0
  path "show flow rtp errors history" depth 0
subscription 201
  dst-grp 200
  snsr-grp 200 sample-interval 60000
  snsr-grp 201 sample-interval 30000
  snsr-grp 205 sample-interval 30000
subscription 202
  dst-grp 200
  snsr-grp 202 sample-interval 30000
subscription 203
  dst-grp 200
  snsr-grp 203 sample-interval 30000
subscription 204
  dst-grp 200
  snsr-grp 204 sample-interval 30000
subscription 300
  dst-grp 200
  snsr-grp 300 sample-interval 30000
  snsr-grp 301 sample-interval 30000
subscription 500
  dst-grp 200
  snsr-grp 500 sample-interval 30000
```


Topology

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

Note

- If you remove a device from the Inventory, the Policy deployment status for that switch is removed. However, clear the policy configuration on the switch also.

Quick Search

Enter the search string to highlight relevant devices.

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

Multicast Group

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

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

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

Host

The Host menu includes the following submenus:

Discovered Host

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

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

Table 8: Discovered Host Table Fields and Description

Field	Description
Host Name	Specifies the configured Host Alias for the host IP address. The Host IP is displayed if the Host Alias is not configured.

Field	Description
Role	Specifies the role of the host device. The role of the host can be one of the following: • Sender • External Sender • Dynamic Receiver • External Receiver • Static Receiver
Multicast Group	Specifies the multicast address of the flow in which the host participates.
Source	Specifies the source of the flow which the discovered host participates in.
Switch	Specifies the name of the switch.
Interface	Specifies the interface to which the host is connected to on the sender or receiver switch.
MAC Address	Specifies the MAC address of a physical host, if the switch has ARP entry for that host).
Host Discovered Time	Specifies the date and time at which the switch discovered the host.
Fault Reason	Specifies the failure reason for the flow that the discovered host has participates in.

Host Alias

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

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

Table 9: 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.

Field	Description
Last Updated At	Specifies the date and time at which the host alias was last updated.

This section contains the following:

Add Host Alias

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

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.

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.

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.

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.

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

A notification window appears.

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

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

Host Policies

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

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

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

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

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

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

Table 10: 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 DCNM. • You can undeploy the default policy, but you cannot delete the default policy. You can delete and undeploy only the custom policies. • When you undeploy the default policies, All Default Policies will be reset to have default permission (Allow).
Delete All	Allows you to delete all custom policies without selecting any policy check box. **Note** • Undeploy policies from all switches before deleting them from DCNM. • You can undeploy the default policy, but you cannot delete the default policy. You can delete and undeploy only the custom policies.
Import	Allows you to import host policies from a CSV file to DCNM. **Note** After import, all policies imported from a CSV file are applied to all managed switches automatically.

Field	Description
Export	Allows you to export host policies from DCNM to a CSV file.

Field	Description
Deployment	

Field	Description

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

Field	Description
	successfully deployed.

Table 11: Host Policies Table Field and Description

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

This section contains the following:

Add Host Policy

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

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

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

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

The **Host Policies** window is displayed.

Step 2 Click the **Add** icon.

Step 3 In the Add Host Policy window, specify the parameters in the following fields.

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

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

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

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

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

Edit Host Policy

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

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

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

The **Host Policies** window is displayed.

Step 2 Check the check box next to the host policy name, that you need to edit.

Step 3 Click **Edit** Host policy icon.

Step 4 In the Edit Host Policy window, edit to specify if the policy will **Allow** or **Deny** traffic.

Note The changes made to Host Policy are applied immediately. If the policy is already applied to any device, the changes may impact the existing flows.

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

Click **Cancel** to discard the changes.

Delete Host Policy

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

Note You can delete only user-defined Host Policies.

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

The **Host Policies** window is displayed.

Step 2 Check the check box next to the host policy name, that you need to delete.

You can select more than one host policy to delete.

Step 3 Click **Delete** Host policy icon.

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

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

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

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

Import Host Policy

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

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

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

The **Host Policies** window is displayed.

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

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

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

Step 4 Click **Open**.

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

Export Host Policy

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

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.

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 12: 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.

Applied Host Polices

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

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

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

Table 13: 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

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

Fields and Descriptions

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

Table 14: Active Tab

Field	Description
Show Chart	Click Show Chart icon to view the graphical representation of the Flow Status. **Note** The data refers to the sender leaf when the sender starts broadcasting. See the receiver start time in the flow status table to find when the receiver started getting data. Click the **Show** drop-down list to view the flow status information in one of the following formats─Chart, Table, or Chart and Table. Click **Chart Type** icon to view the various chart types. Select a chart type to view the flow status information that is depicted in that chart format. You can choose a chart option to see filled patterns or data markers. Click **Actions** icon to print the report or excel chart information to your local directory.
Multicast IP	Specifies the multicast IP address for the flow. **Note** You can click the wave link next to the Multicast IP address to view the pictorial representation of flow statistics.
Flow Alias	Specifies the name of the Flow Alias.
Policed	Specifies whether a flow is policed or not policed.
Sender	Specifies the IP Address or the Host alias of the sender for the multicast group.
Receiver	Specifies the IP Address or the Host alias of the receiver joining the group.

Field	Description
Bandwidth	Specifies the bandwidth that is allotted for the traffic.
Sender Switch	Specifies if the Sender switch is a leaf or spine.
Sender Interface	Specifies the interface to which the sender is connected to.
Receiver Switch	Specifies if the Receiver switch is a leaf or spine.
Receiver Interface	Specifies the interface to which the receiver is connected to.
QOS/DSCP	Specifies the Switch-defined QoS Policy.
Flow Link State	Specifies the state of the flow link. Click **active** link to view the network diagram of the Sender and Receiver. The dotted line displays the direction of the flow of traffic. You can hover over the nodes to view information. The table on the right side shows information about the Sender and Receiver.
Policy ID	Specifies the policy ID applied to the multicast IP.
Sender Start Time	Displays the time from when the sender joined.
Receiver Join Time	Specifies the time at which the receiver joined.

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

Table 15: Inactive Tab

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

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

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

Table 16: Sender Only Tab

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

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

Table 17: Receiver Only Tab

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

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

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

Click the arrow to export the statistical data. You can export it in `.csv` or `.pdf` formats.

Note Cisco DCNM holds the Flow statistics values in the DCNM server internal memory. Therefore, after a DCNM Restart or HA switch over, the Flow statistics 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 DCNM, a message BW_UNAVAIL appears. This is resolved after the uplinks between the switches are detected by DCNM after discovery of the devices.

Flow Alias

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

You can configure a flow alias on **Media Controller > Flow > Flow Alias**.

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

Table 18: Flow Alias Table Field and Description

Field	Description
Flow Alias	Specifies the name of the Flow Alias.
Multicast IP Address	Specifies the multicast IP address for the traffic.
Description	Description added to the Flow Alias.

Field	Description
Last Updated at	Specifies the date on which the flow alias was last updated.

This section contains the following:

Add Flow Alias

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

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

The **Flow Alias** window is displayed.

Step 2 Click the **Add** Flow Alias icon.

Step 3 In the **Add Flow Alias** window, specify the parameters in the following fields.

- **Flow Name**: Specifies a unique flow alias name.
- **Multicast IP Address**: Specifies the multicast IP Address for the flow alias.
- **Description**: Specifies the description that you add for the flow alias.

Step 4 Click **Save** to save the flow alias.

Click **Cancel** to discard.

Edit Flow Alias

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

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

The **Flow Alias** window is displayed.

Step 2 Check the check box next to the flow alias name, that you need to edit.

Step 3 Click **Edit** Flow Alias icon.

Step 4 In the Edit Flow Alias window, edit the **Name**, **Multicast IP**, **Description** fields.

Step 5 Click **Save** to save the new configuration.

Click **Cancel** to discard the changes.

Delete Flow Alias

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

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

The **Flow Alias** window is displayed.

Step 2 Check the check box next to the flow alias, that you need to delete.

You can select more than one flow alias to delete.

Step 3 Click **Delete** Flow Alias icon.

The flow alias is deleted.

Export Flow Alias

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

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

The **Flow Alias** window is displayed.

Step 2 Click **Export** flow alias icon.

A notification window appears.

Step 3 Select a location on your directory to store the Alias details file.

Step 4 Click **OK**.

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

Import Flow Alias

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

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

The **Flow Alias** window is displayed.

Step 2 Click **Import** flow alias icon.

Step 3 Browse the directory and select the file which contains the Flow Alias configuration information.

Step 4 Click **Open**.

The flow alias configuration is imported and displayed on the **Media Controller** > **Flow** > **Flow Alias** window, on the Cisco DCNM Web Client.

Flow Policies

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

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

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

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

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

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

Table 19: Flow Policies Operations

Field	Description
Add	Allows you to add a new flow policy.
Edit	Allows you to view or edit the selected flow policy parameters.
Delete	Allows you to delete the user-defined flow policy. **Note** • You cannot delete the default flow policies. • Undeploy policies from all switches before deleting them from DCNM.
Delete All	Allows you to delete all the flow policies at a single instance. **Note** Undeploy policies from all switches before deleting them from DCNM.
Import	Allows you to import flow policies from a CSV file. **Note** After import, all policies imported from a CSV file are applied to all managed switches automatically.

Field	Description
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 20: Flow Policies Table Field and Description

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

Note A new flow policy or an edited flow policy is effective only under the following circumstances.

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

This section contains the following:

Add Flow Policy

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

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

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

The **Flow Policies** window is displayed.

Step 2 Click the **Add** Flow policy icon.

Step 3 In the Add Flow Policy window, specify the parameters in the following fields.

- **Policy Name**: Specifies a unique policy name for the flow policy.
- **Bandwidth**: Specifies the bandwidth that is allocated for the flow policy. Select of the radio buttons to choose **Gbps** or **Mbps**.

Step 4 From the **QoS/DSCP** drop-down list, choose an appropriate ENUM value.

Step 5 Click the **Policer** toggle switch to enable or disable policer for a flow. By default, the poilcer for a new flow policy is enabled.

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

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

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

Click **Cancel** to discard the changes.

Edit Flow Policy

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

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

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

DETAILED STEPS

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

The **Flow Policies** window is displayed.

Step 2 Check the check box next to the flow policy name, that you need to edit.

Step 3 Click **Edit** Flow policy icon.

Step 4 In the Edit Flow Policy window, edit the **Multicast IP**, **Bandwidth**, **QoS/DSCP** fields.

Step 5 Click the **Policer** toggle switch to enable or disable policer for a flow policy.

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

Click **Cancel** to discard the changes.

Delete Flow Policy

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

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

The **Flow Policies** window is displayed.

Step 2 Check the check box next to the flow policy name, that you need to delete.

You can select more than one flow policy to delete.

Note You cannot delete the default policies.

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

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

Import Flow Policy

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

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

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

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

The **Flow Policies** window is displayed.

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

Step 3 Browse the directory and select the file which contains the Flow Policy configuration information.

Step 4 Click **Open**.

The flow policy configuration is imported and displayed on the **Media Controller** > **Flow** > **Flow Policies** window, on the Cisco DCNM Web Client.

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

Export Flow Policy

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

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.

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 21: 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.

Global

The Global menu includes the following submenus:

Events

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

The PMN Events table is updated real-time.

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

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

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

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

Config

The Config menu includes the following submenus:

Setting Up the SNMP Server for DCNM

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

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

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

Step 2 For an Inband environment, use the `pmn_telemetry_snmp` CLI template that is packaged along with the Cisco DCNM Application, to configure more SNMP settings on the switch. For more information, see Switch Global Config, on page 90.

AMQP Notifications

For all DCNM operations (such as Host Alias, Host Policy, and so on), AMQP notifications are sent. For operations triggered by the switch and received through telemetry (such as Flow Status), Cisco DCNM periodically checks for new events and generate appropriate notifications. This time period can be configured by setting the "AMQP_POLL_TIME" value in the `server.properties`.

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

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

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

   ```
   AMQP_POLL_TIME=5
   ```

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

   appmgr restart dcnm—for Standalone deployment

   appmgr restart ha-apps—for Native HA deployment

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

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

AMQP Notification Components

- **Routing Key**

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

- **Routing Key Format**

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

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

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

- **Message Properties**

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

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

- **Notification Body**

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

Switch Global Config

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

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

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

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

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

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

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

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

AMQP Notifications

As Cisco DCNM uses Telemetry to fetch data from the Fabric, the flow status and AMQP notifications may not reflect the current state in real time. It periodically checks new events and generate appropriate notification. Also, flows are no longer limited to a single spine and may take N or W or M shape. Host policies are applied based on the switch interface configuration and not just-in-time (JIT). All these architecture changes influence current AMQP messages and trigger time. By default, poll interval is set to 2 minutes. For more information, see AMQP Notifications, on page 88.

Unicast Bandwidth Reservation

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

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

ASM Range

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

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

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

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

Table 22: Operations on the Global Config screen

Icon	Description
Save	Click **Save** to save the configurations.
Deploy	To deploy the configuration, you can choose one of the following from the drop-down list: • **All**—Deploys both ASM and Bandwidth configuration to all switches. • **Unicast BW**—Deploys only unicast 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 both ASM and Bandwidth configuration to all switches. • **Unicast BW**—Undeploys only unicast 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 23: 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.

WAN Links

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

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

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

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

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

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

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

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

Table 24: WAN Links Table Field and Description

Field	Description
Status	Specifies if the WAN links are deployed or undeployed on the selected switch.
History	Click this link to view the deployment history. For description about the fields that appear on this page, see the table below.
Interface Name	Specifies the interface which is connected as a WAN link to the end device and this interface will be in Layer 3.
Admin Status	An up arrow depicts that the status is up. A down arrow implies that the status is down.
Oper Status	An up arrow depicts that the operational state of the interface is up. A down arrow implies that the status is down.

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

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

Table 25: Deployment History Field and Description

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

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

DCNM Read-Only Mode for Media Controller

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

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

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

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

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

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

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

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

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

INDEX

R

S

V