



Cisco Nexus 9000 Series NX-OS IP Fabric for Media Solution Guide, Release 9.3(x)

First Published: 2019-07-20

Last Modified: 2022-02-08

Americas Headquarters

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: <http://www.cisco.com/go/softwareterms>. Cisco product warranty information is available at <http://www.cisco.com/go/warranty>. US Federal Communications Commission Notices are found here <http://www.cisco.com/c/en/us/products/us-fcc-notice.html>.

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

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and-if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

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

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019–2022 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1**New and Changed Information 1**

New and Changed Information 1

CHAPTER 2**Overview of Cisco's IP Fabric for Media Solution 3**

Licensing Requirements 3

About the IP Fabric for Media Solution 3

Deployment Types 3

Spine-Leaf Topology 4

Single Modular Switch Topology 4

IP Fabric for Media Solution Components 5

Cisco Nexus 9000 Series Switches 5

DCNM Media Controller 6

Failure Handling 7

Benefits of the IP Fabric for Media Solution 7

Related Documentation 7

CHAPTER 3**Setting Up the IP Fabric for Media 9**

Determining the Number and Types of Leaf Switches Required in the IP Fabric 9

Determining the Number of Achievable Flows in the IP Fabric 12

CHAPTER 4**Configuring IP Fabric for Media 15**

Prerequisites 15

Guidelines and Limitations 16

Guidelines and Limitations for Host Policies 17

Guidelines and Limitations for Unicast PTP 18

Guidelines and Limitations for the Cisco DCNM Media Controller 19

Licensing Requirements for DCNM Media Controller	20
Upgrading to a Cisco NX-OS 9.x Release	20
Upgrading from a Cisco NX-OS 9.x Release	20
Upgrading from a Cisco NX-OS 7.x Release	20
Setting Up the SNMP Server for DCNM	21
Configuring NBM	21
Configuring NBM for a Spine-Leaf Topology	22
Configuring PIM on Spine and Leaf Switches	27
Configuring MSDP on Spine Switches	29
Configuring Fabric and Host Interfaces	30
Configuring NBM for a Single Modular Switch	36
Configuring an NBM VRF	39
Configuring an NBM VRF for Active Flow Provisioning	40
Configuring an NBM VRF for Static Flow Provisioning	44
Establishing a Flow (Optional)	45
Creating an NBM Flow Definition	45
Configuring IGMP Static OIF	49
Configuring Multisite	49
Enabling Multicast and Unicast Flows (Optional)	50
Verifying the NBM Configuration	54
Clearing NBM Flow Statistics	56
Configuring Unicast PTP Peers	56

CHAPTER 5**Configuring Media Flow Analytics** 59

RTP Flow Monitoring	59
Guidelines and Limitations for RTP Flow Monitoring	59
Configuring RTP Flow Monitoring	60
Displaying RTP Flows and Errors	61
Clearing RTP Flows	62

CHAPTER 6**Configuring Multicast Service Reflection with NBM** 65

Multicast Service Reflection with NBM	65
---------------------------------------	----

CHAPTER 7**Media Controller** 67

Generic Multicast Monitoring	69
Topology	72
Host	72
Discovered Host	73
Host Alias	74
Add Host Alias	74
Edit Host Alias	74
Delete Host Alias	75
Import Host Alias	75
Export Host Alias	75
Host Policies	76
Add Host Policy	81
Edit Host Policy	82
Delete Host Policy	82
Import Host Policy	83
Export Host Policy	83
Policy Deployment	83
Applied Host Policies	85
Flow	86
Flow Status	86
Flow Alias	89
Add Flow Alias	90
Edit Flow Alias	90
Delete Flow Alias	91
Export Flow Alias	91
Import Flow Alias	91
Flow Policies	92
Add Flow Policy	97
Edit Flow Policy	98
Delete Flow Policy	99
Import Flow Policy	99
Export Flow Policy	100
Policy Deployment	100
RTP	102

RTP Flow Monitor	102
Global	104
Events	104
Copying Switch Running Configuration to Start-up Configuration	105
Realtime Notifications	105
Threshold Notifications	106
Config	106
Setting Up the SNMP Server for DCNM	106
AMQP Notifications	107
Switch Global Config	109
WAN Links	112
DCNM Read-Only Mode for Media Controller	115

APPENDIX A

Sample Output for Show Commands	119
Sample Show Command Output (Spine-Leaf Deployment)	119
Sample Show Command Output (Single Modular Switches)	134



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 9.3(x)*.

- [New and Changed Information, on page 1](#)

New and Changed Information

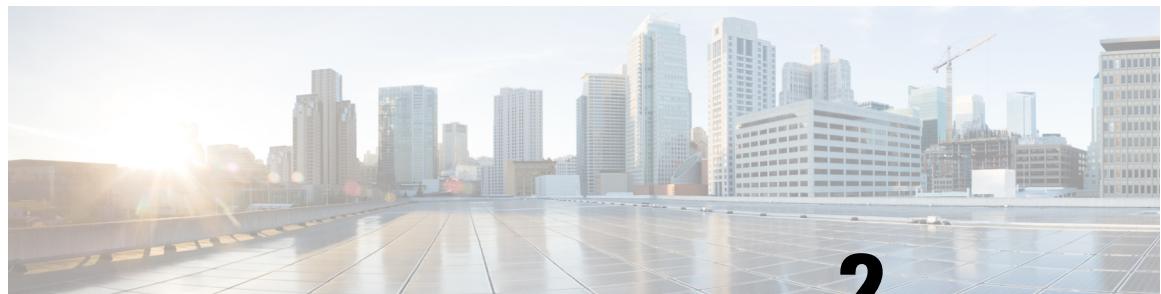
This table summarizes the new and changed features for the *Cisco Nexus 9000 Series NX-OS IP Fabric for Media Solution Guide, Release 9.3(x)* and tells you where they are documented.

Table 1: New and Changed Features

Feature	Description	Changed in Release	Where Documented
No new features	No new updates for this release.	9.3(9)	
RTP flow monitoring	Added support for Cisco Nexus 9300-GX platform switches.	9.3(6)	Configuring Media Flow Analytics, on page 59
IP fabric for media	Added support for the Cisco Nexus 9316D-GX, 9364C-GX, 93600CD-GX, 93180YC-FX3S and switches.	9.3(5)	Cisco Nexus 9000 Series Switches, on page 5
Multicast Service Reflection	Added support for Multicast Service Reflection.	9.3(5)	Multicast Service Reflection with NBM, on page 65
PMN Flow Prioritization	Added support for PMN Flow Prioritization	9.3(5)	Configuring NBM for a Spine-Leaf Topology, on page 22 Configuring NBM for a Single Modular Switch, on page 36 Configuring an NBM VRF for Active Flow Provisioning, on page 40

New and Changed Information

Feature	Description	Changed in Release	Where Documented
IP fabric for media	Added support for the Cisco Nexus 93216TC-FX2 and 93360YC-FX2 as leaf switches.	9.3(3)	Cisco Nexus 9000 Series Switches, on page 5
Static flow provisioning	Introduced this feature for all platforms that support IP fabric for media.	9.3(3)	Configuring an NBM VRF for Static Flow Provisioning, on page 44
NBM	Made NBM VRF aware.	9.3(1)	Configuring an NBM VRF for Active Flow Provisioning, on page 40
Policing, DSCP remarking, and flow statistics	Added support for Cisco Nexus 9504 and 9508 platform switches with -R line cards.	9.3(1)	Guidelines and Limitations, on page 16
RTP flow monitoring	Introduced this feature for Cisco Nexus 9300-FX and 9300-FX2 platform switches.	9.3(1)	Configuring Media Flow Analytics, on page 59



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, on page 3](#)
- [About the IP Fabric for Media Solution, on page 3](#)
- [IP Fabric for Media Solution Components, on page 5](#)
- [Failure Handling, on page 7](#)
- [Benefits of the IP Fabric for Media Solution, on page 7](#)
- [Related Documentation, on page 7](#)

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](#) and the [Cisco NX-OS Licensing Options 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

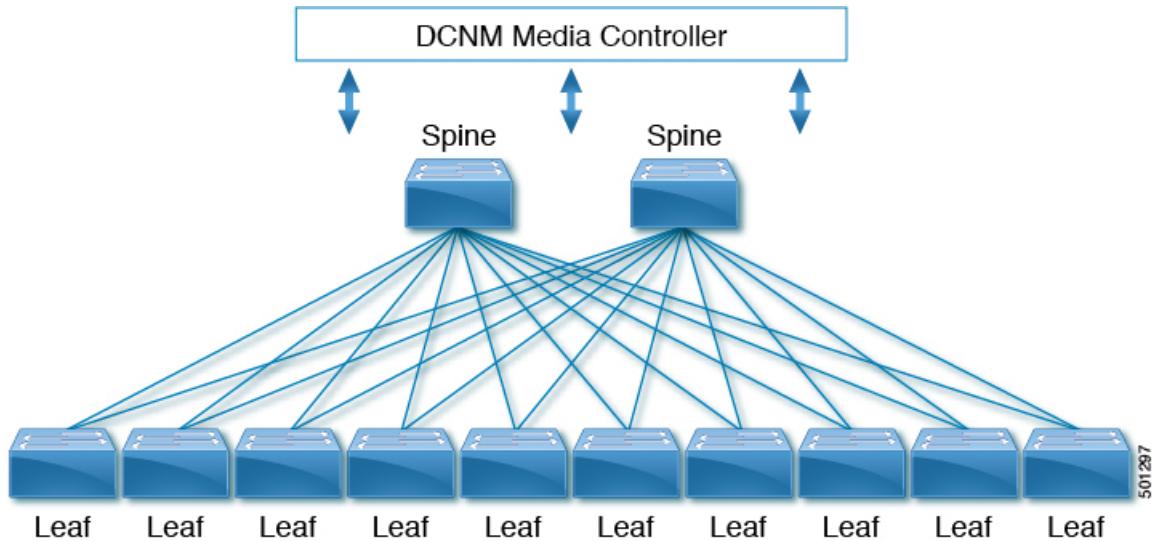
Cisco's IP fabric for media solution supports the following types of deployments:

Spine-Leaf Topology

- 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

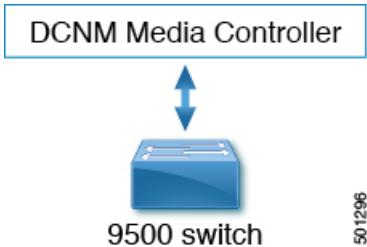
Cisco's IP fabric for media solution supports a spine-leaf topology that consists of multiple spine and leaf switches. The topology supports any combination of leaf switches, including using just one type of leaf switch.



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 93216TC-FX2 switch	96 x 1/10-Gbps ports	Leaf in spine-leaf topology
Cisco Nexus 93240YC-FX2 switch	48 x 10/25-Gbps ports	Leaf in spine-leaf topology
Cisco Nexus 93360YC-FX2 switch	96 x 10/25-Gbps ports	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	36 x 40/100-Gbps ports (for N9K-X9636C-R line cards) 36 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
Note The N9K-X96136YC-R line card is not supported.		
Cisco Nexus 9316D-GX switch	16 x 400/100-Gbps QSFP-DD ports	Leaf in spine-leaf topology

Cisco Nexus 9000 Series Switch	Number and Size of Ports	Role in Topology*
Cisco Nexus 9364C-GX switch	64 x 100/40-Gbps Quad Small Form-Factor Pluggable (QSFP28) ports	Leaf in spine-leaf topology
Cisco Nexus 93600CD-GX switch	28 x 100/40-Gbps Quad Small Form-Factor Pluggable (QSFP28) and 8 x 400/100-Gbps QSFP-DD ports	Leaf in spine-leaf topology
Cisco Nexus 93180YC-FX3S switch	48 25/50/100-Gigabit Ethernet SFP28 ports (ports 1-48) and 6 10/25/40/50/100-Gigabit QSFP28 ports (ports 49-54)	Leaf in spine-leaf topology
Cisco Nexus 93180YC-FX3	48 x 1/10/25 Gbps fiber ports and 6 x 40/100 Gbps QSFP28 ports	Leaf in spine-leaf topology
Cisco Nexus 93108TC-FX3P	48 x 100M/1/2.5/5/10 Gbps BASE-T ports 6 x 40/100 Gbps Quad small form-factor pluggable 28 (QSFP28) ports	Leaf in spine-leaf topology

*The role indicates the place in the fabric that makes the most sense given the port speeds supported by each switch. There are no restrictions as such on the role for which a switch can be used.

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 and Upgrade Guide for Media Deployment Cisco DCNM online help
Cisco NX-OS release information	Cisco Nexus 9000 Series NX-OS IP Fabric for Media Release Information
Cisco NX-OS software upgrades	Cisco Nexus 9000 Series NX-OS Software Upgrade and Installation 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

Related Topic	Document Title
NX-API REST	Cisco Nexus 3000 and 9000 Series NX-API REST SDK User 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, on page 9](#)
- [Determining the Number of Achievable Flows in the IP Fabric, on page 12](#)

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 10-Gbps endpoints, use the Cisco Nexus 92160YC-X, 93108TC-EX, 93108TC-FX, 93216TC-FX2, 93180YC-FX, or 93180YC-EX leaf switches.
 - For 25-Gbps endpoints, use the Cisco Nexus 93180YC-FX, 93180YC-EX, 93240YC-FX2, or 93360YC-FX2 leaf switches.
 - For 40-Gbps endpoints, use the Cisco Nexus 9272Q, 9336C-FX2, 9364C, or 9332C leaf switches.
 - For 100-Gbps endpoints, use the Cisco Nexus 9236C, 9336C-FX2, 9364C, or 9332C 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.

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

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 93216TC-FX2 switch	96 x 1/10-Gbps endpoints	12 x 40/100-Gbps (1200-Gbps) uplinks
Cisco Nexus 93240YC-FX2 switch	48 x 10/25-Gbps endpoints	12 x 100-Gbps (1200-Gbps) uplinks
Cisco Nexus 93360YC-FX2 switch	96 x 10/25-Gbps endpoints	12 x 40/100-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.

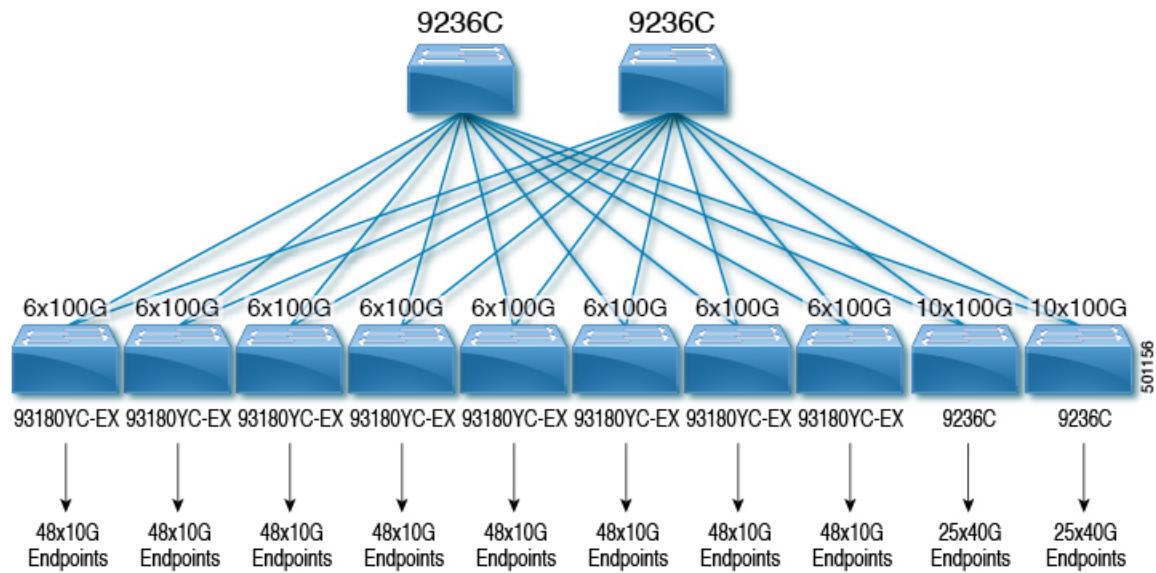
3840-Gbps downstream bandwidth (for eight Cisco Nexus 93180YC-EX leaf switches) + 2000-Gbps downstream bandwidth (for two Cisco Nexus 9236C leaf switches) = 5840-Gbps total downstream bandwidth.

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.

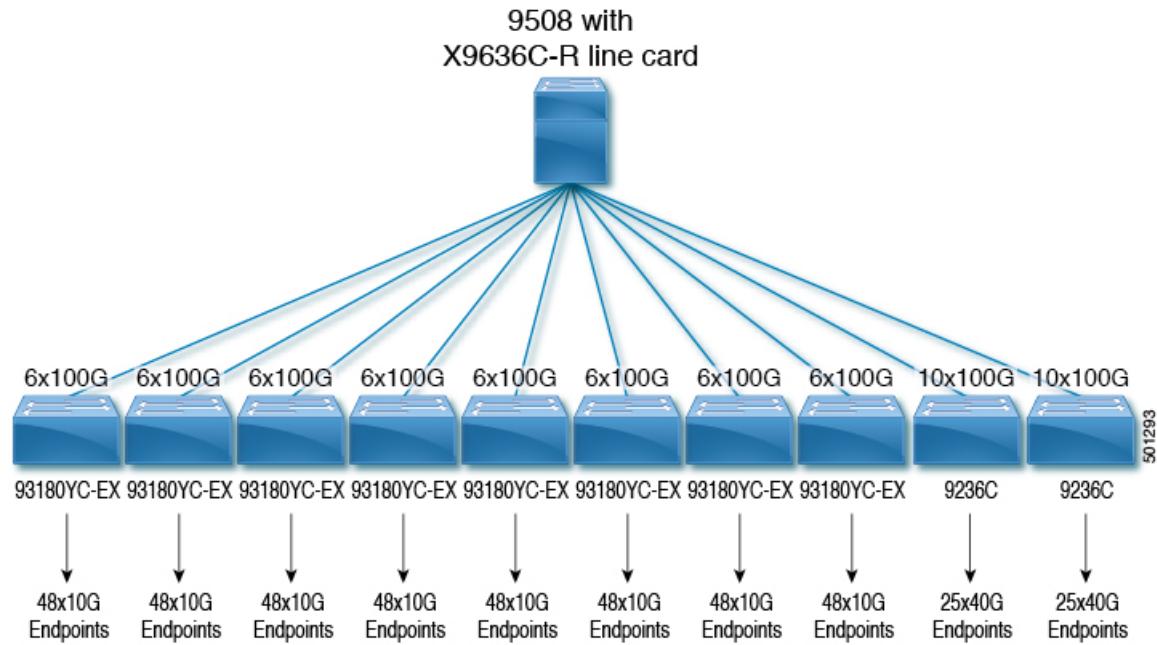
The NBM flows can't utilize all the expected bandwidth as the **PIM bidir RP** configuration utilizes the NBM bandwidth available. To increase the NBM bandwidth, remove the **PIM bidir RP** configuration.

The following topology uses the examples in this section:

Determining the Number of Achievable Flows in the IP Fabric



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:

$$\text{Total Bandwidth} \div \text{Flow Size} = \text{Number of Achievable Flows}$$

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

Determining the Number of Achievable Flows in the IP Fabric



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, on page 15](#)
- [Guidelines and Limitations, on page 16](#)
- [Licensing Requirements for DCNM Media Controller, on page 20](#)
- [Upgrading to a Cisco NX-OS 9.x Release, on page 20](#)
- [Setting Up the SNMP Server for DCNM, on page 21](#)
- [Configuring NBM, on page 21](#)
- [Configuring Unicast PTP Peers, on page 56](#)

Prerequisites

Cisco's IP fabric for media solution has the following prerequisites:

- For Cisco Nexus 9504 and 9508 switches with -R line cards, configure these TCAM carving commands in the following order and then reload the switch:

```
hardware access-list tcam region redirect_v6 0
hardware access-list tcam region ing-nbm 2048
```

- For all other switches, configure these TCAM carving commands in the following order 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 and Upgrade Guide for Media Controller Deployment](#) for your DCNM release.

Cisco NX-OS Release	Cisco DCNM Release
9.3(5)	11.4(1)
9.3(3)	11.3(1)
9.3(1)	11.2(1)

Guidelines and Limitations

The 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.
- 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 allows 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.
- During a failure, the PMN Flow Prioritization feature tries to recover priority flows where possible. By design, PMN Flow Prioritization does not bring down already established flows to accommodate priority flows.
- For Cisco Nexus 9500 -R line cards, when configured in NBM Passive mode there will be increasing input discards and this has been determined to be expected and non-impacting.
- 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:

Guidelines and Limitations for Unicast PTP

```
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, 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, 93216TC-FX2, 93240YC-FX2, 93360YC-FX2, 9336C-FX2, 9348GC-FXP, and 9364C switches
 - Cisco Nexus 9504 and 9508 switches with -R line cards

Guidelines and Limitations for the Cisco 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, it 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. 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 [.](#)
- 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**
18. (Optional) [no] **priority critical**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example:	Enters global configuration mode.

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
Step 2	<p>[no] feature nbm</p> <p>Example: switch(config)# feature nbm</p>	<p>Enables the NBM feature and PIM active mode, which allows the NBM fabric to form a multicast flow without assistance from an external controller.</p> <p>When you enter the feature nbm command, the following commands are also enabled automatically:</p> <ul style="list-style-type: none"> • nbm mode pim-active • ip multicast multipath nbm • ip pim prune-on-expiry • cdp enable <p>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.</p> <p>Note If you disable NBM for Cisco Nexus 9504 and 9508 switches with -R line cards, you must configure these TCAM carving commands in the following order and then reload the switch. The recommended TCAM value is 2048.</p> <pre>hardware access-list tcam region ing-nbm 0 hardware access-list tcam region redirect_v6 TCAM-size</pre> <p>Note If you want to configure an NBM VRF, see Configuring an NBM VRF for Active Flow Provisioning, on page 40.</p>
Step 3	(Optional) [no] nbm host-policy	Configures an NBM host policy for the switch.
	<p>Example: switch(config)# nbm host-policy switch(config-nbm-host-pol)#</p>	
Step 4	(Optional) {sender receiver pim}	Configures the NBM host policy for a sender, local receiver, or external receiver (PIM).
	<p>Example: switch(config-nbm-host-pol)# sender switch(config-nbm-host-pol-sender)#</p>	<p>Note Before you update the default NBM host policy, you must first delete any custom host policies.</p>
Step 5	(Optional) default {permit deny}	Specifies the default action for the NBM host policy. All three types of host policies are allowed by default.
	<p>Example:</p>	

	Command or Action	Purpose								
	switch(config-nbm-host-pol-sender) # default permit									
Step 6	<p>(Optional) Enter one of the following commands:</p> <ul style="list-style-type: none"> 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} <p>Example:</p> <pre>switch(config-nbm-host-pol-sender) # 10 host 10.1.1.3 group 229.1.1.1/32 deny</pre> <p>Example:</p> <pre>switch(config-nbm-host-pol-rcvr) # 40 host 10.1.1.1 source 145.1.1.1 group 234.1.1.1/32 deny</pre> <p>Example:</p> <pre>switch(config-nbm-host-pol-pim) # 50 source 10.1.1.1 group 235.1.1.1/32 deny</pre>	<p>Specifies if the sender or receiver flows are to be permitted or denied.</p> <p>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.</p>								
Step 7	<p>(Optional) [no] nbm reserve unicast fabric bandwidth value</p> <p>Example:</p> <pre>switch(config) # nbm reserve unicast fabric bandwidth 2</pre>	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	<p>[no] nbm flow asm range [group-range-prefixes]</p> <p>Example:</p> <pre>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</pre>	<p>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.</p> <p>Note This command is needed only in a multispine deployment.</p>								
Step 9	<p>[no] nbm flow bandwidth flow-bandwidth {kbps mbps gbps}</p> <p>Example:</p> <pre>switch(config) # nbm flow bandwidth 3000 mbps</pre>	<p>Configures the global NBM flow bandwidth in Kbps, Mbps, or Gbps. The minimum supported flow bandwidth is 200 Kbps.</p> <table border="1"> <thead> <tr> <th>Range</th> <th>Default Value</th> </tr> </thead> <tbody> <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> </tbody> </table>	Range	Default Value	1 to 25,000,000 Kbps	0 Kbps	1 to 25,000 Mbps	0 Mbps	1 to 25 Gbps	0 Gbps
Range	Default Value									
1 to 25,000,000 Kbps	0 Kbps									
1 to 25,000 Mbps	0 Mbps									
1 to 25 Gbps	0 Gbps									

	Command or Action	Purpose						
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.						
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: 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 .						
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. <table border="1" data-bbox="910 1670 1530 1848"> <thead> <tr> <th>Range</th> <th>Default Value</th> </tr> </thead> <tbody> <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> </tbody> </table>	Range	Default Value	1 to 25,000,000 Kbps	0 Kbps	1 to 25,000 Mbps	0 Mbps
Range	Default Value							
1 to 25,000,000 Kbps	0 Kbps							
1 to 25,000 Mbps	0 Mbps							

	Command or Action	Purpose	
		Range	Default Value
		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 with this policy.	
Step 18	(Optional) [no] priority critical Example: switch(config-nbm-flow-pol-attr-prop)# priority critical switch(config-nbm-flow-pol-attr-prop) #	Enables critical flow prioritization for the multicast groups that are being configured.	

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
Applied Local host policies
  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

[Configuring PIM on Spine and Leaf Switches](#)

[Configuring MSDP on Spine Switches](#)

- [Configuring Fabric and Host Interfaces](#)
- [Configuring an NBM VRF, on page 39](#)
- [Establishing a Flow \(Optional\)](#)

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. 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 <i>rp-address</i> group-list <i>ip-prefix</i> 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:	Forces sender traffic to the spine layer, which reduces flow setup latency.

	Command or Action	Purpose
	<code>switch(config)# ip pim ssm range none</code>	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: <code>switch(config)# ip pim spt-threshold infinity group-list mcast-all</code>	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: <code>switch(config)# route-map mcast-all permit 10</code> <code>switch(config-route-map) #</code>	Enters route-map configuration mode.
Step 6	match ip multicast group policy-name permit sequence-number Example: <code>switch(config-route-map) # match ip multicast group 224.0.0.0/4</code>	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: <code>switch(config)# interface ethernet 2/1</code> <code>switch(config-if) #</code>	Specifies an interface to configure and enters the interface configuration mode.
Step 8	mtu mtu-size Example: <code>switch(config-if) # mtu 9216</code>	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: <code>switch(config-if) # ip address 10.3.10.1/24</code>	Configures an IP address for this interface.
Step 10	ip ospf passive-interface Example: <code>switch(config-if) # ip ospf passive-interface</code>	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: <code>switch(config-if) # ip router ospf p1 area 0.0.0.0</code>	Enables OSPF on the interface.
Step 12	ip pim sparse-mode Example: <code>switch(config-if) # ip pim sparse-mode</code>	Enables PIM sparse mode on the interface.

	Command or Action	Purpose
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	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.

	Command or Action	Purpose
Step 2	Configure a loopback interface to establish an MSDP session between the spine switches. Example: <pre>interface loopback1 ip address 2.2.3.3/32 ip router ospf p1 area 0.0.0.0 ip pim sparse-mode</pre>	Establishes an MSDP session between the spine switches.
Step 3	ip msdp originator-id interface Example: <pre>switch(config)# ip msdp originator-id loopback1</pre>	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: <pre>switch(config)# ip msdp peer 2.2.1.1 connect-source loopback1</pre>	Configures an MSDP peer with the specified peer IP address.
Step 5	ip msdp sa-policy peer-ip-address policy-name out Example: <pre>switch(config)# ip msdp sa-policy 2.2.1.1 msdp-mcast-all out</pre>	Enables a route-map policy for outgoing SA messages. By default, all registered sources are sent in SA messages.
Step 6	route-map policy-name permit sequence-number Example: <pre>switch(config)# route-map msdp-mcast-all permit 10 switch(config-route-map)# </pre>	Enters route-map configuration mode.
Step 7	match ip multicast group policy-name permit sequence-number Example: <pre>switch(config-route-map)# match ip multicast group 224.0.0.0/8</pre>	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: <pre>switch# configure terminal switch(config) #</pre>	Enters global configuration mode.
Step 2	interface ethernet slot/port Example: <pre>switch(config)# interface ethernet 1/49 switch(config-if) #</pre>	Specifies the fabric interface and enters interface configuration mode.
Step 3	ip address ip-prefix/length Example: <pre>switch(config-if) # ip address 1.1.1.0/31</pre>	Assigns an IP address and subnet mask to this interface.
Step 4	ip router ospf instance-tag area area-id Example: <pre>switch(config-if) # ip router ospf 100 area 0.0.0.0</pre>	Adds the interface to the OSPFv2 instance and area.
Step 5	ip pim sparse-mode Example: <pre>switch(config-if) # ip pim sparse-mode</pre>	Enables PIM sparse mode on this interface.
Step 6	no shutdown Example: <pre>switch(config-if) # no shutdown</pre>	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.
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.

	Command or Action	Purpose
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:	Enters global configuration mode.

Configuring a Layer 2 with SVI Host Interface

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
Step 2	feature interface-vlan Example: switch(config)# feature interface-vlan	Enables the creation of VLAN interfaces.
Step 3	vlan <i>vlan-id</i> 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 <i>vlan-id</i> Example: switch(config)# vlan configuration 5 switch(config-vlan-config)#	Allows you to configure VLANs without actually creating them.
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 <i>vlan-id</i> 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.

	Command or Action	Purpose
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: switch(config-if)# ip igmp suppress v3-gsq	Prevents the router from generating a query when it receives an IGMPv3 leave report.
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:	Configures one of the following options:

	Command or Action	Purpose
	<code>switch(config-if)# switchport mode trunk</code>	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 <i>vlan-id</i> Example: <code>switch(config-if)# switchport trunk allowed vlan 5</code>	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: <code>switch(config-if)# no shutdown</code>	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.
Step 23	exit Example: <code>switch(config-if)# exit switch(config)#[/b]</code>	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. (Optional) [no] **priority critical**
11. [no] **ip group-range ip-address to ip-address**
12. (Optional) [no] **priority critical**

DETAILED STEPS

	Command or Action	Purpose								
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.								
Step 2	[no] feature nbm Example: <pre>switch(config)# feature nbm</pre>	<p>Enables the NBM feature. The no form of this command disables this feature.</p> <p>Note If you disable NBM for Cisco Nexus 9504 and 9508 switches with -R line cards, you must configure these TCAM carving commands in the following order and reload the switch. The recommended TCAM value is 2048.</p> <pre>hardware access-list tcam region ing-nbm 0 hardware access-list tcam region redirect_v6 TCAM-size</pre> <p>Note If you want to configure an NBM VRF, see Configuring an NBM VRF for Active Flow Provisioning, on page 40.</p>								
Step 3	[no] nbm flow bandwidth flow-bandwidth {kbps mbps gbps} Example: <pre>switch(config)# nbm flow bandwidth 150 mbps</pre>	<p>Configures the global NBM flow bandwidth in Kbps, Mbps, or Gbps. The minimum supported flow bandwidth is 200 Kbps.</p> <table border="1"> <thead> <tr> <th>Range</th><th>Default Value</th></tr> </thead> <tbody> <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> </tbody> </table>	Range	Default Value	1 to 25,000,000 Kbps	0 Kbps	1 to 25,000 Mbps	0 Mbps	1 to 25 Gbps	0 Gbps
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 4	(Optional) [no] nbm flow policer Example:	Enables or disables the policer for all NBM flow policies. The policer is enabled by default.								

	Command or Action	Purpose								
	switch(config)# no nbm flow policer									
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 <i>policy-name</i> 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 the <i>Configuring Shared Policers</i> section in the <i>Configuring Policing</i> chapter of <i>Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide</i> on Cisco.com .								
Step 8	[no] bandwidth <i>flow-bandwidth {kbps mbps gbps}</i> 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. <table border="1" data-bbox="878 1516 1494 1748"> <thead> <tr> <th>Range</th><th>Default Value</th></tr> </thead> <tbody> <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> </tbody> </table>	Range	Default Value	1 to 25,000,000 Kbps	0 Kbps	1 to 25,000 Mbps	0 Mbps	1 to 25 Gbps	0 Gbps
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 <i>ip-address</i> Example:	Specifies the IP address for /32 multicast groups.								

	Command or Action	Purpose
	switch(config-nbm-flow-pol-attr)# ip group 228.0.0.15 switch(config-nbm-flow-pol-attr)# ip group 228.0.255.15	
Step 10	(Optional) [no] priority critical Example: switch(config-nbm-flow-pol-attr-prop)# priority critical switch(config-nbm-flow-pol-attr-prop) #	Enables critical flow prioritization for the multicast group that is being configured.
Step 11	[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.
Step 12	(Optional) [no] priority critical Example: switch(config-nbm-flow-pol-attr-prop)# priority critical switch(config-nbm-flow-pol-attr-prop) #	Enables critical flow prioritization for the multicast groups that are being configured.

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

[Configuring an NBM VRF, on page 39](#)

[Establishing a Flow \(Optional\)](#)

Configuring an NBM VRF

When you configure NBM (using the **nbm feature** command), the system automatically creates a default NBM virtual routing and forwarding instance (VRF). You can also configure custom NBM VRFs.

Configuring an NBM VRF for Active Flow Provisioning

NBM VRFs support multi-tenancy at the fabric level, allowing multiple customers to leverage the same IP fabric for media infrastructure simultaneously. NBM VRFs are independent of the default VRF and support all existing commands. Each VRF has its own set of policies.

You can configure your custom VRFs for either PIM active or PIM passive mode, depending on whether you want to enable active or static flow provisioning. Doing so allows the NBM fabric to form a multicast flow either with or without assistance from an external controller.



Note You must configure all VRFs in the same mode.

See the [Cisco Nexus 9000 Series NX-OS Verified Scalability Guide, Release 9.3\(x\)](#) for the number of supported NBM VRFs.

Configuring an NBM VRF for Active Flow Provisioning

You can configure an NBM VRF for active flow provisioning, which allows the NBM fabric to form a multicast flow without assistance from an external controller.

Before you begin

Configure NBM.

Before you associate an NBM VRF, create the VRF routing context (using the **vrf context vrf-name** command) and complete the unicast routing and PIM configurations.

SUMMARY STEPS

1. **configure terminal**
2. **[no] nbm vrf vrf-name**
3. **nbm mode pim-active**
4. (Optional) **[no] nbm host-policy**
5. (Optional) **{sender | receiver | pim}**
6. (Optional) **default {permit | deny}**
7. (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}**
8. (Optional) **[no] nbm reserve unicast fabric bandwidth value**
9. **[no] nbm flow asm range [group-range-prefixes]**
10. **[no] nbm flow bandwidth flow-bandwidth {kbps | mbps | gbps}**
11. **[no] nbm flow dscp value**
12. (Optional) **[no] nbm flow reserve-bandwidth receiver-only**
13. (Optional) **[no] nbm flow policer**
14. **[no] nbm flow-policy**
15. **[no] policy policy-name**
16. (Optional) **[no] policer**

17. [no] **bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**}
18. [no] **dscp** *value*
19. [no] **ip group-range** *ip-address* **to** *ip-address*
20. (Optional) [no] **priority critical**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	[no] nbm vrf <i>vrf-name</i> Example: switch(config)# nbm vrf nbm	Creates an NBM VRF.
Step 3	nbm mode pim-active Example: switch(config)# nbm mode pim-active	Allows the NBM fabric to form a multicast flow without assistance from an external controller. Note You cannot disable PIM active mode for a custom NBM VRF. You can change the NBM VRF from PIM active mode to PIM passive mode but only if you first delete the custom configuration under the VRF. Otherwise, the following error appears: "NBM cannot be set to PIM-PASSIVE mode while custom config exists. Please delete all custom nbm config and retry."
Step 4	(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 5	(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 6	(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 7	(Optional) Enter one of the following commands: • For sender host policies: <i>sequence-number host ip-address group ip-prefix {deny permit}</i>	Specifies if the sender or receiver flows are to be permitted or denied.

	Command or Action	Purpose								
	<ul style="list-style-type: none"> For local receiver host policies: <code>sequence-number host ip-address source ip-address group ip-prefix {deny permit}</code> For external receiver (PIM) host policies: <code>sequence-number source ip-address group ip-prefix {deny permit}</code> <p>Example: <code>switch(config-nbm-host-pol-sender)# 10 host 101.1.1.3 group 229.1.1.1/32 deny</code></p> <p>Example: <code>switch(config-nbm-host-pol-rcvr)# 40 host 100.1.1.1 source 145.1.1.1 group 234.1.1.1/32 deny</code></p> <p>Example: <code>switch(config-nbm-host-pol-pim)# 50 source 101.1.1.1 group 235.1.1.1/32 deny</code></p>	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.								
Step 8	(Optional) [no] nbm reserve unicast fabric bandwidth value	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 9	[no] nbm flow asm range [group-range-prefixes]	<p>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.</p> <p>Note This command is needed only in a multispine deployment.</p>								
Step 10	[no] nbm flow bandwidth flow-bandwidth {kbps mbps gbps}	<p>Configures the global NBM flow bandwidth in Kbps, Mbps, or Gbps. The minimum supported flow bandwidth is 200 Kbps.</p> <table border="1"> <thead> <tr> <th>Range</th><th>Default Value</th></tr> </thead> <tbody> <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> </tbody> </table>	Range	Default Value	1 to 25,000,000 Kbps	0 Kbps	1 to 25,000 Mbps	0 Mbps	1 to 25 Gbps	0 Gbps
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 11	[no] nbm flow dscp value	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 12	(Optional) [no] nbm flow reserve-bandwidth receiver-only	Enables optimization of bandwidth utilization by determination of no valid receivers on the RP and releases								

	Command or Action	Purpose
	Example: <pre>switch(config)# nbm flow reserve-bandwidth receiver-only</pre>	the unneeded RPF bandwidth. (Prevents RP from pre-reserving bandwidth towards FHR.) Disable the optimization of bandwidth utilization with the no nbm flow reserve-bandwidth receiver-only command. The feature is disabled by default.
Step 13	(Optional) [no] nbm flow policer Example: <pre>switch(config)# no nbm flow policer</pre>	Enables or disables the policer for all NBM flow policies. The policer is enabled by default.
Step 14	[no] nbm flow-policy Example: <pre>switch(config)# nbm flow-policy switch(config-nbm-flow-pol) #</pre>	Configures the flow bandwidth per flow.
Step 15	[no] policy policy-name Example: <pre>switch(config-nbm-flow-pol) # policy nbmflow10 switch(config-nbm-flow-pol-attr) #</pre>	Configures the NBM flow policy. You can specify a maximum of 63 alphanumeric characters for the policy name.
Step 16	(Optional) [no] policer Example: <pre>switch(config-nbm-flow-pol-attr) # no policer</pre>	<p>Enables or disables the policer for the specified NBM flow policy.</p> <p>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.</p> <p>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 the <i>Configuring Shared Policers</i> section in the <i>Configuring Policing</i> chapter of <i>Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide</i> on Cisco.com.</p>
Step 17	[no] bandwidth flow-bandwidth {kbps mbps gbps} Example: <pre>switch(config-nbm-flow-pol-attr) # bandwidth 10 mbps</pre>	Configures the flow bandwidth in Kbps, Mbps, or Gbps for multicast groups matching this policy. The minimum supported flow bandwidth is 200 Kbps.

Configuring an NBM VRF for Static Flow Provisioning

	Command or Action	Purpose	
		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 18	[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 19	[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.	
Step 20	(Optional) [no] priority critical Example: switch(config-nbm-flow-pol-attr-prop)# priority critical switch(config-nbm-flow-pol-attr-prop) #	Enables critical flow prioritization for the multicast groups that are being configured.	

What to do next

[Establishing a Flow \(Optional\)](#)

Configuring an NBM VRF for Static Flow Provisioning

You can configure an NBM VRF for static flow provisioning, which allows the NBM fabric to form a multicast flow with assistance from an external controller.

In this mode, the switch cannot accept any NBM configurations, such as flow policy or host policy. The switch does not participate in any flow-stitching decisions and strictly follows the API calls from the controller. In addition, the static flows are not saved upon reload.

If an error occurs in flow provisioning, the switch does not correct the errors and does not automatically retry the configuration.

Before you begin

Configure NBM.

Before you associate an NBM VRF, create the VRF routing context (using the **vrf context vrf-name** command) and complete the unicast routing and PIM configurations.

You can change the NBM VRF from PIM active mode to PIM passive mode only if you first delete the custom configuration under the VRF. Otherwise, the following error appears: "NBM cannot be set to PIM-PASSIVE mode while custom config exists. Please delete all custom nbm config and retry."

SUMMARY STEPS

1. **configure terminal**
2. **[no] nbm vrf *vrf-name***
3. **nbm mode pim-passive**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	[no] nbm vrf <i>vrf-name</i> Example: switch(config)# nbm vrf nbm	Creates an NBM VRF.
Step 3	nbm mode pim-passive Example: switch(config)# nbm mode pim-passive	Allows the NBM fabric to form a multicast flow with assistance from an external controller.

What to do next

See the [Cisco Nexus NX-API References](#) for API details.

Establishing a Flow (Optional)

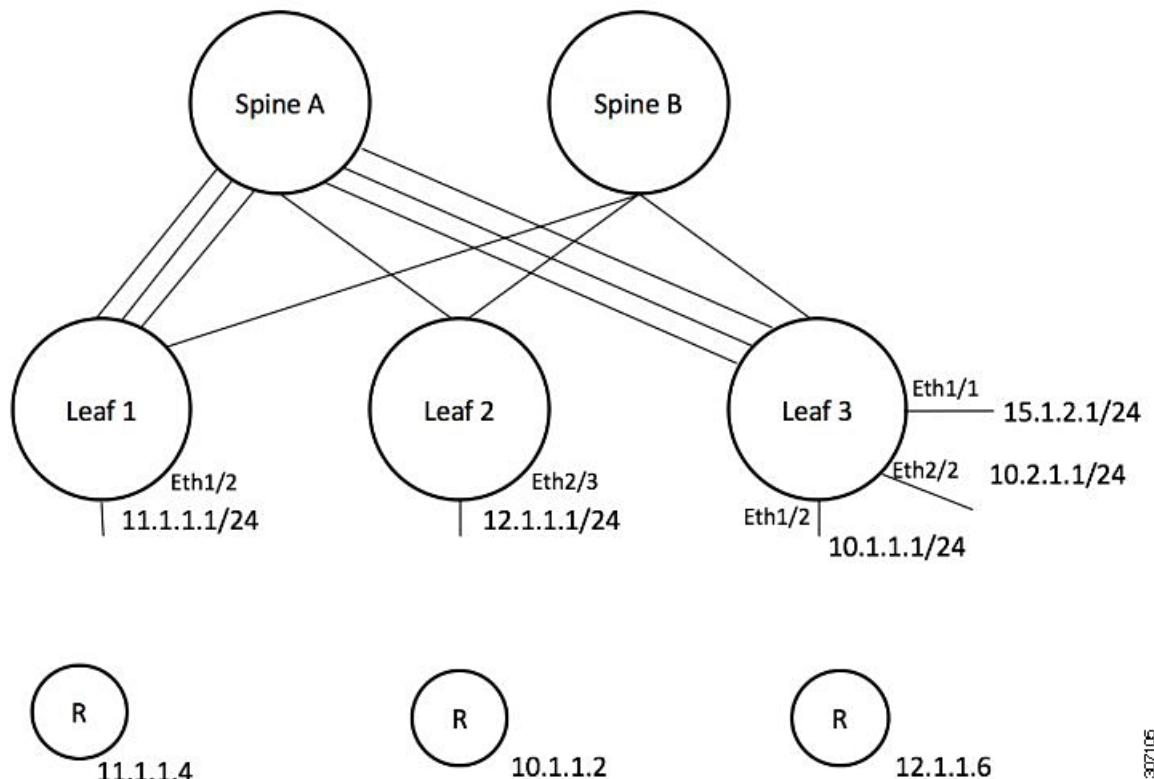
You can establish a flow by creating an NBM flow definition or configuring IGMP static OIF. We recommend configuring an NBM flow definition.

Creating an NBM Flow Definition

You can establish an NBM flow by creating an NBM flow definition.

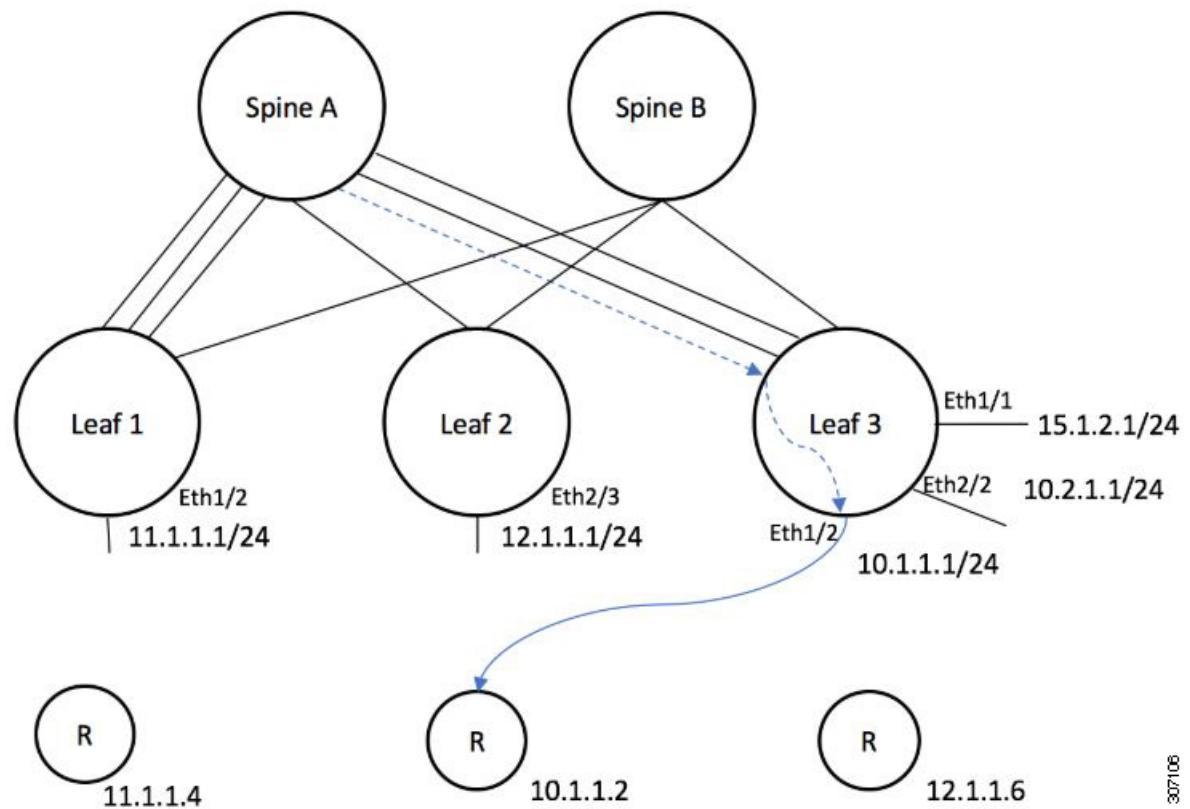
NBM exposes a CLI and an API to provision flows to receivers when they do not use IGMP to signal their interest in joining or leaving a flow. As shown in the following diagrams, you can program a flow to go all the way to the receiver leaf, in order to pre-reserve the network bandwidth, or direct the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

Figure 1: Traffic from a Source to a Leaf



307106

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: <pre>switch# configure terminal switch(config) #</pre>	Enters global configuration mode.

	Command or Action	Purpose
Step 2	[no] nbm flow-definition <i>group [source]</i> 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 <i>interface</i> 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 <i>reporter-ip-address</i> 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

You can establish a flow by configuring a static IGMP OIF, but 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 <i>interface-type slot/port</i> 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 <i>group [source source]</i> 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.

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**

Enabling Multicast and Unicast Flows (Optional)

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 team region ing-racl 256**
- **hardware access-list team 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: <pre>switch# configure terminal switch(config) #</pre>	Enters global configuration mode.
Step 2	ip access-list acl-name Example: <pre></pre>	Creates an IP ACL and enters IP ACL configuration mode.

Enabling Multicast and Unicast Flows (Optional)

	Command or Action	Purpose
	switch(config)# ip access-list pmn-ucast switch(config-acl) #	
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: switch(config-cmap-qos) # match access-group name pmn-ucast	Configures the traffic class by matching packets based on the ACL for unicast traffic.
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:	Creates a class map for multicast traffic and enters class-map configuration mode.

	Command or Action	Purpose
	switch(config)# class-map type qos match-any pmn-mcast switch(config-cmap-qos) #	
Step 12	match access-group name <i>acl-name</i> 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 <i>policy-map-name</i> 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 <i>unicast-class-map-name</i> 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 <i>multicast-class-map-name</i> 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.
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.

Verifying the NBM Configuration

	Command or Action	Purpose
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.

Command	Description
show ip mroute group-address	Displays the IP multicast routing table for the specified group.
show nbm defaults [vrf {all vrf-name}]	Displays the NBM default flow policy, host policies, and unicast fabric bandwidth.
show nbm flow-policy [policy-name] [vrf {all vrf-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 [[group-based [group group-ip] source source-ip [group group-ip] group group-ip [source source-ip] flow-policy pol-name interface if-name] [all active inactive no-receiver] [detail] [vrf {vrf-name all}]]	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 [vrf {all vrf-name}]	Displays the static flows for an NBM flow definition.
show nbm flows static group group-address	Displays the static flows for an NBM flow definition for the specified group.
show nbm flows statistics [group-based [group group-ip] source source-ip [group group-ip] group group-ip [source source-ip] flow-policy pol-name interface if-name] [vrf {all vrf-name}]	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.
show nbm flows summary [vrf {all vrf-name}]	Displays a summary of the NBM flows.
show nbm host-policy {all {receiver external receiver local sender} applied {receiver external receiver local {all interface type slot/port wildcard} sender {all interface type slot/port wildcard}} } [vrf {all vrf-name}]	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.



Note If you do not specify a VRF using the **vrf vrf-name** option, these commands display output for the routing context that you are in. You can set the routing context using the **vrf context vrf-name** command.

For sample **show** command output, see [Sample Output for Show Commands, on page 119](#).

Clearing NBM Flow Statistics

To clear NBM flow statistics, perform one of the following tasks.

<pre>clear nbm flow statistics</pre> <pre>switch# clear nbm flows statistics Clearing all NBM flow statistics for all VRFs ... Done.</pre>	<p>Clears NBM flow statistics for all VRFs.</p>
<pre>clear nbm flow statistics [source source-ip [group group-ip] group group-ip [source source-ip]] [vrf {all vrf-name}]</pre> <pre>switch# clear nbm flows statistics vrf red Clearing all NBM flow statistics for VRF 'red'... Done.</pre> <pre>switch# clear nbm flows statistics vrf all Clearing all NBM flow statistics for all VRFs ... Done.</pre>	<p>Clears NBM flow statistics for the VRF associated with the routing context you are in.</p> <p>Note Only Cisco Nexus 9504 and 9508 switches with -R line cards support the source, group, and vrf options.</p>

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: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	interface ethernet slot/port Example: <pre>switch(config)# interface ethernet 1/1 switch(config-if)#</pre>	Specifies the interface on which you are enabling unicast PTP and enters the interface configuration mode.

	Command or Action	Purpose
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

```

Configuring Unicast PTP Peers

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

Configuring Media Flow Analytics

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

- [RTP Flow Monitoring, on page 59](#)
- [Guidelines and Limitations for RTP Flow Monitoring, on page 59](#)
- [Configuring RTP Flow Monitoring, on page 60](#)
- [Displaying RTP Flows and Errors, on page 61](#)
- [Clearing RTP Flows, on page 62](#)

RTP Flow Monitoring

Real-Time Transport Protocol (RTP) is a network protocol for delivering audio and video over IP networks. It is designed for end-to-end, real-time transfer of streaming media. The protocol provides facilities for jitter compensation and detection of packet loss, which are common during UDP transmissions on an IP network.

RTP flow monitoring caches RTP flows on the switch and detects any gaps in the RTP sequence number, which indicates a loss in RTP frames. This information helps to pinpoint where the loss is occurring and enables you to better plan hardware resources.

Guidelines and Limitations for RTP Flow Monitoring

The following guidelines and limitations apply to RTP flow monitoring:

- Only Cisco Nexus 9300-FX, 9300-FX2, and 9300-FX3 platform switches support RTP flow monitoring. In addition, beginning with Cisco NX-OS 9.3(6), Cisco Nexus 9300-GX platform switches support RTP flow monitoring.
- When RTP flow monitoring is configured with an initial ACL, and then changed to a different ACL, the RTP configuration must be removed with the `no flow rtp` form of the command and then configured again with the required ACL.
- Reboot the switch after configuring UDF for RTP flow monitoring.
- You can configure only one RTP flow monitoring UDF.
- The RTP flow monitoring UDF must be the first UDF.
- Traditional NetFlow Monitor and RTP flow monitoring cannot coexist on the switch.

Configuring RTP Flow Monitoring

You can configure RTP flow monitoring for Cisco Nexus 9300-FX, 9300-FX2, and 9300-FX3 platform switches.

In addition, beginning in Cisco NX-OS 9.3(6), you can configure RTP flow monitoring for Cisco Nexus 9300-GX platform switches.

Before you begin

Enable UDF for RTP flow monitoring using the **udf netflow_rtp netflow-rtp** command, copy the running configuration to startup, and reboot the switch. Make sure that the RTP flow monitoring UDF is the first UDF.

SUMMARY STEPS

1. **configure terminal**
2. **[no] feature netflow**
3. (Optional) **ip access-list acl**
4. **[no] {ip | ipv6} flow rtp [acl]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	[no] feature netflow Example: switch(config)# feature netflow	Enables RTP flow monitoring globally on the switch.
Step 3	(Optional) ip access-list acl Example: ip access-list ipv4-test-acl 10 permit ip any 224.0.1.39/32 20 permit ip any 224.0.1.40/32	Configures an ACL policy to filter any specific traffic.
Step 4	[no] {ip ipv6} flow rtp [acl] Example: switch(config)# ip flow rtp	Enables RTP flow monitoring for IPv4 or IPv6 flows. • This command also creates a system-wide access control list (ACL) to filter the UDP port range of 16384 to 32767. This range is the RFC standard UDP port range for RTP traffic. Note The ignore routable command filters any multicast traffic. switch(config)# show ip access-list IP access list nfm-rtp-ipv4-acl

Command or Action	Purpose
	<pre>ignore routable 10 permit udp any any range 16384 32767</pre> <p>Note When an ACL is specified in the command, only traffic that matches the specified ACL is reported as RTP flows.</p> <pre>switch(config)# ip flow rtp ipv4-test-acl</pre>

Displaying RTP Flows and Errors

To display the RTP flows and errors, perform one of the following tasks.

show flow rtp details	Displays all IPv4 and IPv6 RTP flows.
show flow rtp details {ipv4 ipv6}	Displays either IPv4 or IPv6 RTP flows.
show flow rtp errors active	Displays details of all RTP flows that are currently experiencing losses (if the packet loss is detected in at least one update interval within the last 10 seconds). The loss statistics for the active loss window are also displayed. Because the loss window is still considered active, the loss end time shows as "N/A."
show flow rtp errors history	Displays details of the last 1000 historical loss windows (in reverse chronological order) and their respective flow details.

The following example shows sample output for the **show flow rtp details** command:

```
RTP Flow timeout is 1440 minutes
IPv4 Entries
SIP          DIP          BD ID S-Port D-Port Intf/Vlan Name   Packet Count BytesPerSec  FlowStart
50.1.1.2 20.1.1.2 4151  16385  17999  Ethernet1/49/1    269207033      594468000  00:21:16
PST Apr 07 2019
20.1.1.2 50.1.1.2 4100  16385  18999  port-channel1500 2844253       199000        00:21:59
PST Apr 07 2019

IPv6 Entries
SIP          DIP          BD ID S-Port D-Port Intf/Vlan Name   Packet Count BytesPerSec  FlowStart
20::2        50::2        4100  30000  31999  port-channel1500 2820074       199000        00:22:04
PST Apr 07 2019
50::2        20::2        4151  30000  31999  Ethernet1/49/1   3058232       199000        00:21:16
```

Clearing RTP Flows

PST Apr 07 2019

The following example shows sample output for the **show flow rtp errors active** command:

```
RTP Flow timeout is 1440 minutes
IPV4 Entries
SIP          DIP          BD ID    S-Port   D-Port   Intf/Vlan Name      Packet Count
  BytesPerSec  FlowStart           Packet Loss Loss Start          Loss End
30.30.1.2    20.20.1.2    4197     30000   20392   Ethernet1/98        200993031
  10935633    20:23:15 UTC May 30 2019 1558          03:48:32 UTC May 31 2019 N/A
20.20.1.2    30.30.1.2    4196     30000   20392   Ethernet1/97        204288988
  11114959    20:23:15 UTC May 30 2019 222          03:48:30 UTC May 31 2019 N/A
```



Note When an RTP flow enters the “active-errored” state, the following syslog message appears:

```
%NFM-1-RTP_FLOW_ERROR_DETECTED: Flow SIP: 30.30.1.2 DIP: 20.20.1.2 Interface: Ethernet1/98
loss detected
```

The following example shows sample output for the **show flow rtp errors history** command:

```
RTP Flow timeout is 1440 minutes
IPV4 Entries
SIP          DIP          BD ID    S-Port   D-Port   Intf/Vlan Name      Packet Count
  BytesPerSec  FlowStart           Packet Loss Loss Start          Loss End
20.20.1.2    30.30.1.2    4196     30000   20392   Ethernet1/97        204187441
  11122753    20:23:15 UTC May 30 2019 2061          03:47:57 UTC May 31 2019 03:47:57
UTC May 31 2019
30.30.1.2    20.20.1.2    4197     30000   20392   Ethernet1/98        199495510
  10937237    20:23:15 UTC May 30 2019 1882          03:45:06 UTC May 31 2019 03:45:06
UTC May 31 2019
20.20.1.2    30.30.1.2    4196     30000   20392   Ethernet1/97        202753418
  11116269    20:23:15 UTC May 30 2019 4976          03:45:05 UTC May 31 2019 03:45:05
UTC May 31 2019
20.20.1.2    30.30.1.2    4196     30000   20392   Ethernet1/97        202630465
  11123369    20:23:15 UTC May 30 2019 2139          03:44:32 UTC May 31 2019 03:44:32
UTC May 31 2019
30.30.1.2    20.20.1.2    4197     30000   20392   Ethernet1/98        197973969
  10938370    20:23:15 UTC May 30 2019 1854          03:41:41 UTC May 31 2019 03:41:41
UTC May 31 2019
```



Note When an RTP flow is no longer in the “active-errored” state, the following syslog message appears:

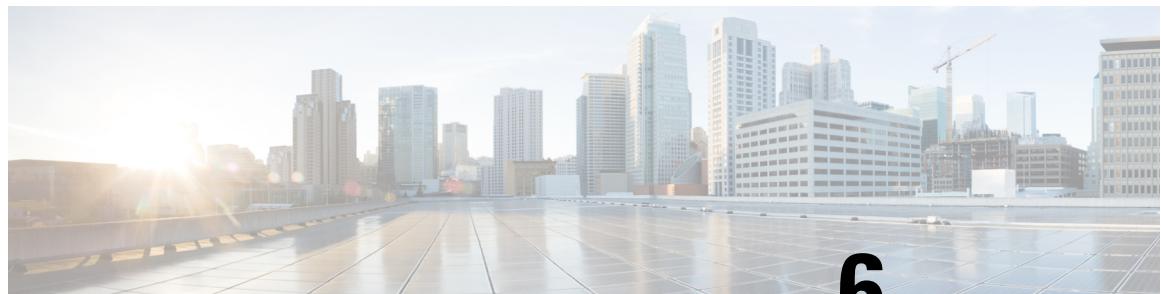
```
%NFM-1-RTP_FLOW_ERROR_STOP: Flow SIP: 30.30.1.2 DIP: 20.20.1.2 Interface: Ethernet1/98 loss
no longer detected
```

Clearing RTP Flows

To clear RTP flows, perform one of the following tasks.

clear flow rtp detail	Clears all RTP flows and loss histories.
------------------------------	--

clear flow rtp detail {ipv4 ipv6}	Clears either IPv4 or IPv6 RTP flows and loss histories.
[no] flow rtp timeout value Example: <pre>switch(config)# flow rtp timeout 100</pre>	Clears non-active RTP flows from the show rtp details , show flow rtp errors active , and show flow rtp errors history tables. The default value is 1440 minutes (24 hours), and the range is from 0 to 1440 minutes. A value of 0 prevents RTP flows from being cleared. Note This command does not clear active RTP flows.



CHAPTER 6

Configuring Multicast Service Reflection with NBM

This chapter describes how to configure the Cisco Nexus 9000 Series switches for Cisco's Multicast Service Reflection with NBM.

- [Multicast Service Reflection with NBM, on page 65](#)

Multicast Service Reflection with NBM

Multicast Service Reflection with NBM enables the users to translate externally received multicast destination addresses to addresses that conform to their organization's internal addressing policy. It is the multicast network address translation (NAT) of an ingress multicast stream (S1,G1) to an egress (S2,G2) interface. This feature is commonly referred to as the multicast service reflection feature (SR feature). Unlike IP multicast Network Address Translation (NAT), which only translates the source IP address, the multicast service reflection translates both the source and destination addresses.

The flow incoming as S1, G1 is translated to S2, G2 and the destination MAC address is re-written to the multicast MAC address of G2.

The S1, G1 flow is translated to S2, G2 and the destination MAC address is not re-written and remains corresponding to group G1.

For more information and commands regarding the Multicast Service Reflection feature, see the [Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide](#).



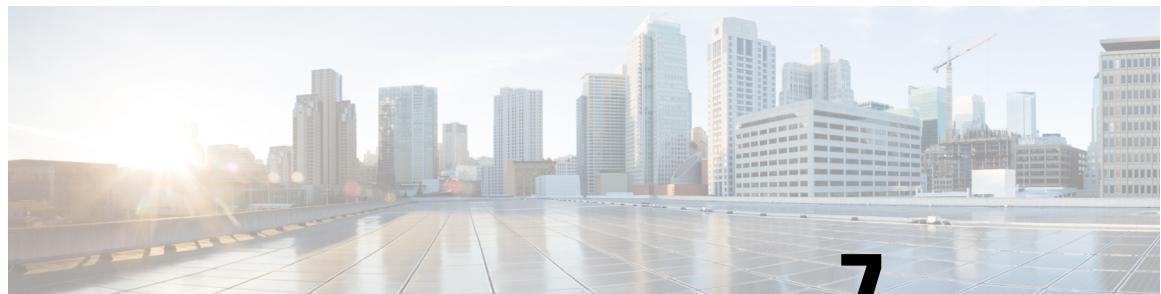
Note If NBM determines that the traffic flow cannot be supported, such as the required bandwidth is not available, the traffic flow is stopped and an alert is issued stating that NBM cannot support the requested translation.



Note Multicast Service Reflection with NBM is supported on Cisco Nexus 9316D-GX, Cisco Nexus 9364C-GX, Cisco Nexus 93600CD-GX, and Cisco Nexus 93180YC-FX3S switches (Cisco Nexus NX-OS 9.3(5) and later releases).

**Note**

Beginning with Cisco Nexus Release 10.1(1), Multicast Service Reflection with NBM is supported on Cisco Nexus 9300-FX3, Cisco Nexus C9316D-GX, Cisco Nexus C93600CD-GX, and Cisco Nexus C9364C-GX platform switches.



CHAPTER 7

Media Controller

This section describes the DCNM Media Controller.



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



Note

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

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



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 ptpt brief"
        path "show ptpt parent"
sensor-group 301
    data-source NX-API
        path "show ptpt corrections"
sensor-group 500
    data-source NX-API
        path "show flow rtp details" depth 0
        path "show flow rtp errors active" depth 0
        path "show flow rtp errors history" depth 0
sensor-group 400
    data-source DME
        path sys/nbm/show/faults depth unbounded
        path sys/nbm/show/notify depth unbounded
subscription 201
    dst-grp 200
        snsgr-grp 200 sample-interval 60000
        snsgr-grp 201 sample-interval 30000
        snsgr-grp 205 sample-interval 30000
subscription 202
    dst-grp 200
        snsgr-grp 202 sample-interval 30000
subscription 203
    dst-grp 200
        snsgr-grp 203 sample-interval 30000
subscription 204

```

```

dst-grp 200
snsr-grp 204 sample-interval 30000
subscription 300
dst-grp 200
snsr-grp 300 sample-interval 30000
snsr-grp 301 sample-interval 30000
subscription 500
dst-grp 200
snsr-grp 500 sample-interval 30000
subscription 400
dst-grp 200
snsr-grp 400 sample-interval 0

```

Scope in Media Controller

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

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

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

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

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



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

- [Generic Multicast Monitoring, on page 69](#)
- [Topology, on page 72](#)
- [Host, on page 72](#)
- [Flow, on page 86](#)
- [RTP, on page 102](#)
- [Global, on page 104](#)
- [Config, on page 106](#)
- [DCNM Read-Only Mode for Media Controller, on page 115](#)

Generic Multicast Monitoring

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

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

Enabling Generic Multicast Mode

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

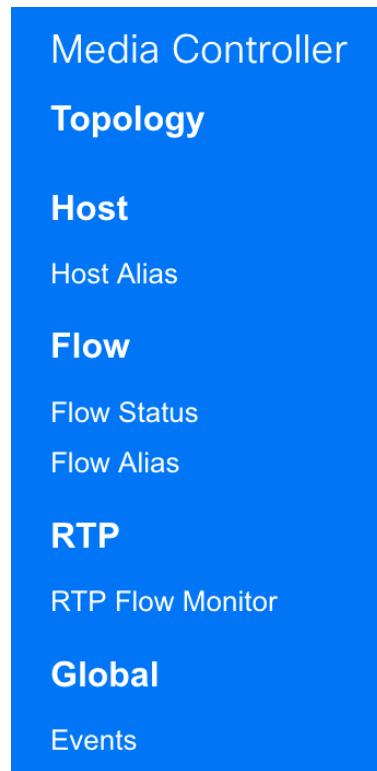
For a DCNM HA mode, set the **pmn.generic-multicast.enabled** server property to **true** and click **Failover** in the **Administration / DCNM Server / Native HA** window. The new DCNM active comes up in the generic multicast mode.

**Note**

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

Generic Multicast Menu

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



NX-OS Streaming Telemetry and DCNM (Generic Multicast)

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

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

Topology

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



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

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



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

Quick Search

Enter the search string to highlight relevant devices.

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

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

Multicast Group

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

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

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

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 4. Discovered Host Table Fields and Description

Field	Description
VRF	Specifies the VRF instance.
Host Name	Specifies the configured Host Alias for the host IP address. The Host IP is displayed if the Host Alias is not configured.
Role	Specifies the role of the host device. The role of the host can be one of the following: <ul style="list-style-type: none"> • 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).
DCNM Discovered Time	Specifies the date and time at which the switch discovered the host.
Fault Reason	Specifies the failure reason for the flow that the discovered host has participates in.

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



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

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 5: Host Alias Table Field and Description

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

This section contains the following:

Add Host Alias

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

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 6: Host Policies Operations

Field	Description
Add	Allows you to add a new host policy.
Edit	Allows you to view or edit the selected host policy parameters.

Field	Description
Delete	<p>Allows you to delete the user-defined host policy.</p> <p>Note</p> <ul style="list-style-type: none"> 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	<p>Allows you to delete all custom policies without selecting any policy check box.</p> <p>Note</p> <ul style="list-style-type: none"> 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	<p>Allows you to import host policies from a CSV file to DCNM.</p> <p>Note</p> <p>After import, all policies imported from a CSV file are applied to all managed switches automatically.</p>
Export	Allows you to export host policies from DCNM to a CSV file.

Field	Description
Deployment	

Field	Description
	<p>From the Deployment drop-down list, select an appropriate value.</p> <ul style="list-style-type: none"> • Deploy <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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. <p>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.</p> <ul style="list-style-type: none"> • Deployment History—Select one policy from the drop-down list. Select this option to view the deployment history of the selected policy. <p>Deployment History shows the following fields.</p> <ul style="list-style-type: none"> • 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 <i>Day MMM DD YYYY HH:MM:SS Timezone</i>. • Failed Reason—Specifies why the policy was not

Field	Description
	successfully deployed.

Table 7: 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: <ul style="list-style-type: none"> • Sender • Receiver-External • Receiver-Local
Operation	Specifies if the operation of the host policy. The policy has the following operations: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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 <i>Day MMM DD YYYY HH:MM:SS Timezone</i> .

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.

Edit Host 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.



Note You cannot undeploy the default configured policies.



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

Redo All Failed Custom Policies

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

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

Deployment History

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

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

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

Deployment History table shows the following fields.

Table 8: Policy Deployment History Table Field and Descriptions

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

Applied Host Policies

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 9: 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: <ul style="list-style-type: none">• 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.

Column Name	Description
Time Stamp	Specifies the date and time at which the policy was created\deployed. The format is Day, MMM DD YYYY HH:MM:SS (Timezone).

Flow

The Flow menu includes the following submenus:

Flow Status



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

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

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

Fields and Descriptions

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

Table 10: Active Tab

Field	Description
Common Fields for IPFM and Generic Multicast Modes	
Multicast IP	Specifies the multicast IP address for the flow. Note You can click the wave link next to the Multicast IP address to view the pictorial representation of flow statistics.
Flow Alias	Specifies the name of the Flow Alias.
Sender	Specifies the IP Address or the Host alias of the sender for the multicast group.
Sender Switch	Specifies if the Sender switch is a leaf or spine.
Sender Interface	Specifies the interface to which the sender is connected to.
Receiver Switch	Specifies if the Receiver switch is a leaf or spine.
Receiver Interface	Specifies the interface to which the receiver is connected to.

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

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

Table 11: Inactive Tab

Field	Description
Common Fields for IPFM and Generic Multicast Modes	
Multicast IP	Specifies the multicast IP address for the flow. Note You can click the wave link next to the Multicast IP address to view the pictorial representation of flow statistics.
Flow Alias	Specifies the name of the Flow Alias.
Sender	Specifies the IP Address or the Host alias of the sender for the multicast group.
Sender Start Time	Displays the time from when the sender joined.
Receiver Join Time	Specifies the time at which the receiver joined.
Fields Specific for IPFM Mode	
Priority	Specifies the flow priority for flows.
Policed	Specifies whether a flow is policed or not policed.
Receiver	Specifies the IP Address or the Host alias of the receiver joining the group.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.
QOS/DSCP	Specifies the Switch-defined QoS Policy.

Policy ID	Specifies the policy ID applied to the multicast IP.
Fault Reason	<p>Specifies reason for the inactive flow.</p> <p>Cisco DCNM determines the inactive flow if both the sender and receiver mroute exists with any of the following combinations.</p> <ul style="list-style-type: none"> • Receiver IIF is null • Receiver OIF is null • Sender IIF is null • Sender OIF is null <p>In this scenario, the switch will not have any fault reason. Therefore, there is no fault reason for such inactive flows.</p>
Field Specific for Generic Multicast Mode	
Receiver Interface IP	Specifies the IP address of the receiver interface joining the group.

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

Table 12: Sender Only Tab

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

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

Table 13: Receiver Only Tab

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

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



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

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



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

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.

Add Flow Alias**Table 14: Flow Alias Table Field and Description**

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

This section contains the following:

Add Flow Alias

To add flow alias from the Cisco 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**.

Flow Policies

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 15: 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 <ul style="list-style-type: none"> • You cannot delete the default flow policies. • Undeploy policies from all switches before deleting them from DCNM.

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

Field	Description
Deployment	

Field	Description
	<p>From the Deployment drop-down list, select an appropriate value.</p> <ul style="list-style-type: none"> • Deploy <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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. <p>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.</p> <ul style="list-style-type: none"> • Deployment History—Select one policy from the drop-down list. Select this option to view the deployment history of the selected policy. <p>Deployment History shows the following fields.</p> <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • Create—Implies that the policy has been deployed on the switch.

Field	Description
	<ul style="list-style-type: none"> • 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 <i>Day MMM DD YYYY HH:MM:SS Timezone</i>. • Failed Reason—Specifies why the policy was not successfully deployed.

Table 16: 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	Specifies if the flow policy is deployed successfully or failed.
Deployment Action	<p>Specifies the action that is performed on the switch for that host policy.</p> <ul style="list-style-type: none"> • 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	<p>Specifies whether the policer for a flow policy is enabled or disabled.</p> <p>Note In adding or editing a flow policy, the default policer state is Enabled.</p>
Last Updated	<p>Specifies the date and time at which the flow policy was last updated.</p> <p>The format is <i>Day MMM DD YYYY HH:MM:SS Timezone</i>.</p>



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 one 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 policer for a new flow policy is enabled.

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

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

Step 7 From the **Flow Priority** drop-down list, choose the priority for the flow. You can choose either **Low** or **Critical**. The default value is **Low**.

The flow priority is used during the following scenarios:

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

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

Step 8 Click **Deploy** to deploy the new policy.

Edit Flow 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. From the **Flow Priority** drop-down list, choose the priority for the flow. You can choose either **Low** or **Critical**. The default value is **Low**.
7. Click **Deploy** to deploy the new policy.

DETAILED STEPS

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

The **Flow Policies** window is displayed.

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

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

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

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

Step 6 From the **Flow Priority** drop-down list, choose the priority for the flow. You can choose either **Low** or **Critical**. The default value is **Low**.

The flow priority is used during the following scenarios:

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

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

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

Click **Cancel** to discard the changes.

Delete Flow Policy

To delete flow policy from the Cisco 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.

Export Flow Policy

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.



Note You cannot undeploy the default configured policies.



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

Redo All Failed Custom Policies

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

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

Deployment History

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

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

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

Deployment History table shows the following fields.

Table 17: Policy Deployment History Table Field and Descriptions

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

RTP



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

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

RTP Flow Monitor

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



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

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

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

The description of the fields in these tabs are:

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

Field	Description
Protocol	Specifies the protocol that is being used for the flow.

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

Active

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

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

Packet Drop

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

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

Flow Topology

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

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

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

The switches experiencing packet drops are circled in red.

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

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

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

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

Drop History

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



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

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

For information about the AMQP based notifications, see [Cisco DCNM IP for Media Deployment - AMQP Notifications](#) and for information about REST APIs, see [Cisco DCNM API Reference Guide](#).

Global

The Global menu includes the following submenus:

Events



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

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	<p>Click to remove the old/unwanted events.</p> <p>Note If the DCNM server restarts, by default a maximum of 5000 event entries are retained for 6 hours.</p> <p>Click one of the radio buttons to choose the Purge options.</p> <ul style="list-style-type: none"> • 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. <p>Click Purge to delete/retain PMN events information.</p>
Category	Specifies if the event category.
Severity	Specifies the severity of the event.

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

Copying Switch Running Configuration to Start-up Configuration

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

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

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

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

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

Realtime Notifications

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

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

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

For AMQP, you should create a queue to get the event. You should bind this queue to an exchange. In this case, it's **DCNMEExchange**. Use this routing key to get real-time notifications:
error.com.cisco.dcnm.event.pmn.realtime.switch.

Threshold Notifications

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

Threshold Notifications

DCNM generates threshold notifications in the following scenarios:

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

The notification is deleted when the condition is resolved.

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

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

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

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

Config

The Config menu includes the following submenus:

Setting Up the SNMP Server for 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 109](#).
-

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)

Key Identifier	Details
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	<p>List of name-value pairs about the message.</p> <ul style="list-style-type: none"> • 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 107](#).

Unicast Bandwidth Reservation

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

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

Reserve Bandwidth to Receiver Only

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

ASM Range

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

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

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

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

Table 18: Operations on the Global Config screen

Icon	Description
Save	Click Save to save the configurations.
Deploy	<p>To deploy the configuration, you can choose one of the following from the drop-down list:</p> <ul style="list-style-type: none"> • All—Deploys ASM, unicast bandwidth, and reserved bandwidth configuration to all switches. • Unicast BW—Deploys only unicast bandwidth configuration. • Reserve BW—Deploys only the reserve bandwidth configuration. • ASM—Deploys only the ASM configuration. • All Failed—Deploys all failed deployments. <p>Success or Failed message appears next to each of the ASM range in the table.</p>

Icon	Description
Undeploy	To undeploy the configuration, you can choose one of the following from the drop-down list: <ul style="list-style-type: none"> • All—Undeploys ASM, unicast bandwidth, and reserved bandwidth configuration to all switches. • Unicast BW—Undeploys only unicast bandwidth configuration. • Reserve BW—Undeploys only the reserve bandwidth configuration. • ASM—Undeploys only the ASM configuration.
Status	Bandwidth reservation status specifies if the bandwidth deployment was success, or failed or not deployed. ASM/Mask Status field displays if the ASM and Mask configuration was deployed successfully, or failed or not deployed.
History	Click the respective History link to view the deployment history for Unicast Bandwidth and ASM deployments.

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

Table 19: 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	<p>From the drop-down list, choose an appropriate filter.</p> <ul style="list-style-type: none"> 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. <p>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.</p> <ul style="list-style-type: none"> All - This removes all the filters and displays the complete deployment history. Manage Preset Filters - Select an appropriate filter from the drop-down list. <p>Click Edit to modify the filter parameters. Click Remove to delete the filter. Click Cancel to discard the changes and revert to Deployment History.</p>
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.

- 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 20: 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.
WAN Links	From the drop-down, list you can choose to designate this interface as a WAN link. <ul style="list-style-type: none"> • 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 21: Deployment History Field and Description

Field	Description
Switch Name	Specifies the switch name in the fabric on which the configuration was deployed.
Action	Specifies the action that is performed on the switch - Deploy or Undeploy .
Deployment Status	Displays the status of deployment. It shows if the deployment was Success or Failed.
Deployment Date/Time	Displays the date and time when the deployment was initialized.
Failed Reason	Specifies the reason why the deployment failed.
Show	<p>From the drop-down list, choose an appropriate filter.</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <ul style="list-style-type: none"> • All - This removes all the filters and displays the complete deployment history. • Manage Preset Filters - Select an appropriate filter from the drop-down list. <p>Click Edit to modify the filter parameters. Click Remove to delete the filter. Click Cancel to discard the changes and revert to Deployment History.</p>
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.

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

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

We recommend that you to take a decision to use 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.

Host Policies - DCNM Read-Only Mode

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

Table 22: Host Policies Table Field and Description

Field	Description
VRF	Specifies the VRF instance on the switch where the policy is defined.
Sequence #	Specifies the sequence number of the policy. This field displays 20000000 for default host policies.
Host Name	Specifies the host ID.
Receiver	Specifies the IP address of the receiving device.
Multicast IP / Mask	Specifies the multicast IP address and mask for the host.
Sender	Specifies the IP Address of the sender.
Host Role	Specifies the host device role. The host device role is one of the following: <ul style="list-style-type: none"> • Sender • Receiver-External • Receiver-Local
Operation	Specifies if the operation of the host policy. The policy has the following operations: <ul style="list-style-type: none"> • Permit • Deny
Last Updated	Specifies the date and time at which the host policy was last updated. The format is <i>Day MMM DD YYYY HH:MM:SS Timezone</i> .

Flow Policies - DCNM Read-Only Mode

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

Table 23: 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.

Field	Description
Policer	Specifies whether the policer for a flow policy is enabled or disabled.
Last Updated	Specifies the date and time at which the flow policy was last updated. The format is <i>Day MMM DD YYYY HH:MM:SS Timezone</i> .

Switch Global Config - Read-Only Mode

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

WAN Links - Read-Only Mode

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

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

Table 24: WAN Links Table Field and Description

Field	Description
Interface Name	Specifies the interface which is connected as a WAN link to the end device.
Admin Status	An up arrow depicts that the status is up. A down arrow implies that the status is down.
Oper Status	An up arrow depicts that the operational state of the interface is up. A down arrow implies that the status is down.
WAN Links	From the drop-down, list you can choose to designate this interface as a WAN link. <ul style="list-style-type: none"> • Select Yes to configure the interface as a WAN link. • Select No to remove the interface as a WAN link.
Deployment Status	Specifies if the interface is deployed as a WAN link or not.



APPENDIX A

Sample Output for Show Commands

This appendix provides output examples for IP fabric for media **show** commands.

- [Sample Show Command Output \(Spine-Leaf Deployment\), on page 119](#)
- [Sample Show Command Output \(Single Modular Switches\), on page 134](#)

Sample Show Command Output (Spine-Leaf Deployment)

This section provides output examples for switches in a spine-leaf deployment.



Note If you do not specify a VRF using the **vrf vrf-name** option, these commands display output for the default VRF.

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

```
switch# show nbm defaults vrf all
-----
Defaults for VRF default (1)
-----
Default Flow Policy:
Bandwidth          : 1000 Kbps
DSCP              : 0
Queue ID          : 7
Policer            : Enabled
Operation mode (cache) : EOR_PIM_A
Operation mode      : EOR_PIM_A
Unicast Fabric Bandwidth : 1
Number of ASM groups : 1
Group 1 : 224.0.0.0/8

Default Host Policies:
Sender             : Permit
Local Receiver     : Permit
External Receiver (PIM) : Permit
-----
Defaults for VRF red (3)
-----
```

Sample Output for Show Commands

Default Flow Policy:

```
Bandwidth : 1500 Kbps
DSCP : 0
Queue ID : 7
Policer : Enabled
Operation mode (cache) : EOR_PIM_A
Operation mode : EOR_PIM_A
Unicast Fabric Bandwidth : 1
Number of ASM groups : 1
Group 1 : 224.0.0.0/8
```

Default Host Policies:

```
Sender : Permit
Local Receiver : Permit
External Receiver (PIM) : Permit
```

This example shows sample output for the **show nbm flow-policy vrf all** command:

```
switch# show nbm flow-policy vrf all
Flow Policy for VRF 'blue'
-----
Total Group Ranges Found = 0
Total Policies Defined = 0

Flow Policy for VRF 'default'
-----
Default BW (Kbps) : 1890
Default DSCP : 36
Default QOS : 7
Default Policer : Enabled

-----
| Group Range | BW (Kbps) | DSCP | QOS | Policer | Policy Name
-----
| 235.1.1.1-235.1.2.255 | 30 | 0 | 7 | Enabled | Dynamic_IGMP
| 238.4.1.1-238.4.1.1 | 3000000 | 0 | 7 | Enabled | NBM_Static_2
| 238.4.1.2-238.4.1.10 | 3000000 | 0 | 7 | Enabled | NBM_Static_2
| 238.4.1.11-238.4.1.11 | 3000000 | 0 | 7 | Enabled | NBM_Static_2
| 238.4.1.12-238.4.1.100 | 3000000 | 0 | 7 | Enabled | NBM_Static_2
| 238.4.1.101-238.4.1.255 | 3000000 | 0 | 7 | Enabled | NBM_Static_2
| 239.1.1.2-239.1.1.2 | 100 | 0 | 7 | Disabled | SVI_239
| 239.1.1.3-239.1.1.9 | 100 | 0 | 7 | Disabled | SVI_239
| 239.1.1.10-239.1.1.10 | 100 | 0 | 7 | Disabled | SVI_239
| 239.1.1.11-239.1.1.30 | 100 | 0 | 7 | Disabled | SVI_239
| 239.1.1.1-239.1.1.1 | 200 | 0 | 7 | Enabled | SVI_239.1.1.1
| 227.1.1.51-227.1.1.51 | 1000 | 0 | 7 | Enabled | Dynamic_227.1
| 227.1.1.52-227.1.1.200 | 1000 | 0 | 7 | Enabled | Dynamic_227.1
| 229.1.1.1-229.1.1.100 | 1000 | 0 | 7 | Disabled | NBM_229
| 234.1.1.1-234.1.1.100 | 30 | 0 | 7 | Disabled | NBM_234
| 234.1.1.101-234.1.1.200 | 30 | 0 | 7 | Disabled | NBM_234
| 237.1.1.1-237.1.1.200 | 3000 | 0 | 7 | Disabled | NBM_Static_237.1
| 237.1.2.1-237.1.2.200 | 3000 | 0 | 7 | Disabled | NBM_Static_237.1
...
| 237.1.1.201-237.1.1.255 | 3000 | 0 | 7 | Enabled | NBM_Static_237_2
| 237.1.2.201-237.1.2.255 | 3000 | 0 | 7 | Enabled | NBM_Static_237_2
| 237.1.3.201-237.1.3.255 | 3000 | 0 | 7 | Enabled | NBM_Static_237_2
| 237.1.4.201-237.1.4.255 | 3000 | 0 | 7 | Enabled | NBM_Static_237_2
```

```

| 232.1.1.9-232.1.1.200 | 200 | 0 | 7 | Enabled | NBM_Static_232_2
| 232.1.1.5-232.1.1.7 | 200 | 0 | 7 | Enabled | NBM_Static_232_2
| 232.1.1.8-232.1.1.8 | 200 | 0 | 7 | Enabled | NBM_Static_232_2
| 235.2.2.2-235.2.2.10 | 3000000 | 24 | 7 | Disabled | Test_R_V
-----
```

```

Total Group Ranges Found = 56
Total Policies Defined = 16
```

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

```

switch# show nbm flows detail vrf all
-----
NBM Flows for VRF 'default'
-----
Active Source-Group-Based Flow(s) :

Mcast-Group      Src-IP          Uptime   Src-Intf      Nbr-Device      LID Profile
Status  Num Rx Bw Mbps    CFG Bw Slot Unit Slice DSCP QOS Policed FHR Policy-name
Rcvr-Num Rcvr-slot Unit      Num-Rcvrs     Rcvr-ifidx  IOD Rcvr-Intf  Nbr-Device
-----
NBM Flows for VRF 'red'
-----
Active Source-Group-Based Flow(s) :

Mcast-Group      Src-IP          Uptime   Src-Intf      Nbr-Device      LID Profile
Status  Num Rx Bw Mbps    CFG Bw Slot Unit Slice DSCP QOS Policed FHR Policy-name
Rcvr-Num Rcvr-slot Unit      Num-Rcvrs     Rcvr-ifidx  IOD Rcvr-Intf  Nbr-Device
-----
225.1.1.11      10.1.4.2        00:00:11  Vlan100    not-applicable * *
ACTIVE      0    1.500      1.500    0    0    0    7 Yes      Yes Default
225.1.7.228     10.1.4.2        00:00:12  Vlan100    not-applicable * *
ACTIVE      0    1.500      1.500    0    0    0    7 Yes      Yes Default
225.1.6.193     10.1.4.2        00:00:12  Vlan100    not-applicable * *
ACTIVE      0    1.500      1.500    0    0    0    7 Yes      Yes Default
...
225.1.19.52     10.2.3.2        00:02:13  Eth1/31    gretta-r10-eor2  349  962
ACTIVE      1    1.500      1.500    1    5    0    0    7 Yes      Yes Default
1           0    0           1           0x09010064  2 Vlan100    not-applicable
225.1.23.31     10.2.3.2        00:35:04  Eth1/31    gretta-r10-eor2  1119  962
ACTIVE      1    1.500      1.500    1    5    0    0    7 Yes      Yes Default
1           0    0           1           0x09010064  2 Vlan100    not-applicable
...
225.1.0.23      10.1.4.2        02:20:38  Vlan100    not-applicable * *
ACTIVE      1    1.500      1.500    0    0    0    0    7 Yes      Yes Default
1           1    5           1           0x1a003c00  48 Eth1/31    gretta-r10-eor2
225.1.0.10      10.1.4.2        02:20:38  Vlan100    not-applicable * *
ACTIVE      1    1.500      1.500    0    0    0    0    7 Yes      Yes Default
1           1    5           1           0x1a003e00  49 Eth1/32    gretta-r10-eor2
...
225.1.0.3       10.1.4.2        02:20:38  Vlan100    not-applicable * *
ACTIVE      1    1.500      1.500    0    0    0    0    7 Yes      Yes Default
1           1    5           1           0x1a003c00  48 Eth1/31    gretta-r10-eor2
```

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

Sample Output for Show Commands

```

switch# show nbm flows static vrf all
+-----+
| NBM Static Flow Table for VRF "default"
+-----+
+-----+
| NBM Static Flow Table for VRF "moon"
+-----+
+-----+
|   Stitched Flows
+-----+
| Source      | Group        | Egress Intf    | Host IP
+-----+
| 22.7.1.2    | 233.10.1.1   | Null0          |
|             |               | eth6/20/3      |
|             |               | eth6/20/3      | 21.7.1.2
| 22.7.1.2    | 233.10.1.2   | Null0          |
|             |               | eth6/20/3      |
|             |               | eth6/20/3      |
| 22.7.1.2    | 233.10.1.3   | Null0          |
|             |               | eth6/20/3      |
|             |               | eth6/20/3      | 21.7.1.2
| 22.7.1.2    | 233.10.1.4   | Null0          |
|             |               | eth6/20/3      |
|             |               | eth6/20/3      | 21.7.1.2
...
| 0.0.0.0     | 233.80.1.149 | Null0          |
|             |               | eth6/20/3      |
|             |               | eth6/20/3      | 21.7.1.2
| 0.0.0.0     | 233.80.1.150 | Null0          |
|             |               | eth6/20/3      |
|             |               | eth6/20/3      | 21.7.1.2
+-----+
+-----+
|   Unstitched Flows
+-----+
| Source      | Group        | Egress Intf   | Host IP
+-----+
| 0.0.0.0     | 233.80.1.1   |           |
|             |               | vlan851        |
+-----+

```

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

```

switch# show nbm flows statistics vrf all
-----
NBM Flow Statistics for VRF 'default'
-----
Source-Group-Based Flow Statistics  :

Mcast-Group      Src-IP          Uptime      Src-Intf  Packets      Bytes
Allow-Bytes       Drop-Bytes

-----
NBM Flow Statistics for VRF 'red'
-----
Source-Group-Based Flow Statistics  :

```

Mcast-Group	Src-IP	Uptime	Src-Intf	Packets	Bytes
Allow-Bytes	Drop-Bytes				
225.1.2.47	10.2.3.2	02:29:53	Eth1/32	1124095	1124095000
1124095000	0				
225.1.2.45	10.2.3.2	02:29:53	Eth1/31	1124096	1124096000
1124096000	0				
225.1.2.44	10.2.3.2	02:29:53	Eth1/32	1124096	1124096000
1124096000	0				
225.1.2.43	10.2.3.2	02:29:53	Eth1/31	1124096	1124096000
1124096000	0				
...					
225.1.2.2	10.2.2.2	02:29:53	Eth1/32	1124115	1124115000
1124115000	0				
225.1.2.1	10.2.2.2	02:29:53	Eth1/31	1124114	1124114000
1124114000	0				
225.1.0.2	10.1.4.2	02:30:13	Vlan100	1125105	1125105000
1125105000	0				
225.1.0.1	10.1.4.2	02:30:13	Vlan100	1125104	1125104000
1125104000	0				
225.1.0.24	10.1.4.2	02:30:13	Vlan100	1125104	1125104000
1125104000	0				
225.1.0.23	10.1.4.2	02:30:13	Vlan100	1125103	1125103000
1125103000	0				
225.1.0.22	10.1.4.2	02:30:13	Vlan100	1125104	1125104000
1125104000	0				
225.1.0.21	10.1.4.2	02:30:13	Vlan100	1125103	1125103000
1125103000	0				
225.1.0.20	10.1.4.2	02:30:13	Vlan100	1125104	1125104000
1125104000	0				
225.1.0.19	10.1.4.2	02:30:13	Vlan100	1125103	1125103000
1125103000	0				
...					
225.1.0.5	10.1.4.2	02:30:13	Vlan100	1125102	1125102000
1125102000	0				
225.1.0.4	10.1.4.2	02:30:13	Vlan100	1125103	1125103000
1125103000	0				
225.1.0.3	10.1.4.2	02:30:13	Vlan100	1125102	1125102000
1125102000	0				
switch1#					

```
switch# show nbm flows statistics group 225.1.2.47 source 10.2.3.2 vrf red
```

```
-----  
NBM Flow Statistics for VRF 'red'  
-----
```

```
Source-Group-Based Flow Statistics for Source 10.2.3.2 Group 225.1.2.47 :
```

Mcast-Group	Src-IP	Uptime	Src-Intf	Packets	Bytes
Allow-Bytes	Drop-Bytes				
225.1.2.47	10.2.3.2	02:29:53	Eth1/32	1124095	1124095000
1124095000	0				

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

```
switch# show nbm flows summary vrf all
```

```
-----  
NBM Flow Summary for VRF 'default'  
-----
```

```
IIF = Incoming Interface  
OIF = Outgoing Interface  
-----
```

Sample Output for Show Commands

Category	(*,G)	(S,G)	Total
All Flows	0	0	0
Flows with No receivers	0	0	0
Flows with OIF	0	0	0
Flows with SVI IIF	0	0	0
Flows with PHY IIF	0	0	0
Flows (SVI) with Policing	0	0	0
Flows (PHY) with Policing	0	0	0

NBM Flow Summary for VRF 'red'

IIF = Incoming Interface
OIF = Outgoing Interface

Category	(*,G)	(S,G)	Total
All Flows	0	72	72
Flows with No receivers	0	0	0
Flows with OIF	0	72	72
Flows with SVI IIF	0	24	24
Flows with PHY IIF	0	48	48
Flows (SVI) with Policing	0	24	0
Flows (PHY) with Policing	0	48	0

Incoming Interface Name	(*,G)	(S,G)	Total
Vlan100	0	24	24
Ethernet1/31	0	24	24
Ethernet1/32	0	24	24

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

```
switch# show nbm flows vrf all
-----
NBM Flows for VRF 'default'
-----
Active Source-Group-Based Flow(s) :

Mcast-Group      Src-IP          Uptime   Src-Intf      Nbr-Device      Num Rx Bw Mbps
Slot Unit Slice DSCP QOS Policed Policy-name

-----
NBM Flows for VRF 'red'
-----
Active Source-Group-Based Flow(s) :

Mcast-Group      Src-IP          Uptime   Src-Intf      Nbr-Device      Num Rx Bw Mbps
Slot Unit Slice DSCP QOS Policed Policy-name
225.1.2.48      10.2.3.2       02:16:27  Eth1/31     gretta-r10-eor2      1  1.001
    1    5    0    1    0 Yes      pol1
225.1.2.47      10.2.3.2       02:16:27  Eth1/32     gretta-r10-eor2      1  1.500
    1    5    0    0    7 Yes      Default
225.1.2.46      10.2.3.2       02:16:27  Eth1/32     gretta-r10-eor2      1  2.002
    1    5    0    3    0 Yes      pol12
```

225.1.2.45		10.2.3.2	02:16:27	Eth1/31	gretta-r10-eor2	1	1.500
1	5	0 0 7 Yes	Default				
225.1.2.44		10.2.3.2	02:16:27	Eth1/32	gretta-r10-eor2	1	1.500
1	5	0 0 7 Yes	Default				
225.1.2.43		10.2.3.2	02:16:27	Eth1/31	gretta-r10-eor2	1	1.500
1	5	0 0 7 Yes	Default				
225.1.2.42		10.2.3.2	02:16:27	Eth1/32	gretta-r10-eor2	1	1.500
1	5	0 0 7 Yes	Default				
...							
225.1.0.2		10.1.4.2	02:16:48	Vlan100	not-applicable	1	1.500
0	0	0 0 7 Yes	Default				
225.1.0.1		10.1.4.2	02:16:48	Vlan100	not-applicable	1	1.500
0	0	0 0 7 Yes	Default				
225.1.0.24		10.1.4.2	02:16:48	Vlan100	not-applicable	1	1.500
0	0	0 0 7 Yes	Default				
225.1.0.23		10.1.4.2	02:16:48	Vlan100	not-applicable	1	1.500
0	0	0 0 7 Yes	Default				
225.1.0.22		10.1.4.2	02:16:48	Vlan100	not-applicable	1	1.500
0	0	0 0 7 Yes	Default				
225.1.0.21		10.1.4.2	02:16:48	Vlan100	not-applicable	1	1.500
0	0	0 0 7 Yes	Default				
225.1.0.20		10.1.4.2	02:16:48	Vlan100	not-applicable	1	1.500
0	0	0 0 7 Yes	Default				
225.1.0.19		10.1.4.2	02:16:48	Vlan100	not-applicable	1	1.500
0	0	0 0 7 Yes	Default				
225.1.0.18		10.1.4.2	02:16:48	Vlan100	not-applicable	1	1.500
0	0	0 0 7 Yes	Default				
225.1.0.17		10.1.4.2	02:16:48	Vlan100	not-applicable	1	1.500
0	0	0 0 7 Yes	Default				
225.1.0.16		10.1.4.2	02:16:48	Vlan100	not-applicable	1	1.500
0	0	0 0 7 Yes	Default				
225.1.0.15		10.1.4.2	02:16:48	Vlan100	not-applicable	1	1.200
0	0	0 11 0 Yes	bw10				
225.1.0.14		10.1.4.2	02:16:48	Vlan100	not-applicable	1	1.200
0	0	0 11 0 Yes	bw10				
225.1.0.13		10.1.4.2	02:16:48	Vlan100	not-applicable	1	1.200
0	0	0 11 0 Yes	bw10				
225.1.0.12		10.1.4.2	02:16:48	Vlan100	not-applicable	1	1.200
0	0	0 11 0 Yes	bw10				
225.1.0.11		10.1.4.2	02:16:48	Vlan100	not-applicable	1	1.200
0	0	0 11 0 Yes	bw10				
225.1.0.10		10.1.4.2	02:16:48	Vlan100	not-applicable	1	1.500
0	0	0 0 7 Yes	Default				
...							

This example shows sample output for the **show nbm host-policy all receiver external vrf all** command:

```
switch# show nbm host-policy all receiver external vrf all
-----
VRF 'blue': External Receiver Policy Table
-----
```

Default External Receiver Policy: Deny

Seq Num	Source	Group	Group Mask	Permission
1	70.20.10.110	228.1.1.1	32	Allow
2	70.20.10.110	228.1.1.0	24	Deny
3	70.20.10.110	228.1.0.0	16	Deny
4	0.0.0.0	228.1.1.0	24	Allow
5	0.0.0.0	228.1.1.2	32	Deny
6	0.0.0.0	227.1.1.0	24	Allow
11	70.20.10.102	229.1.1.2	32	Deny

Sample Output for Show Commands

```

-----
Total Policies Found = 7

-----
VRF 'default': External Receiver Policy Table
-----

Default External Receiver Policy: Allow

-----
Seq Num      Source       Group      Group Mask  Permission
-----
4096        70.30.1.103   235.1.1.121    32         Allow
4352        70.30.1.104   235.1.1.178    32         Allow
1           70.20.10.110   228.1.1.1      32         Deny
4097        70.30.1.103   235.1.1.122    32         Allow
4353        70.30.1.104   235.1.1.179    32         Allow
...
4094        70.30.1.103   235.1.1.119    32         Allow
4350        70.30.1.104   235.1.1.176    32         Allow
4095        70.30.1.103   235.1.1.120    32         Allow
4351        70.30.1.104   235.1.1.177    32         Allow
-----
```

Total Policies Found = 601

This example shows sample output for the **show nbm host-policy all receiver local vrf all** command:

```
switch# show nbm host-policy all receiver local vrf all
```

```

-----
VRF 'blue': Local Receiver Policy Table
-----
```

Default Local Receiver Policy: Allow

Total Policies Found = 0

```

-----
VRF 'blue': Local Receiver Policy Table
-----
```

Default Local Receiver Policy: Allow

Total Policies Found = 0

```

-----
VRF 'default': Local Receiver Policy Table
-----
```

Default Local Receiver Policy: Allow

```

-----
Seq Num      Source       Group      Group Mask  Reporter    Permission
-----
256          0.0.0.0     228.1.1.246   32         70.30.1.102  Allow
512          0.0.0.0     228.1.2.247   32         70.30.1.102  Allow
768          0.0.0.0     228.1.3.248   32         70.30.1.102  Allow
4864         0.0.0.0     228.1.2.30    32         100.1.1.101  Allow
-----
```

100096	0.0.0.0	231.1.1.106	32	0.0.0.0	Deny	
100352	0.0.0.0	236.1.1.112	32	0.0.0.0	Deny	
257	0.0.0.0	228.1.1.247	32	70.30.1.102	Allow	
513	0.0.0.0	228.1.2.248	32	70.30.1.102	Allow	
769	0.0.0.0	228.1.3.249	32	70.30.1.102	Allow	
...						
511	0.0.0.0	228.1.2.246	32	70.30.1.102	Allow	
767	0.0.0.0	228.1.3.247	32	70.30.1.102	Allow	
4863	0.0.0.0	228.1.2.29	32	100.1.1.101	Allow	
100095	0.0.0.0	231.1.1.105	32	0.0.0.0	Deny	
100351	0.0.0.0	236.1.1.111	32	0.0.0.0	Deny	

Total Policies Found = 1470

This example shows sample output for the **show nbm host-policy all sender vrf all** command:

```
switch# show nbm host-policy all sender vrf all
-----
VRF 'blue': Sender Policy Table
-----
Default Sender Policy: Allow
Total Policies Found = 0
-----
VRF 'default': Sender Policy Table
-----
Default Sender Policy: Allow
-----
Seq Num      Source        Group       Group Mask  Permission
-----
776          70.20.10.201  234.1.1.1   32          Allow
777          70.20.10.201  234.1.1.2   32          Allow
778          70.20.10.201  234.1.1.3   32          Allow
779          70.20.10.201  234.1.1.4   32          Allow
780          70.20.10.201  234.1.1.5   32          Allow
781          70.20.10.201  234.1.1.6   32          Allow
782          70.20.10.201  234.1.1.7   32          Allow
783          70.20.10.201  234.1.1.8   32          Allow
784          70.20.10.201  234.1.1.9   32          Allow
...
3970         70.20.10.215  234.1.1.195 32          Allow
3971         70.20.10.215  234.1.1.196 32          Allow
3972         70.20.10.215  234.1.1.197 32          Allow
3973         70.20.10.215  234.1.1.198 32          Allow
3974         70.20.10.215  234.1.1.199 32          Allow
3975         70.20.10.215  234.1.1.200 32          Allow
-----
Total Policies Found = 3000
```

This example shows sample output for the **show nbm host-policy applied receiver external vrf all** command:

```
switch# show nbm host-policy applied receiver external vrf all
-----
VRF 'blue': Applied External Receiver Policy Table
-----
```

Sample Output for Show Commands

Default External Receiver Policy: Deny

Applied policy for interface 'ALL':

Seq Num	Source	Group	Group Mask	Permission	Deny Counter
6	0.0.0.0	227.1.1.0	24	Allow	0
4	0.0.0.0	228.1.1.0	24	Allow	0
5	0.0.0.0	228.1.1.2	32	Deny	1116
11	70.20.10.102	229.1.1.2	32	Deny	0
3	70.20.10.110	228.1.0.0	16	Deny	0
2	70.20.10.110	228.1.1.0	24	Deny	6839
1	70.20.10.110	228.1.1.1	32	Allow	0

Total Policies Found = 7

VRF 'default': Applied External Receiver Policy Table

Default External Receiver Policy: Allow

Applied policy for interface 'ALL':

Seq Num	Source	Group	Group Mask	Permission	Deny Counter
5	0.0.0.0	228.1.1.1	32	Deny	0
1	70.20.10.110	228.1.1.1	32	Deny	0
3976	70.30.1.103	235.1.1.1	32	Allow	0
3977	70.30.1.103	235.1.1.2	32	Allow	0
3978	70.30.1.103	235.1.1.3	32	Allow	0
...					
4567	70.30.1.105	235.1.1.193	32	Allow	0
4568	70.30.1.105	235.1.1.194	32	Allow	0
4569	70.30.1.105	235.1.1.195	32	Allow	0
4570	70.30.1.105	235.1.1.196	32	Allow	0
4571	70.30.1.105	235.1.1.197	32	Allow	0
4572	70.30.1.105	235.1.1.198	32	Allow	0
4573	70.30.1.105	235.1.1.199	32	Allow	0
4574	70.30.1.105	235.1.1.200	32	Allow	0

Total Policies Found = 601

This example shows sample output for the **show nbm host-policy applied receiver local all vrf all** command:

```
switch# show nbm host-policy applied receiver local all vrf all
```

VRF 'blue': Applied Local Receiver Policy Table

Default Local Receiver Policy: Allow

Total Policies Found = 0

VRF 'default': Applied Local Receiver Policy Table

Default Local Receiver Policy: Allow

Applied policy for interface 'Vlan1001':

Seq Num	Source	Group	Group Mask	Permission	Deny Counter
4831	0.0.0.0	228.1.2.1	32	Allow	0
4836	0.0.0.0	228.1.2.2	32	Allow	0
4837	0.0.0.0	228.1.2.3	32	Allow	0
4838	0.0.0.0	228.1.2.4	32	Allow	0
4839	0.0.0.0	228.1.2.5	32	Allow	0
4840	0.0.0.0	228.1.2.6	32	Allow	0
4841	0.0.0.0	228.1.2.7	32	Allow	0
4842	0.0.0.0	228.1.2.8	32	Allow	0
...					
5086	0.0.0.0	228.1.2.252	32	Allow	0
5087	0.0.0.0	228.1.2.253	32	Allow	0
5088	0.0.0.0	228.1.2.254	32	Allow	0
5089	0.0.0.0	228.1.2.255	32	Allow	0

Applied policy for interface 'Wildcard':

Seq Num	Source	Group	Group Mask	Permission	Deny Counter
10000	0.0.0.0	231.1.0.0	16	Deny	0
10001	0.0.0.0	231.1.1.1	32	Deny	0
10002	0.0.0.0	231.1.1.2	32	Allow	0
100001	0.0.0.0	231.1.1.11	32	Deny	0
100002	0.0.0.0	231.1.1.12	32	Deny	0
100003	0.0.0.0	231.1.1.13	32	Deny	0
...					
100440	0.0.0.0	236.1.1.200	32	Deny	0
10300	0.0.0.0	237.1.0.0	16	Deny	0
10301	0.0.0.0	237.1.1.1	32	Allow	0
10401	0.0.0.0	238.1.0.0	16	Deny	0
10402	0.0.0.0	238.1.1.1	32	Allow	0

Total Policies Found = 705

This example shows sample output for the **show nbm host-policy applied receiver local interface interface vrf vrf-name** command:

```
switch# show nbm host-policy applied receiver local interface vlan 1001
```

VRF 'blue': Applied Local Receiver Policy Table

Default Local Receiver Policy: Allow

Applied policy for interface 'Vlan1001':

Seq Num	Source	Group	Group Mask	Permission	Deny Counter
4831	0.0.0.0	228.1.2.1	32	Allow	0
4836	0.0.0.0	228.1.2.2	32	Allow	0
4837	0.0.0.0	228.1.2.3	32	Allow	0
4838	0.0.0.0	228.1.2.4	32	Allow	0
4839	0.0.0.0	228.1.2.5	32	Allow	0

Sample Output for Show Commands

4840	0.0.0.0	228.1.2.6	32	Allow	0	
4841	0.0.0.0	228.1.2.7	32	Allow	0	

...

5087	0.0.0.0	228.1.2.253	32	Allow	0	
5088	0.0.0.0	228.1.2.254	32	Allow	0	
5089	0.0.0.0	228.1.2.255	32	Allow	0	

Total Policies Found = 255

This example shows sample output for the **show nbm host-policy applied receiver local wildcard vrf default** command:

```
switch# show nbm host-policy applied receiver local wildcard vrf default
```

VRF 'default': Applied Local Receiver Policy Table

Default Local Receiver Policy: Allow

Applied policy for interface 'Wildcard':

Seq Num	Source	Group	Group Mask	Permission	Deny Counter
10000	0.0.0.0	231.1.0.0	16	Deny	0
10001	0.0.0.0	231.1.1.1	32	Deny	0
10002	0.0.0.0	231.1.1.2	32	Allow	0
100001	0.0.0.0	231.1.1.11	32	Deny	0
100002	0.0.0.0	231.1.1.12	32	Deny	0
100003	0.0.0.0	231.1.1.13	32	Deny	0
100004	0.0.0.0	231.1.1.14	32	Deny	0
100005	0.0.0.0	231.1.1.15	32	Deny	0
100006	0.0.0.0	231.1.1.16	32	Deny	0
...					
100439	0.0.0.0	236.1.1.199	32	Deny	0
100440	0.0.0.0	236.1.1.200	32	Deny	0
10300	0.0.0.0	237.1.0.0	16	Deny	0
10301	0.0.0.0	237.1.1.1	32	Allow	0
10401	0.0.0.0	238.1.0.0	16	Deny	0
10402	0.0.0.0	238.1.1.1	32	Allow	0

Total Policies Found = 450

This example shows sample output for the **show nbm host-policy applied sender all vrf all** command:

```
switch# show nbm host-policy applied sender all vrf all
```

VRF 'default': Applied Sender Policy Table

Default Sender Policy: Allow

Total Policies Found = 0

```
VRF 'red': Applied Sender Policy Table
-----
Default Sender Policy: Allow

Applied policy for interface 'Ethernet1/32':
-----
Seq Num      Source       Group      Group Mask  Permission
-----
20          10.1.31.10   228.31.1.1    32        Allow
-----
Total Policies Found = 1

-----
VRF 'blue': Applied Sender Policy Table
-----
Default Sender Policy: Allow

Applied policy for interface 'Ethernet1/31':
-----
Seq Num      Source       Group      Group Mask  Permission
-----
10          10.1.31.10   228.31.1.1    32        Allow
11          10.1.31.10   228.31.1.2    32        Allow
12          10.1.31.10   228.31.1.3    32        Allow
13          10.1.31.10   228.31.1.4    32        Allow
-----
Total Policies Found = 4
```

This example shows sample output for the **show nbm host-policy applied sender interface *interface vrf-name*** command:

```
switch# show nbm host-policy applied sender interface e1/31
-----
VRF 'blue': Applied Sender Policy Table
-----
Default Sender Policy: Allow

Applied policy for interface 'Ethernet1/31':
-----
Seq Num      Source       Group      Group Mask  Permission
-----
10          10.1.31.10   228.31.1.1    32        Allow
11          10.1.31.10   228.31.1.2    32        Allow
12          10.1.31.10   228.31.1.3    32        Allow
13          10.1.31.10   228.31.1.4    32        Allow
-----
```

Sample Output for Show Commands

```
Total Policies Found = 4
```

This example shows sample output for the **show nbm host-policy applied sender wildcard vrf all** command:

```
switch# show nbm host-policy applied sender wildcard vrf all
```

```
-----  
VRF 'default': Applied Sender Policy Table  
-----
```

```
Default Sender Policy: Allow
```

```
Total Policies Found = 0
```

```
-----  
VRF 'red': Applied Sender Policy Table  
-----
```

```
Default Sender Policy: Allow
```

```
Applied policy for interface 'Wildcard':
```

Seq Num	Source	Group	Group Mask	Permission
10	0.0.0.0	228.1.10.1	32	Allow
20	0.0.0.0	228.1.20.1	32	Deny
30	0.0.0.0	228.1.30.1	32	Deny
40	0.0.0.0	228.1.40.1	32	Deny
50	0.0.0.0	228.1.50.1	32	Allow

```
Total Policies Found = 5
```

This example shows sample output for the **show nbm flows static** command when static flow provisioning is enabled:

```
switch# show nbm flows static
```

```
+-----  
| NBM Static API Flow Table for VRF default  
+-----
```

```
+-----  
| Provisioned Static Flows  
+-----
```

Source	Group	Ingress Intf	BW (in Kbps)	Policed
Is LHR	Egress Intf	Fault Reason		
10.1.103.10	231.1.1.1	Vlan103	1000000	Yes
		None		
YES	Vlan104	None		
YES	Vlan105	None		
NO	Ethernet1/64	None		

This example shows sample output for the **show nbm flows static group** command when static flow provisioning is enabled. The Fault Reason column shows the reason for any errors that occur.

switch# show nbm flows static group 231.1.1.2				
+-----+ NBM Static API Flow Table for VRF default +-----+				
+-----+ Provisioned Static Flows +-----+				
Source	Group	Ingress Intf	BW (in Kbps)	Policed
Is LHR	Egress Intf	Fault Reason		
10.1.103.10	231.1.1.2	Vlan103 None	1000000	Yes
YES	Vlan104	Intf down		
YES	Vlan105	None		
NO	Ethernet1/64	None		

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: Fri Mar 29 05:21:38 2019
!Time: Fri Mar 29 10:09:24 2019

version 9.3(1) Bios:version 08.35
feature nbm

nbm mode pim-active
nbm host-policy
  sender
    default permit
  receiver
    default permit
  pim
    default permit
nbm reserve unicast fabric bandwidth 2
nbm flow asm range 225.0.0.0/8 234.80.0.0/16 232.6.0.0/16 233.80.0.0/16
nbm flow asm range 235.6.0.0/16 239.80.0.0/16 227.0.0.0/8 238.80.0.0/16
nbm flow asm range 238.100.0.0/16 239.100.0.0/16
nbm flow bandwidth 1002 kbps
nbm flow-policy
  policy v2.leaf1.1.225.50
    bandwidth 1001 kbps
    dscp 26
    ip group-range 225.50.1.6 to 225.50.1.10
  policy v2.leaf1.1.225.80
    bandwidth 1001 kbps
    dscp 24
    ip group-range 225.80.1.1 to 225.80.1.5
nbm vrf mars
  nbm mode pim-active
  nbm host-policy
    sender
      default permit
    receiver
      default permit
    pim
      default permit
```

Sample Show Command Output (Single Modular Switches)

```

nbm reserve unicast fabric bandwidth 1
nbm flow asm range 225.0.0.0/8 227.0.0.0/8 234.80.0.0/16 233.80.0.0/16
nbm flow asm range 235.6.0.0/16 239.80.0.0/16 232.6.0.0/16 238.80.0.0/16
nbm flow asm range 238.100.0.0/16 239.100.0.0/16
nbm flow bandwidth 1004 kbps
nbm flow-policy
    policy static.v2.leaf3.1.238.80
        bandwidth 1001 kbps
        dscp 35
        ip group-range 238.80.1.1 to 238.80.1.5
    policy static.v2.leaf4.1.239.80
        bandwidth 1001 kbps
        dscp 35
        ip group-range 239.80.1.1 to 239.80.1.5
nbm flow-definition 233.80.1.1 0.0.0.0
    egress-interface eth6/20/3
    egress-interface vlan851
    stage-flow
    egress-host 21.7.1.2
nbm flow-definition 233.80.1.2 0.0.0.0
    egress-interface eth6/20/3
    stage-flow
    egress-host 21.7.1.2

```

Sample Show Command Output (Single Modular Switches)

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.

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
```

Sample Output for Show Commands

```
bandwidth 123 kbps
dscp 10
  ip group-range 237.1.1.0 to 238.1.1.0
policy POL_A
policy flow
policy nbml_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
```



INDEX

B

bandwidth **25, 38, 44**

C

class **51, 53**

class-map type qos match-all **51–52**

class-map type qos match-any **51–52**

clear flow rtp detail **62**

clear nbm flow statistics **56**

D

default deny **24, 41**

default permit **24, 41**

dscp **26, 44**

E

egress-host **48**

egress-interface **48**

F

feature interface-vlan **33–34**

feature nbm **23, 37, 50**

feature netflow **60**

flow priority **26, 39, 44**

flow rtp timeout **63**

H

host **24, 42**

I

interface vlan **33–34**

ip access-list **51–52, 60**

ip address **27–28, 31–33, 35**

ip flow rtp **60**

ip group **39**

ip group-range **26, 39, 44**

ip igmp immediate-leave **27, 29, 32–33**

ip igmp snooping **33–34**

ip igmp snooping fast-leave **33–34**

ip igmp suppress v3-gsq **33, 35**

ip igmp version **27, 29**

ip igmp version 3 **32–34**

ip ospf passive-interface **27–28, 32**

ip pim passive **33, 35**

ip pim rp-address **27**

ip pim sparse mode **50**

ip pim sparse-mode **27–28, 31–33, 35**

ip pim spt-threshold infinity group-list **27–28**

ip pim ssm range none **27**

ip router ospf **27–28, 31–33, 35**

ipv6 flow rtp **60**

M

master ipv4 **56–57**

match access-group name **51–53**

match ip multicast group **27–28**

N

nbm external-link **50**

nbm flow asm range **24, 42**

nbm flow bandwidth **24, 37, 42**

nbm flow dscp **25, 42**

nbm flow reserve-bandwidth receiver-only **43**

nbm flow-definition **48**

nbm flow-policy **25, 38, 43**

nbm host-policy **23, 41**

nbm mode pim-active **41**

nbm mode pim-passive **45**

nbm reserve unicast fabric bandwidth **24, 42**

nbm vrf **41, 45**

no nbm flow policer **25, 38, 43**

no policer **25, 38, 43**

no shutdown **31–33, 35–36**

P

permit **51–52**

pim **23, 41**

policy **25, 38, 43**

policy-map type qos **51, 53**
ptp transport ipv4 ucast master **56–57**
ptp ucast-source **56–57**

R

receiver **23, 41**
route-map **27–28**

S

sender **23, 41**
service-policy type qos input **51, 54**
set qos-group **51, 53**
show flow rtp details **61**
show flow rtp errors active **61**
show flow rtp errors history **61**
show ip mroute **55**
show nbm defaults **55**
show nbm flow-policy **55**
show nbm flows **55**

show nbm flows static **55**
show nbm flows static group **55**
show nbm flows statistics **55**
show nbm flows summary **55**
show nbm host-policy **55**
show nbm interface bandwidth **55**
show ptp brief **57**
show ptp counters interface ethernet **57**
show running-config nbm **55**
slave ipv4 **56–57**
source **24, 42**
stage-flow **48**
switchport **33, 35**
switchport access vlan **33, 36**
switchport mode **33, 35**
switchport trunk allowed vlan **33, 36**

V

vlan configuration **33–34**