

Cisco Nexus 9000 Series NX-OS IP Fabric for Media Solution Guide, Release 10.6(x)

First Published: 2025-08-13

Last Modified: 2026-04-27

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: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html. Cisco product warranty information is available at https://www.cisco.com/c/en/us/products/warranty-listing.html. US Federal Communications Commission Notices are found here https://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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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)

© 2025–2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface ix

Audience ix

Documentation Conventions ix

Related Documentation x

Related Documentation for Cisco Nexus 9000 Series NX-OS Software xi

Documentation Feedback xiii

Communications, Services, and Additional Information xiii

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

Supported Platforms 3

About the IP Fabric for Media Solution 3

Deployment Types 4

Spine-Leaf Topology 4

Single Modular Switch Topology 4

IP Fabric for Media Solution Components 5

Cisco Nexus 9000 Series Switches 5

NDFC with IPFM 7

Enhanced Payload for IPFM Critical Event 8

Enhanced Fault and Notification Payload Structure 9

Failure Handling 19

Benefits of the IP Fabric for Media Solution 19

Related Documentation 20

CHAPTER 3 **Setting Up the IP Fabric for Media** 21

Determining the Number and Types of Leaf Switches Required in the IP Fabric 21

Determining the Number of Achievable Flows in the IP Fabric 23

CHAPTER 4 **Configuring IP Fabric for Media** 25

Prerequisites 25

Guidelines and Limitations 26

Guidelines and Limitations for Host Policies 28

Guidelines and Limitations for Unicast PTP 30

Guidelines and Limitations for the Cisco NDFC 30

Licensing Requirements for NDFC Media Controller 31

Upgrading to a Cisco NX-OS 9.x Release 32

Upgrading from a Cisco NX-OS 9.x Release 32

Upgrading from a Cisco NX-OS 7.x Release 32

Setting Up the SNMP Server for NDFC 33

Configuring IPFM 33

Configuring IPFM for a Spine-Leaf Topology 33

Configuring PIM on Spine and Leaf Switches 39

Configuring MSDP on Spine Switches 41

Priority-based flow 42

Configuring Fabric and Host Interfaces 45

Configuring IPFM for a Single Modular Switch 51

Configuring an IPFM VRF 55

Configuring an IPFM VRF for Active Flow Provisioning 55

Configuring an IPFM VRF for Static Flow Provisioning 60

Configuring IPFM Subinterface Type 61

Establishing a Flow (Optional) 62

Creating an IPFM Flow Definition 62

Configuring IGMP Static OIF 66

Configuring Unicast Bandwidth Reservation Per Port 66

Configuring Multisite 67

Enabling Multicast and Unicast Flows (Optional) 69

Verifying the IPFM Configuration 73

Clearing IPFM Flow Statistics 74
Configuring Unicast PTP Peers 74
vPC Support 76

CHAPTER 5 Configuring Media Flow Analytics 77
RTP Flow Monitoring 77
Guidelines and Limitations for RTP Flow Monitoring 77
Configuring RTP Flow Monitoring 78
Displaying RTP Flows and Errors 79
Clearing RTP Flows 81

CHAPTER 6 Configuring Multicast Service Reflection with IPFM 83
Multicast Service Reflection with IPFM 83

CHAPTER 7 Non-Blocking Multicast Service Reflection 85
NAT Guidelines and Limitations 85
Multicast to Multicast Ingress NAT 85
Multicast to Multicast Egress NAT 86
Examples for ENAT PIM Passive 86
Multicast to Unicast NAT 87
Examples for MU NAT PIM Passive 87
Unicast to Multicast NAT 88

CHAPTER 8 Media Controller 95
Generic Multicast Monitoring 97
Topology 100
Host 101
Discovered Host 101
Host Alias 102
Add Host Alias 103
Edit Host Alias 103
Delete Host Alias 104
Import Host Alias 104
Export Host Alias 105

Host Policies 105
Add Host Policy 110
Edit Host Policy 111
Delete Host Policy 111
Import Host Policy 112
Export Host Policy 112
Policy Deployment 113
Applied Host Polices 114
Flow 115
Flow Status 115
Flow Alias 120
Add Flow Alias 120
Edit Flow Alias 121
Delete Flow Alias 121
Export Flow Alias 122
Import Flow Alias 122
Flow Policies 122
Add Flow Policy 127
Edit Flow Policy 128
Delete Flow Policy 129
Import Flow Policy 129
Export Flow Policy 130
Policy Deployment 130
Static Flow 132
Adding Static Flow 133
Deleting Static Flow 133
RTP 133
RTP Flow Monitor 133
Multicast NAT 135
NAT Modes 136
Adding a NAT Mode 138
Deleting a NAT Mode 138
Egress Interface Mappings 139
Adding Egress Interface Mapping 141

Editing Egress Interface Mapping 142
Deleting Egress Interface Mapping 142
NAT Rules 142
Adding NAT Rule 144
Deleting NAT Rule 145
Border Router Config 145
Deploying Border Router Config 146
Global 147
Events 147
Copying Switch Running Configuration to Start-up Configuration 148
Realtime Notifications 148
Threshold Notifications 149
Config 149
Setting Up the SNMP Server for NDFC 149
AMQP Notifications 150
Switch Global Config 152
Interface Configs 155
NDFC Read-Only Mode for Media Controller 158

APPENDIX A **Sample Output for Show Commands** 163
Sample Show Command Output (Spine-Leaf Deployment) 163
Sample Show Command Output (Single Modular Switches) 178



Preface

This preface includes these sections:

- Audience, on page ix
- Documentation Conventions, on page ix
- Related Documentation, on page x
- Related Documentation for Cisco Nexus 9000 Series NX-OS Software, on page xi
- Documentation Feedback, on page xiii
- Communications, Services, and Additional Information, on page xiii

Audience

This publication is for network administrators who install, configure, and maintain Cisco Nexus switches.

Documentation Conventions

Command descriptions use these conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.

Convention	Description
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use these conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Related Documentation

Cisco Application Centric Infrastructure (ACI) Documentation

The ACI documentation is available at the following URLhttps://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.

Cisco Application Centric Infrastructure (ACI) Simulator Documentation

The Cisco ACI Simulator documentation is available at https://www.cisco.com/c/en/us/support/cloud-systems-management/application-centric-infrastructure-simulator/series.html.

Cisco Nexus 9000 Series Switches Documentation

The Cisco Nexus 9000 Series Switches documentation is available at https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/series.html.

Cisco Application Virtual Switch Documentation

The Cisco Application Virtual Switch (AVS) documentation is available at https://www.cisco.com/c/en/us/support/switches/retired.html.

Cisco Application Centric Infrastructure (ACI) Integration with OpenStack Documentation

Cisco ACI integration with OpenStack documentation is available at https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.

Related Documentation for Cisco Nexus 9000 Series NX-OS Software

The entire Cisco NX-OS 9000 Series documentation set is available at this URL:

https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/series.html#Collections

Release Notes

The release notes are available at the this URL:

https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html

Configuration Guides

These guides are available at this URL:

https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-installation-and-configuration-guides-list.html

The documents in this category include:

- *Cisco Nexus 2000 Series NX-OS Fabric Extender Software Configuration Guide for Cisco Nexus 9000 Series Switches*
- *Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide*
- *Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*
- *Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*
- *Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide*
- *Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide*
- *Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide*
- *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*
- *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*
- *Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide*
- *Cisco Nexus 9000 Series NX-OS Verified Scalability Guide*
- *Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide*

Hardware Documents

These guides are available at this URL:

https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-installation-guides-list.html

The documents in this category include:

- *Cisco Nexus 3000 Series Hardware Installation Guide*

- *Cisco Nexus 92160YC-X NX-OS Mode Switch Hardware Installation Guide*
- *Cisco Nexus 92300YC NX-OS Mode Switch Hardware Installation Guide*
- *Cisco Nexus 92304QC NX-OS Mode Switch Hardware Installation Guide*
- *Cisco Nexus 9236C NX-OS Mode Switch Hardware Installation Guide*
- *Cisco Nexus 9272Q NX-OS Mode Switch Hardware Installation Guide*
- *Cisco Nexus 93108TC-EX NX-OS Mode Switch Hardware Installation Guide*
- *Cisco Nexus 93120TX NX-OS Mode Switch Hardware Installation Guide*
- *Cisco Nexus 93128TX NX-OS Mode Switch Hardware Installation Guide*
- *Cisco Nexus 93180LC-EX NX-OS Mode Switch Hardware Installation Guide*
- *Cisco Nexus 93180YC-EX NX-OS Mode Switch Hardware Installation Guide*
- *Cisco Nexus 9332PQ NX-OS-Mode Switch Hardware Installation Guide*
- *Cisco Nexus 9372PX and 9372PX-E NX-OS Mode Switches Hardware Installation Guide*
- *Cisco Nexus 9372TX and 9372TX-E NX-OS Mode Switches Hardware Installation Guide*
- *Cisco Nexus 9396PX NX-OS Mode Switch Hardware Installation Guide*
- *Cisco Nexus 9396TX NX-OS Mode Switch Hardware Installation Guide*
- *Cisco Nexus 9504 NX-OS Mode Switch Hardware Installation Guide*
- *Cisco Nexus 9508 NX-OS Mode Switch Hardware Installation Guide*
- *Cisco Nexus 9516 NX-OS Mode Switch Hardware Installation Guide*
- *Regulatory, Compliance, and Safety Information for the Cisco Nexus 3000 and 9000 Series*

Other Software Documents

These guides are available at this URL:

https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-installation-guides-list.html

- *Cisco Nexus 7000 Series and 9000 Series NX-OS MIB Quick Reference*
- *Cisco Nexus 9000 Series NX-OS Programmability Guide*
- *Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide*
- *Cisco Nexus 9000 Series NX-OS System Messages Reference*
- *Cisco Nexus 9000 Series NX-OS Troubleshooting Guide*
- *Cisco NX-OS Licensing Guide*
- *Cisco NX-OS XML Interface User Guide*

Documentation Feedback

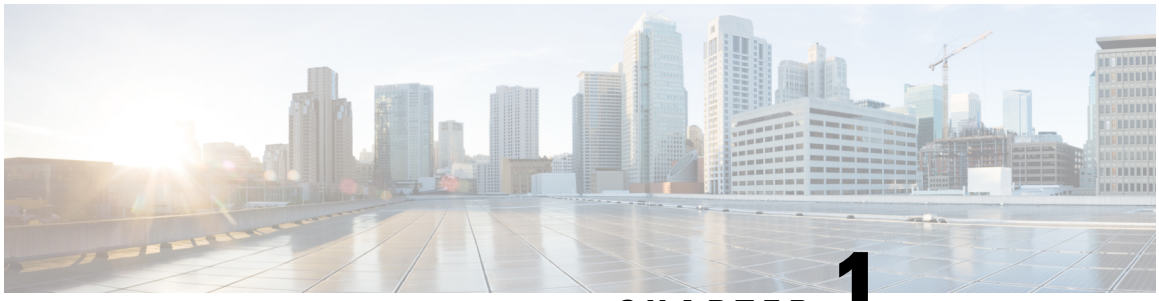
To provide technical feedback on this document, or to report an error or omission, please send your comments to apic-docfeedback@cisco.comnexus9k-docfeedback@cisco.com. We appreciate your feedback.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

New and Changed Information

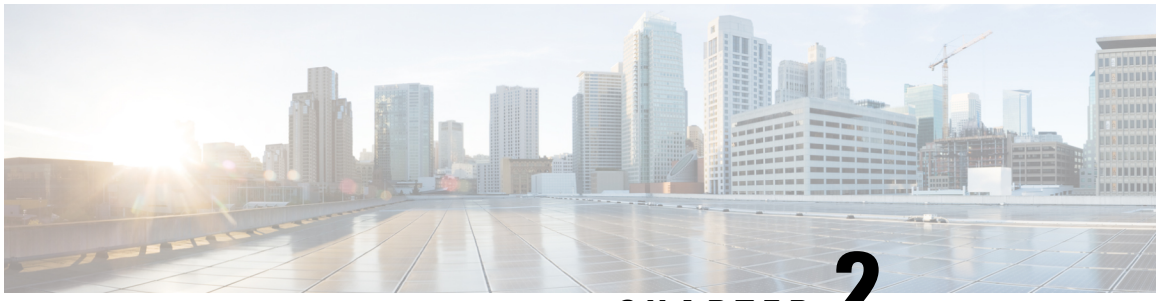
- New and changed information, on page 1

New and changed information

Table 1: New and changed features

Feature	Description	Changed in release	Where documented
PFM-SD multi-site support	Added support for PFM-SD multi-site on Cisco Nexus switches.	10.6(3)F	Guidelines and Limitations, on page 26
Media eXchange Layer (MXL) Use for AI/ML applications in media industry	Added support to use MXL for AI/ML applications in media.	10.6(3)F	Guidelines and Limitations, on page 26
Enhanced Flow bandwidth to support 100 Gbps	Enhanced bandwidth range for flow policies from 25 Gbps (25,000,000 Kbps) to 100 Gbps (100,000,000 Kbps).	10.6(2)F	Configuring IPFM for a Spine-Leaf Topology, on page 33 Configuring IPFM for a Single Modular Switch, on page 51 Configuring an IPFM VRF for Active Flow Provisioning, on page 55
RTP flow monitoring	Added DME support for RTP flow monitoring	10.6(2)F	Guidelines and Limitations for RTP Flow Monitoring, on page 77

Feature	Description	Changed in release	Where documented
Enhanced Fault and Notification Payload Structure	Enhanced flow analytics with new fault categories and payload structure, allowing precise troubleshooting and optimization of traffic flows.	10.6(1)F	Enhanced Payload for IPFM Critical Event, on page 8 Enhanced Fault and Notification Payload Structure, on page 9



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
- Supported Platforms, on page 3
- About the IP Fabric for Media Solution, on page 3
- IP Fabric for Media Solution Components, on page 5
- Enhanced Payload for IPFM Critical Event, on page 8
- Failure Handling, on page 19
- Benefits of the IP Fabric for Media Solution, on page 19
- Related Documentation, on page 20

Licensing Requirements

See the Cisco NX-OS Licensing Guide and Cisco NX-OS Licensing Options Guide for Cisco NX-OS licensing recommendations and instructions to obtain and apply licenses.

Supported Platforms

See the Nexus Switch Platform Support Matrix to know from which Cisco NX-OS releases various Cisco Nexus 9000 and 3000 switches support a selected feature.

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 IP Fabric for Media algorithm

(an intelligent traffic management algorithm) and with or without the Nexus Dashboard Fabric Controller (NDFC). Using open APIs, the Cisco Nexus Dashboard Fabric Controller (NDFC) can integrate with various broadcast controllers. The solution provides a highly reliable (zero drop multicast), highly visible, highly secure, and highly available network.

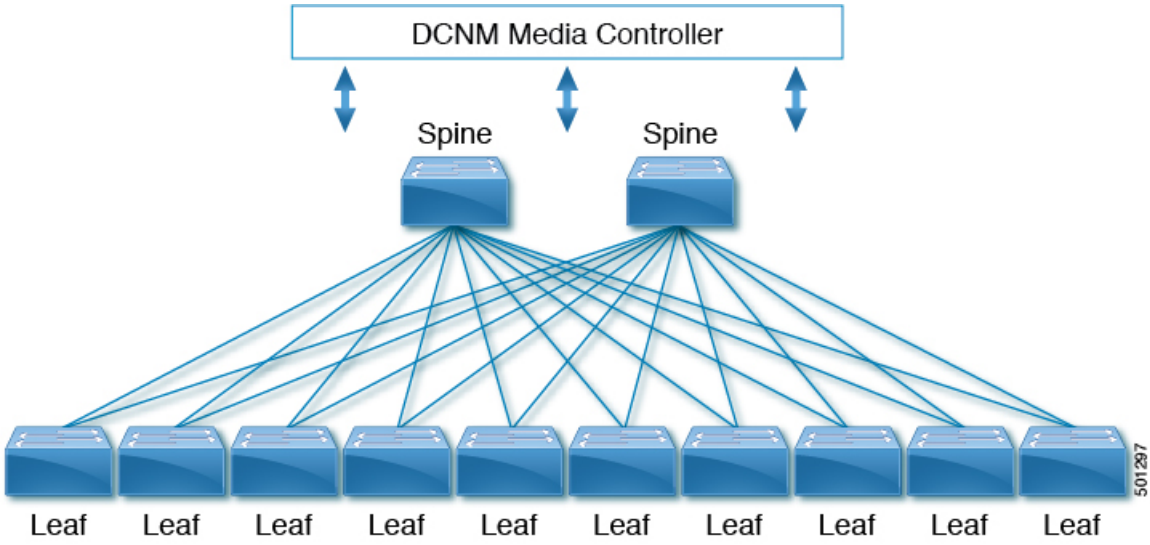
Deployment Types

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

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

Spine-Leaf Topology

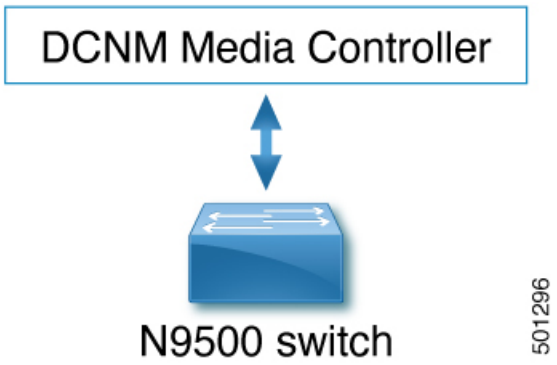
Cisco's IP fabric for media solution supports a spine-leaf topology that consists of multiple spine and leaf switches. The topology supports any combination of leaf switches, including using just one type of leaf switch.



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

Single Modular Switch Topology

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



IP Fabric for Media Solution Components

Cisco Nexus 9000 Series Switches

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

Cisco Nexus 9000 Series Switch	Number and Size of Ports	Role in Topology*
Cisco Nexus 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 93108TC-FX switch	48 x 10-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 **Note** The N9K-X96136YC-R line card is not supported.	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
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
Cisco Nexus 9348GC-FX3	48 x 10M/100M/1 Gbps BASE-T ports 4x 10/25 Gbps SFP28 ports 2 x 40/100 Gbps Quad small form-factor pluggable 28 (QSFP28) ports	Leaf in spine-leaf topology
N9K-X9624D-R2 line card	Line card with 24 400G QSFP-DD ports (only to be used with 8-slot chassis)	Spine or leaf in spine-leaf topology
Cisco Nexus 9508-FM-R2 line card	Fabric module for 400G line card (only to be used with 8-slot chassis)	Spine or leaf in spine-leaf topology
Cisco Nexus 9364D-GX2A switch	64 x 40/100/400G QSFP-DD ports 2 x 1/10G SFP+ ports	Spine or leaf switch in spine-leaf topology
Cisco Nexus 9348D-GX2A switch	48 x 40/100/400G QSFP-DD ports 2 x 1/10G SFP+ ports	Spine or leaf switch in spine-leaf topology
Cisco Nexus 9332D-GX2B switch	32 x 40/100/400G QSFP-DD ports 2 x 1/10G SFP+ ports	Spine or leaf switch in spine-leaf topology

Cisco Nexus 9000 Series Switch	Number and Size of Ports	Role in Topology*
Cisco Nexus 9808 switch with the following line cards: Cisco Nexus X9836DM-A Cisco Nexus 9808-FM-A	36 x 40/100/400G QSFP-DD ports (only to be used with 8-slot chassis) Fabric module for Nexus 9808	Spine in spine-leaf topology or single modular switch
Cisco Nexus 9332D-H2R	32-port 400G QSFP-DD ports	Spine or leaf in spine-leaf topology
Cisco Nexus 93400LD-H1 switch	48-port 50G SFP56 and 4-port 400G QSFP-DD ports	Leaf in spine-leaf topology
Cisco Nexus 9364C-H1 switch	64-port 100G QSFP28 ports	Leaf in spine-leaf topology
Cisco Nexus 93400LD-GX2A switch	32 x 400-Gbps and 16 x 100-Gbps QSFP-DD/QSFP28 ports	Spine or leaf in spine-leaf topology
Cisco Nexus 9804 switch	4-slot modular chassis (ports and capabilities vary by installed line cards)	Spine or leaf in spine-leaf topology or single modular switch
Cisco Nexus 9408 switch	8-slot modular chassis (ports and capabilities vary by installed line cards)	Spine or leaf in spine-leaf topology or single modular switch
Cisco Nexus 9364C-GX switch	64 x 100/40-Gbps QSFP28 ports	Leaf in spine-leaf topology
Cisco Nexus 9336C-SE1 switch	36 x 40/100-Gbps QSFP28 ports	Spine or 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.

NDFC with IPFM

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

The NDFC with IPFM 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.

Enhanced Payload for IPFM Critical Event

Beginning with Cisco NX-OS Release 10.6(1)F, enhancements provide more granular and user-friendly fault and notification information for improved network visibility and operational insight. This allows for faster identification and resolution of network issues. Key improvements include:

- Clearer fault reasons and resolutions.
- Key information, previously embedded within the Distinguished Name (DN), is now included as individual attributes in the payload. These attributes include:
  - **source:** The source IP address.
  - **group:** The multicast group IP address.
  - **faultCode:** The code that identifies the fault.
  - **vrf:** The Virtual Routing and Forwarding instance.

  This change eliminates the need to parse the DN to extract these values, providing a more direct way to access the information.
- Improved presentation of switch critical events in network management and monitoring interfaces.

The enhancements to flow analytics, with the new fault categories and payload structure, provide a more detailed and actionable view of network behavior. This allows for more precise troubleshooting and optimization of traffic flows.

- The new fault categories provide a more specific classification of fault conditions. This allows administrators to quickly pinpoint the source and nature of a problem.
- The faultReason and faultResolution attributes in the enhanced payload provide clear explanations of the fault and specific steps to resolve it.
- The new notification categories provide more granular information about network events. This allows administrators to proactively identify potential issues and optimize traffic flows before they impact performance.
- The new notification categories provide more granular information about network events. This enables administrators to proactively identify potential issues and take appropriate actions to optimize traffic flows.



Note Beginning with Cisco NX-OS Release 10.6(1)F, the legacy fault and notification outputs are deprecated. Subscribers and integrations must now consume the enhanced JSON payload structure, which provides enhanced name-value attribute pairs for all Fault and Notification Managed Objects (MOs). Ensure that any automated integrations or monitoring tools are updated accordingly.

Payload Structure: Old Vs New

The following example highlights the changes to the payload structure for flow faults:

Before Enhancement	After Enhancement

<pre>"nbmFaults": {
 	
"attributes": {
 	
"dn": "sys/nbm/show/faults/dm-default/faults-[s-[47.20.20.9]-g-[233.1.4.255]]",
 	
"faultDn": "s-[47.20.20.9]-g-[233.1.4.255]",
 	
"faultReason": "No Policer Avail",
 	
"faultResolution": "Please consult documentation",
 	
"modTs": "2025-04-01T16:03:15.175+00:00",
 	
"tStamp": "1743523395174"
 	
}</pre>
	<pre>"nbmFlowFaults": {
	
	"attributes": {
	
	"dn": "sys/nbm/show/faults/dm-default/flowfaults-[s-[47.20.20.9]-g-[233.1.4.255]]",
	
	"faultCode": "2076",
	
	"faultDn": "s-[47.20.20.9]-g-[233.1.4.255]",
	
	"faultReason": "Policer resources exhausted. Configured TCAM max has been reached",
	
	"faultResolution": "Review TCAM configuration if needed",
	
	"group": "233.1.4.255",
	
	"modTs": "2025-04-01T14:35:04.081+00:00",
	
	"source": "47.20.20.9",
	
	"tStamp": "1743518104080",
	
	"vrf": "default"
	
	}</pre>

Enhanced Fault and Notification Payload Structure

Starting with Cisco NX-OS Release 10.6(1)F, new fault and notification categories provide clearer and more useful information for troubleshooting and optimizing the network. The following sections detail the new Fault and Notification Managed Objects (MO), along with examples of their enhanced payload structures.

Fault MO

The enhanced Fault Managed Objects (MOs) provide detailed and categorized information about various network issues, enabling more precise troubleshooting and quicker resolution. These MOs are designed to offer granular insights into different types of faults. These are the Fault MOs:

- Flow Faults

  Indicate issues related to specific multicast flows, such as bandwidth shortages or policer resource exhaustion.

- Sender Faults

  Report problems originating from the source device or endpoint, such as policy denials or connectivity issues.

- Receiver Faults

Highlight conditions impacting the receiver, such as insufficient bandwidth or configuration issues that prevent flow delivery.

- Pim Passive Ingress Faults

  Identify faults associated with the ingress (incoming) interface of a flow, including VRF context or interface misconfigurations.

- Pim Passive Egress Faults

  Relate to faults on the egress (outgoing) interface of a flow, such as invalid interface IPs or VRF mismatches.

Notify MO

The new Notification Managed Objects (MOs) offer granular information about network events and operational states, helping administrators proactively identify potential issues and optimize traffic flows before they impact performance. These are the Notification MOs:

- Interface Level Usage MOs:

  Provide notifications on bandwidth utilization for ingress and egress interfaces, helping to monitor interface usage health.

  - Egress Event

    Notifies when bandwidth usage on an egress interface reaches or exceeds critical thresholds.

  - Ingress Event

    Notifies when bandwidth usage on an ingress interface reaches or exceeds critical thresholds.

- Event MO for Flow Rate

  Indicates when a flow's rate falls below or rises above configured thresholds.

- Flow Provisioned MO

  Confirms when a new flow has been successfully provisioned in the network.

- NAT Event MOs:

  Provide events related to NAT-specific bandwidth or translation state issues.

  - Oversubscription Event

    Alerts when cumulative pre-NAT bandwidth usage exceeds post-NAT bandwidth capacity.

  - Bandwidth Mismatch Event

    Signals when there is a mismatch between pre- and post-NAT flow bandwidths.

Flow Faults

The nbmFlowFaults Managed Object provides information about faults related to a specific flow, such as bandwidth or policer issues.

```
"nbmFlowFaults": {

    "attributes": {
```

```
"dn": "sys/nbm/show/faults/dom-default/flowfaults-[s-[47.20.20.9]-g-[233.1.4.255]]",

 "faultCode": "2076",

  "faultDn": "s-[47.20.20.9]-g-[233.1.4.255]",

 "faultReason": "Policer resources exhausted. Configured TCAM max has been reached",

  "faultResolution": "Review TCAM configuration if needed",

  "group": "233.1.4.255",

 "modTs": "2025-04-01T14:35:04.081+00:00",

 "source": "47.20.20.9",

 "tStamp": "1743518104080",

  "vrf": "default"

}
```


This table provides a list of flow fault codes, their reasons, and suggested resolutions for the flow fault type.

Fault Code	Fault Reason	Fault Resolution
3051	No bandwidth available for sender	Please review bandwidth configuration and modify if needed
3201	Flow denied remotely	Please revisit participating upstream switches
3202	Flow denied remotely (external link)	Please revisit participating upstream switches
3376	Impacted by higher priority flow due to bandwidth contention	Effects of granular flow priority configuration
3126	Sender is not reachable	Please check the unicast routing table for the sender IP
3176	PIM not enabled	Please configure PIM
3151	PIM/IGMP host proxy not enabled	Please configure PIM/IGMP host proxy
3152	PIM/IGMP host proxy not enabled (external link)	Please configure PIM/IGMP host proxy

Sender Faults

The nbmSenderFaults Managed Object provides information about faults originating from the media sender, such as host policy denials or resource limitations.


```
"nbmSenderFaults": {
```

```
    "attributes": {

        "dn":
"sys/nbm/show/faults/dom-default/senderfaults-[sys/nbm/show/endpoints/dom-default/h-[47.20.20.9]-if-0/g-[227.10.10.1]]",


       "faultCode": "2001",

       "faultDn": "sys/nbm/show/endpoints/dom-default/h-[47.20.20.9]-if-0/g-[227.10.10.1]",


        "faultReason": "Denied by sender host policy",

        "faultResolution": "Review sender host policy configuration and modify if needed"

         "group": "227.10.10.1",

          "modTs": "2025-04-01T14:25:13.635+00:00",

          "senderEndpoint": "47.20.20.9",

          "tStamp": "1743517513635",

          "vrf": "default"

}
```


This table provides a list of sender fault codes, their reasons, and suggested resolutions for the sender fault type.

Fault Code	Fault Reason	Fault Resolution
2001	Denied by sender host policy	Review sender host policy configuration and modify if needed
2002	Denied by sender host policy (external link)	Review sender host policy config and modify if needed
2051	No bandwidth available for sender	Please review bandwidth configuration and modify if needed
2052	No bandwidth available for sender (external link)	Please review bandwidth configuration and modify if needed
2076	Policer resources exhausted. Configured TCAM max has been reached	Review TCAM configuration if needed
2077	Policer resources exhausted (external link), configured TCAM max has been reached	Review TCAM configuration if needed
2377	Impacted by a higher priority flow due to policer unavailability	Effects of granular flow priority configuration
2101	No matching flow policy found	Please define the flow policy and bandwidth for this group

Fault Code	Fault Reason	Fault Resolution
2151	PIM/IGMP host proxy not enabled	Please configure PIM/IGMP host proxy
2152	PIM/IGMP host proxy not enabled (external link)	Please configure PIM/IGMP host proxy
2351	No TCAM allocated to ing-nbm region	Please revisit TCAM configuration
2352	No TCAM allocated to ing-nbm region for external ingress interface	Please revisit TCAM configuration

Receiver Faults

The nbmReceiverFaults Managed Object provides information about faults related to the media receiver, such as bandwidth limitations or connectivity issues.


```
"nbmReceiverFaults": {

     "attributes": {

          "dn":
"sys/nbm/show/faults/dom-default/receiverfaults-[sys/nbm/show/endpoints/dom-default/h-[47.20.10.1]-if-436231169/s-[47.20.20.9]-g-[227.10.10.1]]",


          "faultCode": "1026",

          "faultDn":
"sys/nbm/show/endpoints/dom-default/h-[47.20.10.1]-if-436231169/s-[47.20.20.9]-g-[227.10.10.1]",


          "faultReason": "No bandwidth currently available for receiver",

          "faultResolution": "Please review flow policy if receiver needs to be stitched"

          "group": "227.10.10.1",

          "modTs": "2025-04-01T14:27:46.801+00:00",

          "receiverEndpoint": "47.20.10.1",

          "receiverInterface": "Ethernet1/47.1",

          "source": "47.20.20.9",

          "tStamp": "1743517666801",

          "vrf": "default"

}
```


This table provides a list of receiver fault codes, their reasons, and suggested resolutions for the receiver fault type.

Fault Code	Fault Reason	Fault Resolution
1026	No bandwidth currently available for receiver	Please review flow policy, if receiver needs to be stitched

Pim Passive Ingress Faults

The nbmFlowIngressFaults Managed Object provides information about faults related to the ingress interface of a media flow, such as VRF context issues or invalid interface configurations.


```
"nbmFlowIngressFaults": {
                "attributes": {
                "dn":
"sys/nbm/show/faults/dom-default/flowingressfaults-[sys/nbm/conf/flows/dom-default/s-[47.20.20.9]-g-[230.1.0.1]]",

                "faultCode": "4230",
                "faultDn": "sys/nbm/conf/flows/dom-default/s-[47.20.20.9]-g-[230.1.0.1]",
                "faultReason": "IIF is not part of valid VRF context",
                "faultResolution": "Update VRF context on IIF if needed, then delete and
re-add DN in fault",
                "group": "230.1.0.1",
                "ingressif": "null0_iif",
                "modTs": "2025-04-01T15:07:15.248+00:00",
                "source": "47.20.20.9",
                "tStamp": "1743520035248",
                "vrf": "default"
                }
```


This table provides a list of PIM passive ingress fault codes, their reasons, and suggested resolutions for the PIM passive ingress fault type.

Fault Code	Fault Reason	Fault Resolution
4226	Invalid interface IP on IIF	Configure interface IP address, then set RPF to unspecified and validate
4230	IIF is not part of valid VRF context	Update VRF context on IIF if needed, then delete and re-add DN in fault
4251	VRF context is shut down for ingress interface	Enable VRF context, then delete and re-add DN in fault
4276	Ingress interface mroute clear command initiated	Delete and re-add DN in fault
4076	Policer resources exhausted. Configured TCAM max has been reached	Review TCAM configuration if needed
4228	Interface IP (IIF) VRF context was changed	Revert interface VRF configuration if needed, then delete and re-add DN in fault
4232	Missing PIM/IGMP host proxy config on RPF	Please configure PIM/IGMP host proxy on interface, then delete and re-add DN in fault

Pim Passive Egress Faults

The nbmFlowEgressFaults Managed Object provides information about faults related to the egress interface of a media flow, such as invalid interface IP addresses or configuration errors.


```
"nbmFlowEgressFaults": {
                "attributes": {
                "dn":
"sys/nbm/show/faults/dom-default/flowegressfaults-[sys/nbm/conf/flows/dom-default/s-[47.20.20.9]-g-[230.1.0.1]/if-[eth1/47.1]]",

                "egressif": "Eth1/47.1",
                "faultCode": "4227",
                "faultDn":
"sys/nbm/conf/flows/dom-default/s-[47.20.20.9]-g-[230.1.0.1]/if-[eth1/47.1]",
                "faultReason": "Invalid interface IP on OIF",
                "faultResolution": "Configure interface IP address, then delete and re-add
 DN in fault",
                "group": "230.1.0.1",
                "modTs": "2025-04-01T15:06:59.738+00:00",
                "source": "47.20.20.9",
                "tStamp": "1743520019738",
                "vrf": "default"
                }
```


This table provides a list of PIM passive egress fault codes, their reasons, and suggested resolutions for the PIM passive egress fault type.

Fault Code	Fault Reason	Fault Resolution
4227	Invalid interface IP on OIF	Configure interface IP address, then delete and re-add DN in fault
4229	OIF is not part of valid VRF context	Update VRF context on OIF if needed, then delete and re-add DN in fault
4231	Missing OIF-PIM config on egress interface	Configure PIM on interface, then delete and re-add DN in fault
4252	VRF context is shut down for outgoing interface	Enable VRF context, then delete and re-add DN in fault
4277	Egress interface mroute clear command initiated	Delete and re-add DN in fault

Interface Level Usage

Egress Event: nbmEgressEvent

The nbmEgressEvent Managed Object provides information about interface-level usage, such as bandwidth utilization on egress interfaces.


```
"nbmEgressEvent": {

                "attributes": {

                "dn":
"sys/nbm/show/notify/dom-vrf_pmn1/egressevent-[vrf:vrf_pmn1-INTF:Eth1/47.2-EGRESS]",
```

```
"egressinterface": "Eth1/47.2",

"modTs": "2025-04-03T08:12:36.338+00:00",

"notifyCode": "5301",

"notifyDn": "vrf:vrf_pmn1-INTF:Eth1/47.2-EGRESS",

"reason": "CRITICAL: egress bandwidth usage is at or above 90%",

"tStamp": "1743667956338",

"vrf": "vrf_pmn1"

}
```


This table provides a list of notification codes and their corresponding reasons for the egress event type.

Notify Code	Reason
5301	CRITICAL: egress bandwidth usage is at or above 90%

Ingress Event: nbmIngressEvent

The nbmIngressEvent Managed Object provides information about interface-level usage, such as bandwidth utilization on ingress interfaces.


```
"nbmIngressEvent": {

                "attributes": {

                "dn":
"sys/nbm/show/notify/dom-vrf_pmn1/ingressevent-[vrf:vrf_pmn1-INTF:Eth1/42.1-INGRESS]",

                "ingressinterface": "Eth1/42.1",

                "modTs": "2025-04-03T08:16:11.366+00:00",

                "notifyCode": "5302",

                "notifyDn": "vrf:vrf_pmn1-INTF:Eth1/42.1-INGRESS",

                "reason": "CRITICAL: ingress bandwidth usage is at or above 90%",

                "tStamp": "1743668171366",

                "vrf": "vrf_pmn1"

                }
```


This table provides a list of notification codes and their corresponding reasons for the ingress event type.

Notify Code	Reason
5302	CRITICAL: ingress bandwidth usage is at or above 90%

Event MO for Flow Rate

nbmEvent

The nbmEvent Managed Object provides information about flow rate events, such as when the flow rate falls below a configured threshold or exceeds a threshold.


```
"nbmEvent": {
                "attributes": {
                "dn":
"sys/nbm/show/notify/dom-default/event-[vrf:default-BW:s-47.20.20.1-g-225.1.1.1]",
                "group": "225.1.1.1",
                "modTs": "2025-04-01T14:09:01.530+00:00",
                "notifyCode": "5304",
                "notifyDn": "vrf:default-BW:s-47.20.20.1-g-225.1.1.1",
                "reason": "Rate below 60% of the configured flow policy",
                "source": "47.20.20.1",
                "tStamp": "1743516541530",
                "vrf": "default"
                }
                }
```


This table provides a list of notification codes and their corresponding reasons for the flow rate event type.

Notify Code	Reason
5303	Rate is over 100% of the configured flow policy
5304	Rate is below 60% of the configured flow policy

Flow Provisioned Event

nbmFlowEvent

The nbmFlowEvent Managed Object provides information about flow provisioning events, such as when a flow is successfully provisioned.


```
"nbmFlowEvent": {
                "attributes": {
                "dn":
"sys/nbm/show/notify/dom-default/flowevent-[vrf:default-FLOW:s-[47.20.20.1]-g-[226.1.1.1]/oif-[Lo1]]",

                "egressinterface": "Lo1",
                "group": "226.1.1.1",
                "modTs": "2025-04-01T14:02:43.330+00:00",
                "notifyCode": "5201",
                "notifyDn": "vrf:default-FLOW:s-[47.20.20.1]-g-[226.1.1.1]/oif-[Lo1]",
                "reason": "Flow provisioned successfully",
                "source": "47.20.20.1",
                "tStamp": "1743516163330",
                "vrf": "default"
                }
                }
```


This table provides a list of notification codes and their corresponding reasons for the flow provisioned event type.

Notify Code	Reason
5201	Flow provisioned successfully

NAT Event

Oversubscription Event

The nbmInatOversubscriptionEvent Managed Object provides information about NAT oversubscription events, such as when the cumulative pre-NAT bandwidth exceeds the post-NAT bandwidth.


```
"nbmInatOversubscriptionEvent": {
                "attributes": {
                "dn":
"sys/nbm/show/notify/dom-default/inatoversubscriptionevent-[vrf:default-post_s-[51.51.51.51]-post_g-[226.1.1.1]-ingress]",

                "group": "226.1.1.1",
                "modTs": "2025-04-01T14:19:04.393+00:00",
                "notifyCode": "5305",
                "notifyDn": "vrf:default-post_s-[51.51.51.51]-post_g-[226.1.1.1]-ingress",
                "reason": "Oversubscription: cumulative pre-NAT bandwidth is higher than
post-NAT bandwidth from the respective flow policies",
                "source": "51.51.51.51",
                "tStamp": "1743517144393",
                "vrf": "default"
                }
                }
```


This table provides a list of notification codes and their corresponding reasons for the NAT oversubscription event type.

Notify Code	Reason
5305	Oversubscription: cumulative pre-NAT bandwidth is higher than post-NAT bandwidth from the respective flow policies

Bandwidth Mismatch Event

The nbmEnatBandwidthmismatchEvent Managed Object provides information about NAT bandwidth mismatch events, such as when there is a mismatch between the pre-NAT and post-NAT flow bandwidth.


```
"nbmEnatBandwidthmismatchEvent": {
                "attributes": {
                "destPort": "0",
                "dn":
"sys/nbm/show/notify/dom-default/enatbandwidthmismatchevent-[vrf:default-post_s-[100.1.1.1]-post_g-[226.1.2.1]-pre_s-[47.20.20.1]-pre_g-[226.1.1.1]-S[0]-D[0]-egress/if-[Eth1/47.1]]",

                "group": "226.1.2.1",
                "modTs": "2025-04-01T14:02:44.123+00:00",
                "notifyCode": "5307",
                "notifyDn":
"vrf:default-post_s-[100.1.1.1]-post_g-[226.1.2.1]-pre_s-[47.20.20.1]-pre_g-[226.1.1.1]-S[0]-D[0]-egress/if-[Eth1/47.1]",

                "preGroup": "226.1.1.1",
                "preSource": "47.20.20.1",
                "reason": "Pre- and post-translation flow bandwidth mismatch",
                "source": "100.1.1.1",
                "sourcePort": "0",
                "tStamp": "1743516164123",
                "vrf": "default"
                }
                }
```


This table provides a list of notification codes and their corresponding reasons for the NAT bandwidth mismatch event type.

Notify Code	Reason
5307	Pre- and post-translation flow bandwidth mismatch

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.

Cisco NX-OS Release 10.6(1)F introduces enhancements to failure handling that provide more detailed and actionable fault information. This allows administrators to effectively understand fault information, identify the root cause of failures, and implement appropriate remediation steps using their preferred network management tools.

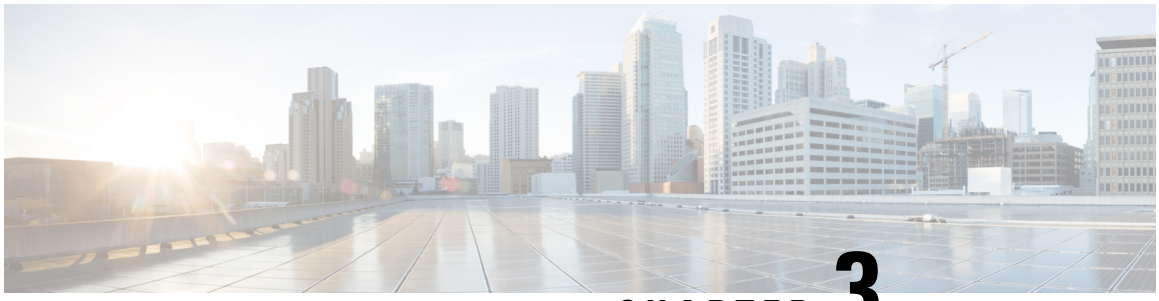
Benefits of the IP Fabric for Media Solution

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 NDFC	Cisco Nexus Dashboard Fabric Controller Installation and Up Guide Cisco DCNM online help
Cisco Nexus Dashboard	Cisco Nexus Dashboard
Cisco NX-OS release information	Cisco Nexus 9000 Series NX-OS IP Fabric for Media Releas
Cisco NX-OS software upgrades	Cisco Nexus 9000 Series NX-OS Software Upgrade and Dow Guide
IGMP snooping and PIM	Cisco Nexus 9000 Series NX-OS Multicast Routing Configurat
IP fabric for media scalability numbers	Cisco Nexus 9000 Series NX-OS Verified Scalability Guide
NX-API REST	Cisco Nexus 3000 and 9000 Series NX-API REST SDK User API Reference
OSPF	Cisco Nexus 9000 Series NX-OS Unicast Routing Configurat
PTP	Cisco Nexus 9000 Series NX-OS System Management Confi Guide
QoS	Cisco Nexus 9000 Series NX-OS Quality of Service Configurat
TCAM carving	Cisco Nexus 9000 Series NX-OS Security Configuration Gui
VLANs	Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configurat



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 21
- Determining the Number of Achievable Flows in the IP Fabric, on page 23

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 93108TC-FX, 93216TC-FX2, 93180YC-FX leaf switches.
   - For 25-Gbps endpoints, use the Cisco Nexus 93180YC-FX, 93240YC-FX2, or 93360YC-FX2 leaf switches.
   - For 40-Gbps endpoints, use the Cisco Nexus 9336C-FX2 leaf switches.
   - For 100-Gbps endpoints, use the Cisco Nexus 9336C-FX2 leaf switches.
3. Determine the number of leaf switches required based on the number of endpoints and uplinks that each leaf switch supports.

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

Table 2: Endpoints and Uplinks Supported Per Leaf Switch

Leaf Switch	Endpoint Capacity	Uplink Capacity
Cisco Nexus 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 93108TC-FX switch	48 x 1/10-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

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
      ```

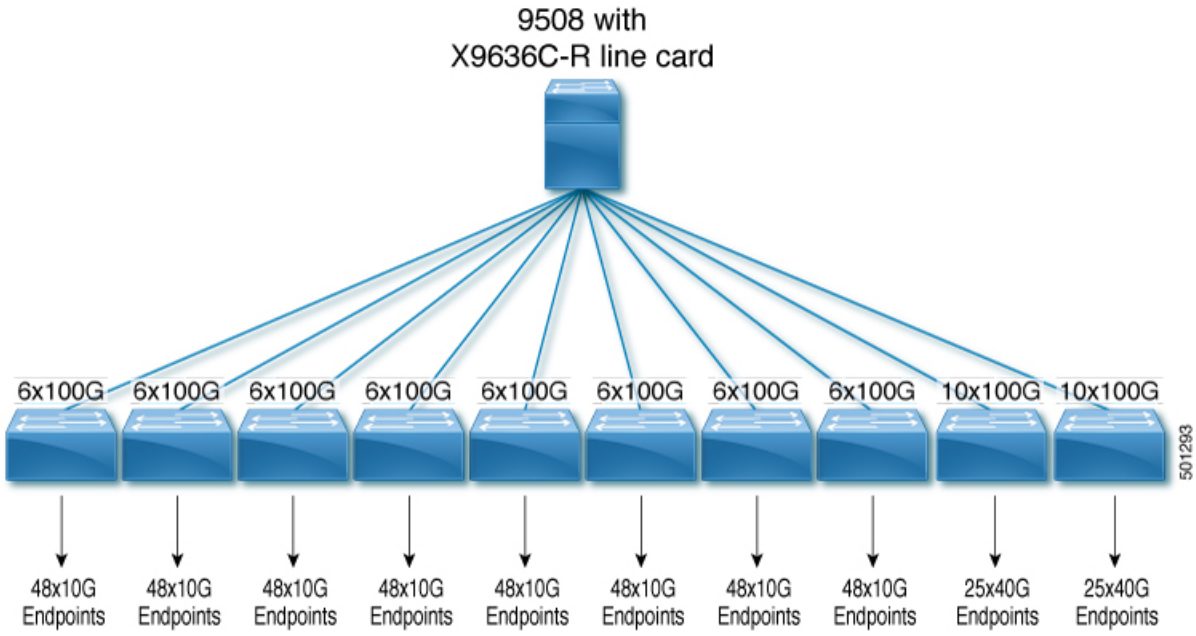
   b. Use this equation to determine the downstream bandwidth:

      ```
      Endpoint Capacity per Leaf Switch x Number of Leaf Switches = 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 IPFM flows can't utilize all the expected bandwidth as the **PIM bidir RP** configuration utilizes the IPFM bandwidth available. To increase the IPFM bandwidth, remove the **PIM bidir RP** configuration.

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



Determining the Number of Achievable Flows in the IP Fabric

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

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

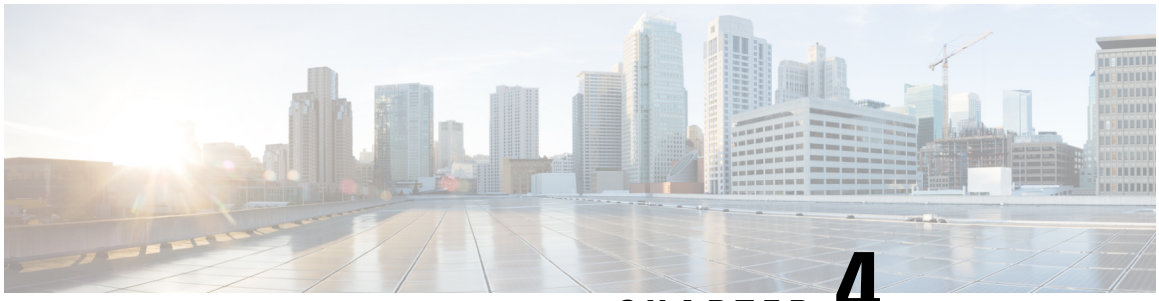
The flow size is configurable and is typically based on the type of video technology that is used in your broadcasting center.

Table 3: Flow Sizes Per Video Technology

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

For example:

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



CHAPTER 4

Configuring IP Fabric for Media

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

- Prerequisites, on page 25
- Guidelines and Limitations, on page 26
- Licensing Requirements for NDFC Media Controller, on page 31
- Upgrading to a Cisco NX-OS 9.x Release, on page 32
- Setting Up the SNMP Server for NDFC, on page 33
- Configuring IPFM, on page 33
- Configuring Unicast PTP Peers, on page 74
- vPC Support, on page 76

Prerequisites

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

Note For Cisco Nexus 9800 switches, TCAM carving configuration is not required.

- 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 Nexus Dashboard Fabric Controller (NDFC) releases. For NDFC installation instructions, see the Cisco Nexus Dashboard Fabric Controller Installation and Upgrade Guide for your NDFC release.

  For more information about compatible releases and supported switches, refer to Software and Hardware Compatibility Matrix for Nexus Dashboard Fabric Controller (formerly DCNM).

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 IPFM, 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 IPFM.
- 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 IPFM.
- 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.
- Enhanced ISSU is not supported with IPFM.
- 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 IPFM external links. If a Layer 3 interface is changed to a switch port, the IPFM external link configuration is removed.

- When you configure a Layer 3 interface as an IPFM 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 IPFM flow policer.
- During a failure, the IPFM Flow Prioritization feature tries to recover priority flows where possible. By design, IPFM Flow Prioritization does not bring down already established flows to accommodate priority flows.
- Beginning with Cisco Nexus Release 10.1(1) IPFM Flow Prioritization with IPFM is supported on Cisco Nexus 9300-FX3 platform switches.
- Beginning with Cisco NX-OS Release 10.1(2), IPFM is supported on the N9K-X9624D-R2, and N9K-C9508-FM-R2 platform switches.
- Beginning with Cisco NX-OS Release 10.2(1q)F, IPFM is supported on the N9K-C9332D-GX2B platform switches.
- For Cisco Nexus 9500 -R line cards, when configured in IPFM Passive mode there will be increasing input discards and this has been determined to be expected and non-impacting.
- Beginning with Cisco NX-OS Release 10.3(1)F, the IPFM feature and VXLAN can co-exist on the same box but in two different VRFs.
- Beginning with Cisco NX-OS Release 10.3(1)F, the following IPFM features are supported on the Cisco Nexus 9808 platform switches:
  - Spine and single-box support (L3 front panel ports only, no L2 ports/SVI support).
  - Flow Policy/Host policy for host administration.
  - Pim-Active and Pim-Passive modes of flow provisioning.
  - Oper MO publishing for flows/ends points published for NDFC enablement.
- Beginning with Cisco NX-OS Release 10.4(1)F, this feature is also supported on Cisco Nexus X98900CD-A line cards with Cisco Nexus 9808 switches.
- Beginning with Cisco NX-OS Release 10.4(1)F, this feature is supported on Cisco Nexus X98900CD-A and X9836DM-A line cards with Cisco Nexus 9804 switches.
- Beginning with Cisco NX-OS Release 10.3(2)F, Multicast service reflection (Multicast NAT) is now extended to sub-interfaces on all host and fabric ports for IPFM mode pim-active and IPFM mode pim-passive on Cisco Nexus 9300, 9408 and 9800 platform switches, and Cisco Nexus 9504 and 9508 switches with -R line cards.

- Parent port and its corresponding subinterfaces are expected to be part of the VRFs which are in same IPFM pim-active or IPFM pim-passive mode.

  For example: If the parent port is part of IPFM VRF which is in PIM active mode, its subinterfaces must also be in the VRF (can be different VRF context) with the same PIM active mode.

- Beginning with Cisco NX-OS Release 10.3(2)F, Sub-interface type is now supported in IPFM mode pim-active and IPFM mode pim-passive.
- Layer 3 port-channels and port-channel subinterfaces are not supported with IPFM. Only routed physical Layer 3 interfaces are supported for use with IPFM.
- Beginning with Cisco NX-OS Release 10.3(2)F, IPFM mode pim-active and IPFM mode pim-passive can coexist on the same switch.
- From Cisco NX-OS Release 10.4(1)F, ISIS is supported with IPFM.
- From Cisco NX-OS Release 10.4(1)F, IPFM is supported on Cisco Nexus 9348GC-FX3 switch.
- From Cisco NX-OS Release 10.4(2)F, IPFM is supported on Cisco Nexus C93108TC-FX3 switch.
- Beginning with Cisco NX-OS Release 10.4(2)F, endpoint MOs published based on Interface IP instead of host IP, for the receiver in SVI interface and reporterIP on the flowMO, the SVI receivers will have interfaceIP instead of hostIP.
- Beginning from Cisco NX-OS Release 10.4(2)F, with IPFM you can now access L2 port information in addition to the existing L3 port flow data, improving better visibility into the flow path. This feature is supported for the following TOR and EOR switches:
  - Nexus 9300-FX/FX2/FX3/H1 Platform Switches
  - Nexus 9300-GX/GX2 Platform Switches
  - Nexus X97160YC-EX, 9700-FX/GX line cards
  - Nexus 9600-R/R2 line cards
- Beginning with Cisco Nexus Release10.4(3)F, IPv6 unicast traffic is supported on Cisco Nexus 9000 Series switches.
- Beginning from Cisco NX-OS Release 10.5(2)F, the IPFM granular priority-based flow feature provides 16 levels of priorities to the IPFM flow and allows prioritization of critical flows over lower priority flows, when link bandwidth constraints are present. This feature provides you the option to control, customize, and assign priority for the flows as required. The priority flow feature is controlled by a new command. However, priority flow is not supported on PIM passive mode.
- Beginning with Cisco NX-OS Release 10.6(3)F, Media Exchange Layer (MXL) traffic can co-exist along with Multicast NBM PIM Active traffic in two different VRFs.
- Beginning with Cisco NX-OS Release 10.6(3)F, PFM-SD multi-site support is provided on Cisco Nexus switches. For more information on PFM-SD multi-site, see the Configuring MSDP.

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

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



Note If you enter a wild card (0.0.0.0) for the host IP address for a local receiver host policy, 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.
- gRPC traffic destined to a NX-OS switch hits the CoPP in the default class. To limit the possibility of gRPC drop, it is recommended to configure a custom CoPP policy using gRPC configured port in the management class.
- 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 Unicast PTP on Cisco Nexus 9300-SE1 Series switches

- Beginning with Cisco NX-OS Release 10.6(1)F, unicast PTP is supported on Cisco Nexus 9336C-SE1 switches.

Guidelines and Limitations for the Cisco NDFC

The following guidelines and limitations apply to NDFC 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 NDFC. Make any modifications using NDFC.
- When you change any IP fabric for media-related server properties using **NDFC Administration** > **NDFC Server** > **Server Properties**, you must restart NDFC. For installation instructions, see the Cisco Nexus Dashboard Fabric Controller Installation and Upgrade Guide.
- NDFC leverages the telemetry feature on the switch to stream out IP fabric for media data and uses ElasticSearch for persistence. By default, NDFC stores the historical telemetry data for up to seven days. You can adjust the data retention period using NDFC server property **pmn.elasticsearch.history.days**.
- When a switch is imported into NDFC, 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 NDFC. NDFC 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.

- NDFC listens for a switch's SNMP reload trap. When NDFC 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 NDFC server property **pmn.deploy-on-import-reload.enabled** to **'false'** and then restart NDFC to make the change effective.

The following guidelines and limitations apply to the flow setup:

- NDFC 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 NDFC 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.
- NDFC supports a multicast range for host policies. By default, NDFC 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 NDFC server property **pmn.hostpolicy.multicast-ranges.enabled** to **'true'** and restart NDFC.

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

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

Licensing Requirements for NDFC Media Controller

Product	License Requirement
Cisco NDFC	The Cisco NDFC Media Controller requires the Advanced Server NDFC licens license, see the Cisco Nexus Dashboard Fabric Controller Installation and Upgr

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.

Procedure

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

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

Step 3 Upgrade NDFC.

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.

Procedure

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

Step 2 Disable IPFM (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 IPFM and reload the switch.

Step 7 Upgrade NDFC.

Step 8 Configure PIM and MSDP, if applicable.

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

Step 10 Configure IPFM policies using the CLI or NDFC.

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

Step 12 Enable all ports facing the endpoints.

Setting Up the SNMP Server for NDFC

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

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

Procedure

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

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

Step 3 Save the configuration and restart NDFC.

Configuring IPFM

The procedure for configuring IP Fabric for Media (IPFM) varies depending on which deployment method you are using for your IP fabric for media solution.

- Spine-leaf topology
- Single modular switch

Configuring IPFM for a Spine-Leaf Topology

Follow this procedure to configure IPFM 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 IPFM along with Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP) for provisioning flows within the fabric. The fabric must be configured with PIM sparse mode and MSDP.

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**
19. (Optional) [**no**] **priority level** <*1-15*>

DETAILED STEPS

Procedure

	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 IPFM feature and PIM active mode, which allows the IPFM fabric to form a multicast flow without assistance from an external controller. When you enter the **feature nbm** command, the following commands are also enabled automatically: • **nbm mode pim-active** • **ip multicast multipath nbm**

	Command or Action	Purpose
		• **ip pim prune-on-expiry** • **cdp enable** The **no** form of this command disables the following commands: **feature nbm**, **nbm mode pim-active**, **ip multicast multipath nbm**, and **ip pim prune-on-expiry**. **Note** If you disable IPFM 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. `hardware access-list tcam region ing-nbm 0` `hardware access-list tcam region redirect_v6` *TCAM-size* **Note** If you want to configure an IPFM VRF, see Configuring an IPFM VRF for Active Flow Provisioning, on page 55.

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

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

Step 5	(Optional) **default** {**permit** | **deny**} **Example:** `switch(config-nbm-host-pol-sender)# default permit`	Specifies the default action for the IPFM host policy. All three types of host policies are allowed by default.
Step 6	(Optional) Enter one of the following commands: • For sender host policies: *sequence-number* **host** *ip-address* **group** *ip-prefix* {**deny** | **permit**} • For local receiver host policies: *sequence-number* **host** *ip-address* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**} • For external receiver (PIM) host policies: *sequence-number* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**} **Example:**	Specifies if the sender or receiver flows are to be permitted or denied. 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

	Command or Action	Purpose

	`switch(config-nbm-host-pol-sender)# 10 host 101.1.1.3 group 229.1.1.1/32 deny`
	Example:
	`switch(config-nbm-host-pol-rcvr)# 40 host 100.1.1.1 source 145.1.1.1 group 234.1.1.1/32 deny`
	Example:
	`switch(config-nbm-host-pol-pim)# 50 source 101.1.1.1 group 235.1.1.1/32 deny`
		source IP address is also a wildcard. See the wildcard configuration example at the end of this procedure.

Step 7	(Optional) [**no**] **nbm reserve unicast fabric bandwidth** *value* **Example:** `switch(config)# nbm reserve unicast fabric bandwidth 2`	Reserves a percentage of bandwidth on fabric ports for unicast flows. IPFM flow management does not use this bandwidth for flow setup and reserves it on all fabric interfaces for the unicast traffic. The range is from 0 to 100 percent, and the default value is 0.
Step 8	[**no**] **nbm flow asm range** [*group-range-prefixes*] **Example:** `switch(config)# nbm flow asm range 224.0.0.0/8 225.0.0.0/8 226.0.0.0/8 227.0.0.0/8`	Programs the IPFM ASM group range for *,G joins. The IGMP joins in this group range are expected to be V2 joins or (*, G) joins. You can configure up to 20 group ranges. The default is no configured group range. **Note** This command is needed only in a multispine deployment.
Step 9	[**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} **Example:** `switch(config)# nbm flow bandwidth 3000 mbps`	Configures the global IPFM flow bandwidth in Kbps, Mbps, or Gbps. The minimum supported flow bandwidth is 200 Kbps. **Range** / **Default Value** 1 to 25,000,000 Kbps / 0 Kbps 1 to 25,000 Mbps / 0 Mbps 1 to 25 Gbps / 0 Gbps **Note** Beginning with Cisco NX-OS Release 10.6(2)F, the maximum supported bandwidth range for flow policies has been increased from 25 Gbps (25,000,000 Kbps) to 100 Gbps (100,000,000 Kbps) on Cisco Nexus 9300-FX, FX2, FX3, GX, GX2, H2R, H1, and 9800 Series switches.
Step 10	[**no**] **nbm flow dscp** *value* **Example:** `switch(config)# nbm flow dscp 10`	Configures the global IPFM flow DSCP value. The range is from 0 to 63. If any of the flows do not match the IPFM 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 IPFM flow policies. The policer is enabled by default.

	Command or Action	Purpose

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 IPFM 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 IPFM 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 IPFM. 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. **Note** Beginning with Cisco NX-OS Release 10.6(2)F, the maximum supported bandwidth range for flow policies has been increased from 25 Gbps (25,000,000 Kbps) to 100 Gbps (100,000,000 Kbps) on Cisco Nexus 9300-FX, FX2, FX3, GX, GX2, H2R, H1, and 9800 Series switches.

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 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. **Critical** is the highest priority.

Step 19	(Optional) [**no**] **priority level** *<1-15>* **Example:** `switch(config-nbm-flow-pol-attr-prop)# priority level 1`	Enables granular flow prioritization from level 1 to 15 for the multicast groups that are being configured. The default value is **low**, which is zero (0); this is also the lowest priority.

Example

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

```
switch(config)# nbm host-policy
  sender
    default permit
    1100 host 0.0.0.0 group 224.1.1.1/32 permit  << Sender wildcard
  receiver
    default permit
    1100 host 0.0.0.0 source 0.0.0.0 group 231.1.1.1/32 permit  << Receiver wildcards

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

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

What to do next

Configure PIM

Configure MSDP

Configure Fabric and Host Interfaces

Configuring an IPFM VRF, on page 55

Establish an IPFM Flow

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 IPFM 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

Procedure

	Command or Action	Purpose

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

Step 2	**ip pim rp-address** *rp-address* **group-list** *ip-prefix* **Example:** `switch(config)# ip pim rp-address 1.2.1.1 group-list 224.0.0.0/4`	Configures a PIM static RP address for a multicast group range. The spine must be configured as the RP. In a multi-spine deployment, all spines must be configured as the RP with the same IP address configured on a loopback interface.

	Command or Action	Purpose
Step 3	**ip pim ssm range none** **Example:** `switch(config)# ip pim ssm range none`	Forces sender traffic to the spine layer, which reduces flow setup latency. **Note** SSM is still supported in the fabric, and this command does not disable SSM.
Step 4	**ip pim spt-threshold infinity group-list** *route-map-name* **Example:** `switch(config)# ip pim spt-threshold infinity group-list mcast-all`	Creates the IPv4 PIM (*, G) state only, for the group prefixes defined in the specified route map.

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

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

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

Step 8	**mtu** *mtu-size* **Example:** `switch(config-if)# mtu 9216`	Configures an MTU size to support jumbo traffic. It should be configured on all host and fabric interfaces.
Step 9	**ip address** *ip-prefix* **Example:** `switch(config-if)# ip address 10.3.10.1/24`	Configures an IP address for this interface.
Step 10	**ip ospf passive-interface** **Example:** `switch(config-if)# ip ospf passive-interface`	Suppresses routing updates on the interface. This command overrides the router or VRF command mode configuration. OSPF runs passive on host-facing interfaces only. This configuration is needed only on endpoint interfaces and is not needed on fabric interfaces.
Step 11	**ip router ospf** *instance-tag* **area** *area-id* **Example:** `switch(config-if)# ip router ospf p1 area 0.0.0.0`	Enables OSPF on the interface.

	Command or Action	Purpose
Step 12	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on the interface.
Step 13	**ip igmp version** *number* **Example:** `switch(config-if)# ip igmp version 3`	Enables IGMPv3 packet support on endpoint interfaces only.
Step 14	**ip igmp immediate-leave** **Example:** `switch(config-if)# ip igmp immediate-leave`	Configures IGMP immediate leave on endpoint interfaces only.

Step 15	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

Procedure

	Command or Action	Purpose

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

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

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

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

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

Priority-based flow

The IPFM priority-based flow feature provides you an option to prioritize certain critical or high-priority flows by impacting lower-priority flows to secure necessary bandwidth or policer in situations where there are constraints for these resources.

This action is governed by a specific command, see Enable priority-based flow feature. Thus, when a high-priority flow or report or join arrives in a feature-supported system, and the system is saturated either with OIF or IIF bandwidth or policer resources, low-priority flows are impacted. The low-priority flows are impacted based on their bandwidth, to release the required bandwidth to accommodate and grant passage to the high-priority flow. The sequence in which the low-priority flows are impacted, based on their bandwidth, is in the ascending order, starting from priority level zero and moving on to priority level 1 to 15. For more information, see Impact of hgh-priority flows on lower priority flows.

The IPFM ensures priority for critical or high-priority flow at the inception or beginning of the flow. This implies that when an IGMP process requests to join a flow classified as high priority, IPFM proactively discontinues some of the lower-priority flows thereby granting passage for the high-priority flows.

Enable priority-based flow feature

The granular priority-based flow feature is disabled by default. To enable this feature use the **nbm flow impact-low-priority** command.

If you want to disable this feature, use the **no** form of this command.

Guidelines and limitations for configuring priority-based flow

This section provides information about guidelines and limitations for the granular priority-based flow configuration.

Feature support through releases

Release	Feature description
9.3(x)	During network events such as link flap, topology change notifications (TCN), or prefix change, the MRIB performs a re-RPF for the impacted flows. While doing so, it prioritizes the critical priority flows to find the alternate RPF, and then visits the low-priority flows.
10.5(2)F	The priority-based flow feature can be enabled or disabled. This feature supports multilevel priority, that is, priority zero (0) and priority levels 1–15.

ISSU and ISSD

- Feature priority-based flow does not support nondisruptive (ND) ISSU.
- Before performing ISSD to releases earlier than 10.5(2)F, remove all the configured multilevel priorities and disable the priority-based flow feature.

Features not supported

Priority-based flow is not supported on PIM passive mode.

Impact of high-priority flows on lower priority flows

The flows are prioritized always. However, the method in which the flows are prioritized differs based on the flow priority feature being enabled or disabled as well as on whether the various levels of priorities are defined

or not. This section explains how the low-priority flow and priority levels 1 to 15 get impacted when a critical flow comes in.

Low-priority flows are impacted if there is a little bandwidth in ingress or egress or both interfaces or if there are no policers.

Note SVI flows have the following guidelines and limitations:

- If no low-priority flows are present, the SVI specific slot, unit, slice, or UMNAT flow is impacted.
- If no low-priority flows are present for SVI, then the first low-priority flow in all slots, units, or slices is impacted.

Example

An example of a multiple-priority flow where you need to accommodate critical priority is explained in this section. This example illustrates how the configured priorities get impacted to accommodate a series of critical flows.

In the following scenario, the bandwidth is exhausted with priority 0 and priority 1 flows, and there is a requirement to accommodate higher priority flows.

The first higher priority flow that comes in is 225.3.3.1.

Priority 0	Bandwidth	Priority 1	Bandwidth	Priority 2	Bandwidth	Priority critical	Bandwidth
225.1.1.1	10	225.2.2.1	40	225.3.3.1	160	225.64.64.1	160
225.1.1.2	20	225.2.2.2	50	225.3.3.2	20	225.64.64.2	110
225.1.1.3	30	225.2.2.3	100	225.3.3.3	10	-	-

The lower priority flows that get impacted are 225.1.1.1, 225.1.1.2, 225.1.1.3, and 225.2.2.3.

Next, there is a need to accommodate the higher-priority flow 225.64.64.2. The table depicts the priority flows and the available bandwidth.

Priority 0	Bandwidth	Priority 1	Bandwidth	Priority 2	Bandwidth	Priority critical	Bandwidth
-	-	225.2.2.1	40	225.3.3.1	160	225.64.64.1	160
-	-	225.2.2.2	50	225.3.3.2	20	225.64.64.2	110
-	-	-	-	225.3.3.3	10	-	-

Based on the priority level and available bandwidth, the flows that will be impacted in this scenario are 225.2.2.1, 225.2.2.2, and 225.3.3.2.

Configuration examples for priority-based flow

This is an example of multilevel priority flow.

```
switch(config-nbm-flow-pol-attr-prop)# priority ?
critical Critical Priority (Highest)
level Configurable levels
switch(config-nbm-flow-pol-attr-prop)# priority level ?
<1-15> Priority level
```

This is an example of priority level configuration.

```
policy iptv
bandwidth 10 kbps
ip group-range 225.1.1.0 to 225.1.1.255
priority level 9
```

Configuring Fabric and Host Interfaces

You can configure the fabric and host interfaces using the CLI commands in this section or use the NDFC 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

Procedure

	Command or Action	Purpose

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

	Command or Action	Purpose

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

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

Configuring a Layer 3 Host Interface

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

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	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.
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

Procedure

	Command or Action	Purpose

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

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

	Command or Action	Purpose

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

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

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

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

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

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

Step 10	(Optional) **ip igmp version 3** **Example:** `switch(config-if)# ip igmp version 3`	Sets the IGMP version to 3. Enter this command if you are using IGMP version 3.
Step 11	**ip router ospf** *instance-tag* **area** *area-id* **Example:** `switch(config-if)# ip router ospf 201 area 0.0.0.15`	Adds the interface to the OSPFv2 instance and area.
Step 12	**ip address** *ip-address* **Example:**	Configures an IP address for this interface.

	Command or Action	Purpose
	`switch(config-if)# ip address 192.0.2.1/8`	
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:** `switch(config-if)# switchport mode trunk`	Configures one of the following options: **access**—Sets the interface as a nontrunking, nontagged, single-VLAN Layer 2 interface. An access port can carry traffic in one VLAN only. By default, an access port carries traffic for VLAN 1. **trunk**—Sets the interface as a Layer 2 trunk port. A trunk port can carry traffic in one or more VLANs on the same physical link. (VLANs are based on the trunk-allowed

	Command or Action	Purpose
		VLANs list.) By default, a trunk interface can carry traffic for all VLANs.
Step 21	**switchport** {**access** | **trunk allowed**} **vlan** *vlan-id* **Example:** `switch(config-if)# switchport trunk allowed vlan 5`	Configures one of the following options: **access**—Specifies the VLAN for which this access port will carry traffic. If you do not enter this command, the access port carries traffic on VLAN 1 only. **trunk allowed**—Specifies the allowed VLANs for the trunk interface. The default is to allow all VLANs on the trunk interface: 1 to 3967 and 4048 to 4094. VLANs 3968 to 4047 are the default VLANs reserved for internal use by default.
Step 22	**no shutdown** **Example:** `switch(config-if)# no shutdown`	Clears the errors on the interfaces and VLANs where policies correspond with hardware policies. This command allows policy programming to continue and the port to come up.

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

Configuring IPFM for a Single Modular Switch

After you have set up the IP fabric, you must enable the IPFM feature on the switch. The IPFM 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 IPFM 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**
13. (Optional) [**no**] **priority level** <*1-15*>

DETAILED STEPS

Procedure

	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 IPFM feature. The **no** form of this command disables this feature. **Note** If you disable IPFM 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. `hardware access-list tcam region ing-nbm 0` `hardware access-list tcam region redirect_v6` *`TCAM-size`* **Note** If you want to configure an IPFM VRF, see Configuring an IPFM VRF for Active Flow Provisioning, on page 55.
Step 3	[**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} **Example:** `switch(config)# nbm flow bandwidth 150 mbps`	Configures the global IPFM flow bandwidth in Kbps, Mbps, or Gbps. The minimum supported flow bandwidth is 200 Kbps. **Range** / **Default Value** 1 to 25,000,000 Kbps / 0 Kbps 1 to 25,000 Mbps / 0 Mbps 1 to 25 Gbps / 0 Gbps **Note** Beginning with Cisco NX-OS Release 10.6(2)F, the maximum supported bandwidth range for flow policies has been increased from 25 Gbps (25,000,000 Kbps) to 100 Gbps (100,000,000 Kbps) on Cisco Nexus 9300-FX, FX2, FX3, GX, GX2, H2R, H1, and 9800 Series switches.

	Command or Action	Purpose
Step 4	(Optional) [**no**] **nbm flow policer** **Example:** `switch(config)# no nbm flow policer`	Enables or disables the policer for all IPFM flow policies. The policer is enabled by default.

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

Step 6	[**no**] **policy** *policy-name*
	Example:
	`switch(config-nbm-flow-pol)# policy 1.5gbps`
	`switch(config-nbm-flow-pol-attr)#`
		Configures the IPFM 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 IPFM 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 IPFM. For information on configuring an aggregate policer, see the *Configuring Shared Policers* section in the *Configuring Policing* chapter of *Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide* on Cisco.com.
Step 8	[**no**] **bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} **Example:** `switch(config-nbm-flow-pol-attr)# bandwidth 1500 mbps`	Configures the flow bandwidth in Kbps, Mbps, or Gbps for multicast groups matching this policy. The minimum supported flow bandwidth is 200 Kbps. **Note**

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
		Beginning with Cisco NX-OS Release 10.6(2)F, the maximum supported bandwidth range for flow policies has been increased from 25 Gbps (25,000,000 Kbps) to 100 Gbps (100,000,000 Kbps) on Cisco Nexus 9300-FX, FX2, FX3, GX, GX2, H2R, H1, and 9800 Series switches.

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

Step 10	(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. **Critical** is the highest priority.

Step 13	(Optional) [**no**] **priority level** <*1-15*> **Example:** `switch(config-nbm-flow-pol-attr-prop)# priority level 1`	Enables granular flow prioritization from level 1 to 15 for the multicast groups that are being configured. The default value is **low**, which is zero (0); this is also the lowest priority.

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 IPFM VRF, on page 55

Establish an IPFM Flow

Configuring an IPFM VRF

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

IPFM VRFs support multi-tenancy at the fabric level, allowing multiple customers to leverage the same IP fabric for media infrastructure simultaneously. IPFM 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 IPFM fabric to form a multicast flow either with or without assistance from an external controller.

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

Configuring an IPFM VRF for Active Flow Provisioning

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

Before you begin

Configure IPFM.

Before you associate an IPFM 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**
21. (Optional) [**no**] **priority level** *<1-15>*

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

Step 2	[**no**] **nbm vrf** *vrf-name* **Example:** `switch(config)# nbm vrf nbm`	Creates an IPFM VRF.
Step 3	**nbm mode pim-active** **Example:** `switch(config)# nbm mode pim-active`	Allows the IPFM fabric to form a multicast flow without assistance from an external controller. **Note** You cannot disable PIM active mode for a custom IPFM VRF. You can change the IPFM 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: "IPFM cannot be set to PIM-PASSIVE mode while custom config exists. Please delete all custom IPFM config and retry."

Step 4	(Optional) [**no**] **nbm host-policy**
	Example:
	`switch(config)# nbm host-policy`
	`switch(config-nbm-host-pol)#`
		Configures an IPFM host policy for the switch.

Step 5	(Optional) {**sender** | **receiver** | **pim**} **Example:**	Configures the IPFM host policy for a sender, local receiver, or external receiver (PIM).

	Command or Action	Purpose
	`switch(config-nbm-host-pol)# sender` `switch(config-nbm-host-pol-sender)#`	**Note** Before you update the default IPFM 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 IPFM 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: *sequence-number* **host** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
	• For local receiver host policies: *sequence-number* **host** *ip-address* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
	• For external receiver (PIM) host policies: *sequence-number* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
	Example:
	`switch(config-nbm-host-pol-sender)# 10 host 101.1.1.3 group 229.1.1.1/32 deny`
	Example:
	`switch(config-nbm-host-pol-rcvr)# 40 host 100.1.1.1 source 145.1.1.1 group 234.1.1.1/32 deny`
	Example:
	`switch(config-nbm-host-pol-pim)# 50 source 101.1.1.1 group 235.1.1.1/32 deny`
		Specifies if the sender or receiver flows are to be permitted or denied.
		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* **Example:** `switch(config)# nbm reserve unicast fabric bandwidth 2`	Reserves a percentage of bandwidth on fabric ports for unicast flows. IPFM 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*] **Example:** `switch(config)# nbm flow asm range 224.0.0.0/8 225.0.0.0/8 226.0.0.0/8 227.0.0.0/8`	Programs the IPFM ASM group range for *,G joins. The IGMP joins in this group range are expected to be V2 joins or (*, G) joins. You can configure up to 20 group ranges. The default is no configured group range. **Note** This command is needed only in a multispine deployment.
Step 10	[**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} **Example:** `switch(config)# nbm flow bandwidth 3000 mbps`	Configures the global IPFM flow bandwidth in Kbps, Mbps, or Gbps. The minimum supported flow bandwidth is 200 Kbps. **Range**: 1 to 25,000,000 Kbps **Default Value**: 0 Kbps

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Range</th><th>Default Value</th></tr>
<tr><td>1 to 25,000 Mbps</td><td>0 Mbps</td></tr>
<tr><td>1 to 25 Gbps</td><td>0 Gbps</td></tr>
</table>
Note
Beginning with Cisco NX-OS Release 10.6(2)F, the maximum supported bandwidth range for flow policies has been increased from 25 Gbps (25,000,000 Kbps) to 100 Gbps (100,000,000 Kbps) on Cisco Nexus 9300-FX, FX2, FX3, GX, GX2, H2R, H1, and 9800 Series switches.
</td></tr>
<tr><td>Step 11</td><td>[no] nbm flow dscp value
Example:
<code>switch(config)# nbm flow dscp 10</code></td><td>Configures the global IPFM flow DSCP value. The range is from 0 to 63. If any of the flows do not match the IPFM flow group range, the default flow DSCP is used for bandwidth management and flow setup.</td></tr>
<tr><td>Step 12</td><td>(Optional) [no] nbm flow reserve-bandwidth receiver-only
Example:
<code>switch(config)# nbm flow reserve-bandwidth receiver-only</code></td><td>Enables optimization of bandwidth utilization by determination of no valid receivers on the RP and releases 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.</td></tr>
<tr><td>Step 13</td><td>(Optional) [no] nbm flow policer
Example:
<code>switch(config)# no nbm flow policer</code></td><td>Enables or disables the policer for all IPFM flow policies. The policer is enabled by default.</td></tr>
<tr><td>Step 14</td><td>[no] nbm flow-policy
Example:
<code>switch(config)# nbm flow-policy
switch(config-nbm-flow-pol)#</code></td><td>Configures the flow bandwidth per flow.</td></tr>
<tr><td>Step 15</td><td>[no] policy policy-name
Example:
<code>switch(config-nbm-flow-pol)# policy nbmflow10
switch(config-nbm-flow-pol-attr)#</code></td><td>Configures the IPFM flow policy. You can specify a maximum of 63 alphanumeric characters for the policy name.</td></tr>
<tr><td>Step 16</td><td>(Optional) [no] policer
Example:
<code>switch(config-nbm-flow-pol-attr)# no policer</code></td><td>Enables or disables the policer for the specified IPFM 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</td></tr>
</table>

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td></td><td></td><td>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 IPFM. For information on configuring an aggregate policer, see the Configuring Shared Policers section in the Configuring Policing chapter of Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide on Cisco.com.</td></tr>
<tr><td>Step 17</td><td>[no] bandwidth flow-bandwidth {kbps | mbps | gbps}
Example:
<pre>switch(config-nbm-flow-pol-attr)# bandwidth 10 mbps</pre></td><td>Configures the flow bandwidth in Kbps, Mbps, or Gbps for multicast groups matching this policy. The minimum supported flow bandwidth is 200 Kbps.
<table><tr><th>Range</th><th>Default Value</th></tr><tr><td>1 to 25,000,000 Kbps</td><td>0 Kbps</td></tr><tr><td>1 to 25,000 Mbps</td><td>0 Mbps</td></tr><tr><td>1 to 25 Gbps</td><td>0 Gbps</td></tr></table>Note
Beginning with Cisco NX-OS Release 10.6(2)F, the maximum supported bandwidth range for flow policies has been increased from 25 Gbps (25,000,000 Kbps) to 100 Gbps (100,000,000 Kbps) on Cisco Nexus 9300-FX, FX2, FX3, GX, GX2, H2R, H1, and 9800 Series switches.</td></tr>
<tr><td>Step 18</td><td>[no] dscp value
Example:
<pre>switch(config-nbm-flow-pol-attr)# dscp 10</pre></td><td>Configures the differentiated services code point (DSCP) value on the first-hop redundancy for flows matching the specified group range.</td></tr>
<tr><td>Step 19</td><td>[no] ip group-range ip-address to ip-address
Example:
<pre>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</pre></td><td>Specifies the IP address range for multicast groups that are associated to this policy.</td></tr>
<tr><td>Step 20</td><td>(Optional) [no] priority critical
Example:
<pre>switch(config-nbm-flow-pol-attr-prop)# priority critical
switch(config-nbm-flow-pol-attr-prop)#</pre></td><td>Enables critical flow prioritization for the multicast groups that are being configured. Critical is the highest priority.</td></tr>
</table>

	Command or Action	Purpose
Step 21	(Optional) [**no**] **priority level** *<1-15>* **Example:** `switch(config-nbm-flow-pol-attr-prop)# priority level 1`	Enables granular flow prioritization from level 1 to 15 for the multicast groups that are being configured. The default value is **low**, which is zero (0); this is also the lowest priority.

What to do next

Establish an IPFM Flow

Configuring an IPFM VRF for Static Flow Provisioning

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

In this mode, the switch cannot accept any IPFM 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 IPFM.

Before you associate an IPFM 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 IPFM 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: "IPFM cannot be set to PIM-PASSIVE mode while custom config exists. Please delete all custom IPFM config and retry."

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

	Command or Action	Purpose
Step 2	[**no**] **nbm vrf** *vrf-name* **Example:** `switch(config)# nbm vrf nbm`	Creates an IPFM VRF.
Step 3	**nbm mode pim-passive** **Example:** `switch(config)# nbm mode pim-passive`	Allows the IPFM 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.

Configuring IPFM Subinterface Type

Beginning with Cisco NX-OS Release 10.3(2)F, the subinterface with IPFM is supported where you can manage the bandwidth for the subinterface as well. This is applicable for subinterface host/fabric ports on both PIM active/PIM passive IPFM modes.

Total bandwidth capacity % on the parent port and its subinterfaces must not exceed 100%. By default the parent port is allocated with 100% bandwidth capacity. To configure the subinterface with capacity, the parent interface has to be first configured with the capacity %.

A corresponding configuration Model Object (MO) is provided to provision the bandwidth capacity reservation.

Along with bandwidth capacity reservation, existing IPFM interface configurations are supported with subinterface as well.

Note The **nbm bandwidth capacity** command is applicable only for the IPFM VRF which is in PIM active mode. With the PIM passive VRF, the broadcast controller will take care of the bandwidth management.

- Configuring Unicast Bandwidth Reservation Per Port
- `nbm external-link`

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **[no] nbm bandwidth capacity** *percentage*
4. **[no] nbm bandwidth unicast** *percentage*

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

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

Step 3	**[no] nbm bandwidth capacity** *percentage* **Example:** `switch(config-subif)# nbm bandwidth capacity 1`	Configures the bandwidth for IPFM subinterface. Percentage range is 0-100, where 0 denotes no reservation for IPFM bandwidth on this link. To unconfigure IPFM bandwidth, use the **no nbm bandwidth capacity** command.
Step 4	**[no] nbm bandwidth unicast** *percentage* **Example:** `switch(config-subif)# nbm bandwidth unicast 10`	Configures the bandwidth for unicast. Percentage range is 0-100, where 0 denotes no reservation for unicast bandwidth on this link. To unconfigure unicast bandwidth, use the **no nbm bandwidth unicast** command.

Establishing a Flow (Optional)

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

Creating an IPFM Flow Definition

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

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

Figure 1: Traffic from a Source to a Leaf

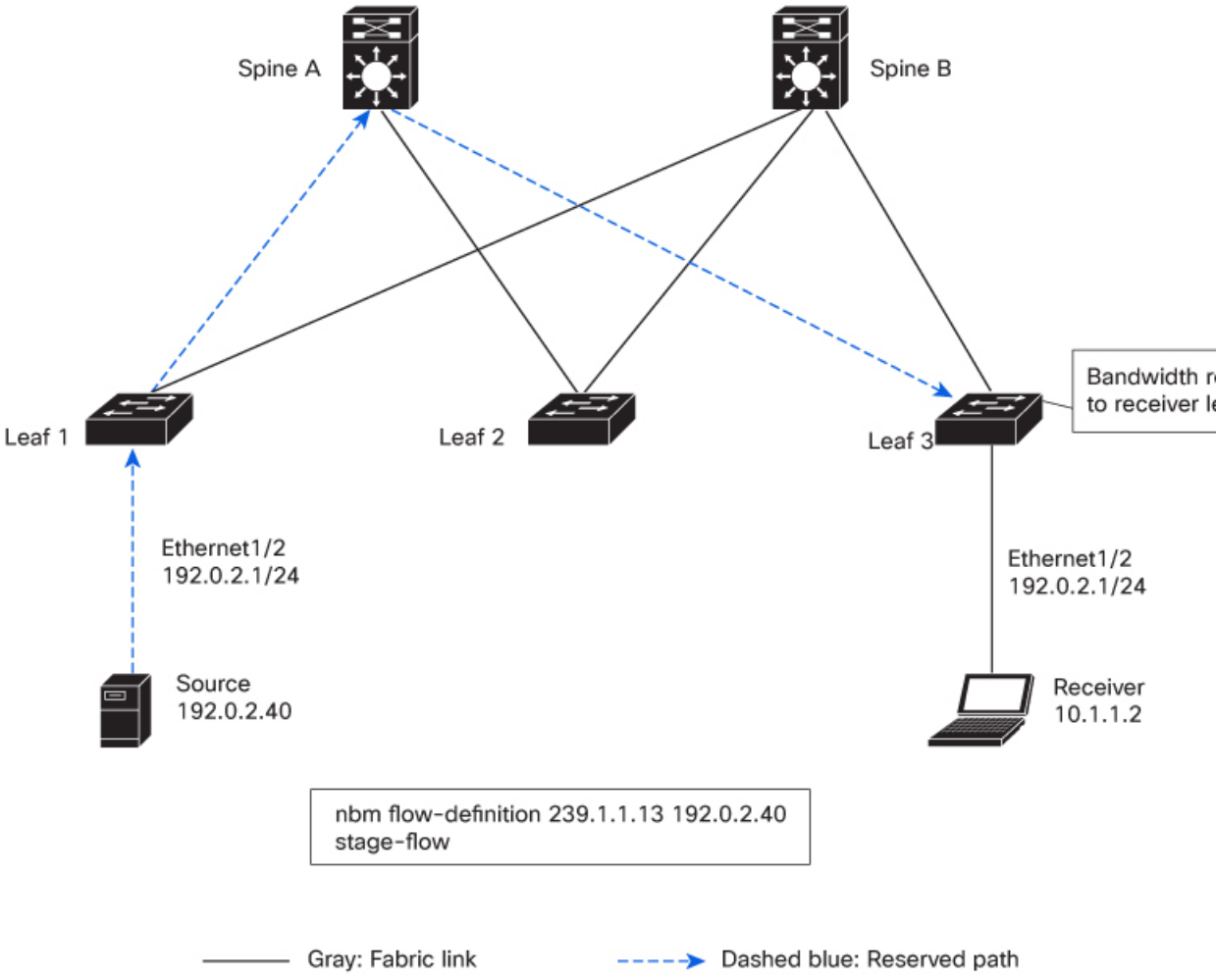
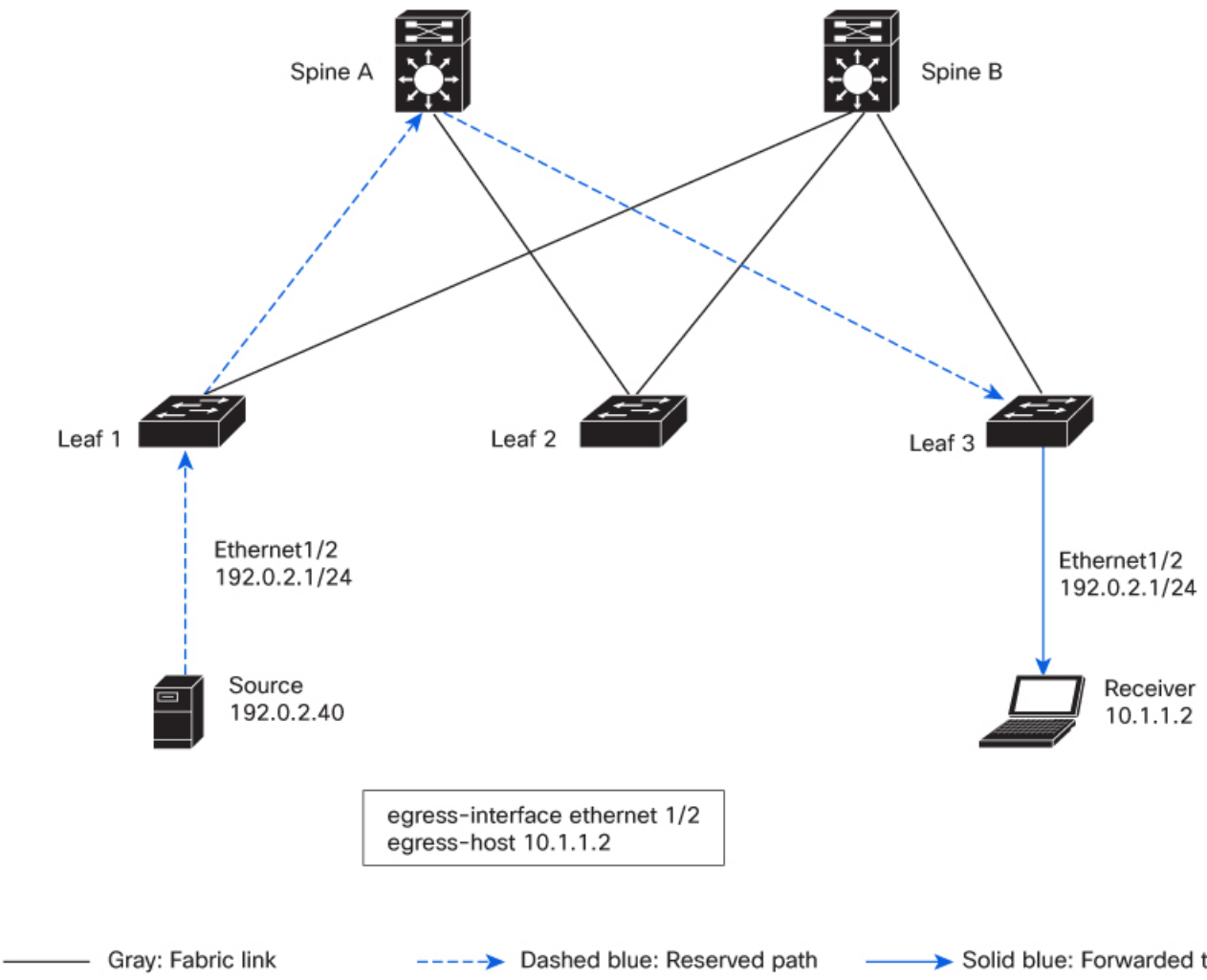


Figure 2: Traffic from the Leaf to a Receiver



Before you begin

Enable IPFM.

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

Procedure

	Command or Action	Purpose

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

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

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

Example

The following example shows a sample configuration:

```
nbm flow-definition 225.0.0.16 11.1.1.40
  stage-flow
  egress-interface ethernet 1/3
  egress-host 145.1.1.23
  egress-host 145.1.1.22
  egress-host 145.1.1.24
  egress-host 145.1.1.25
  egress-host 145.1.1.26
  egress-host 145.1.1.27
  egress-host 145.1.1.28
  egress-host 145.1.1.29
nbm flow-definition 225.0.0.11 100.1.1.40
  stage-flow
```

```
  egress-interface ethernet 1/4
  egress-host 100.1.1.21
nbm flow-definition 235.1.1.13 100.1.1.40
  stage-flow
  egress-interface vlan 12
  egress-host 101.1.1.11
  egress-host 101.1.1.12
  egress-host 101.1.1.13
  egress-host 101.1.1.14
```

Configuring IGMP Static OIF

You can establish a flow by configuring a static IGMP OIF, but we recommend that you create an IPFM 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

Procedure

	Command or Action	Purpose

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

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

Step 3	[**no**] **ip igmp static-oif** *group* [**source** *source*] **Example:** `switch(config-if)# ip igmp static-oif 230.0.0.0`	Establishes a flow for the specified multicast group. **Note** This command does not support the **route-map** option.

Configuring Unicast Bandwidth Reservation Per Port

The Unicast bandwidth (BW) is currently managed only at the fabric level. There is no provision to granularly reserve bandwidth for unicast per port. In case of multisite scenario, there is a need for a config knob which can manage the unicast bandwidth per port. The new config knob that is introduced reserves the unicast bandwidth on a per port basis. A corresponding configuration Model Object (MO) is provided to provision the unicast bandwidth reservation.

On configuring the per-port unicast BW percentage (%) reservation, the switch will check for the bandwidth to set aside for unicast purpose on both the ingress and egress directions. If sufficient bandwidth is available and either one direction or both directions satisfy the configured percentage, the switch will immediately reserve the BW for the unicast utilization purpose. If the configured percentage is unavailable in either of the directions, the switch will do the partial reservation for the unicast purpose. Later, when a multicast flow gets a teardown, the switch will repurpose the freed bandwidth to unicast purpose and continues to do so until it reaches the configured percentage.

Per-port % reserve configuration for unicast BW always takes precedence over the per-vrf fabric unicast BW reservation. If the per-port configuration is removed and the link has a Cisco Discovery Protocol (CDP) neighbor established, the switch uses per-vrf fabric unicast BW percentage. Configuring per-port value to 0 on a link indicates no reservation for unicast on that link. This can be possible, if the link has CDP neighbor established and the per-vrf fabric unicast BW % is configured. For the switch to use the per-vrf fabric unicast BW % to reserve, remove the per-port % BW reserve on the link.

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-type slot/port*
3. **[no] nbm unicast bandwidth percentage**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

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

Step 3	**[no] nbm unicast bandwidth percentage**
	Example:
	`switch(config-if)# nbm bandwidth unicast ?`
	`<0-100> Percentage value`
	`switch(config-if)# no nbm bandwidth unicast`
		0 denotes no reservation for unicast on this link.
		To unconfig unicast BW, use **no nbm bandwidth unicast**

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 IPFM 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.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	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 IPFM feature. The **no** form of this command disables this feature.

Step 3	**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 4	**ip pim sparse-mode** **Example:** `switch(config)# ip pim sparse-mode`	Configures PIM on the IPFM external link.
Step 5	**nbm external-link** **Example:** `switch(config-if)# nbm external-link`	Configures the IPFM 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 supports multicast and unicast flows. IPFM automatically assigns IPFM-managed multicast traffic to QoS Group 7 and allows user to set custom defined queue for the unicast traffic or use the system configured queue. The QoS Group 7 assignment is a system-controlled IPFM setting. User-configured QoS policies cannot override this assignment. This behavior prevents unicast traffic from congesting IPFM-managed 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 NDFC.

Before you begin

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

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

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

SUMMARY STEPS

1. **configure terminal**
2. **ip access-list** *acl-name*
3. *sequence-number* **permit** *protocol source destination*
4. **exit**
5. **ip access-list** *acl-name*
6. *sequence-number* **permit** *protocol source destination*
7. **exit**
8. **class-map type qos match-all** *unicast-class-name*
9. **match access-group name** *acl-name*
10. **exit**
11. **class-map type qos match-any** *multicast-class-name*
12. **match access-group name** *acl-name*
13. **exit**
14. **policy-map type qos** *policy-map-name*
15. **class** *unicast-class-map-name*
16. **set qos-group 0**

17. **exit**
18. **class** *multicast-class-map-name*
19. **set qos-group 7**
20. **exit**
21. **exit**
22. **interface ethernet** *slot/port*
23. **service-policy type qos input** *policy-map-name*
24. (Optional) **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

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

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

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

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

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

Step 6	*sequence-number* **permit** *protocol source destination* **Example:** `switch(config-acl)# 2 permit ip any 224.0.0.0/4`	Creates a rule to match all multicast flows.
Step 7	**exit** **Example:**	Exits IP ACL configuration mode.

	Command or Action	Purpose
	`switch(config-acl)# exit` `switch(config)#`	

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

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

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

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

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

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

	Command or Action	Purpose

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

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

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 IPFM multicast class map. **Note** If IPFM feature is enabled, IPFM automatically assigns IPFM-managed multicast traffic to QoS Group 7.

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

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

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

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

Example

Configuration example:

```
ip access-list pmn-ucast
  10 permit ip any 0.0.0.0 31.255.255.255
```

```
  20 permit ip any 128.0.0.0 31.255.255.255
  30 permit ip any 192.0.0.0 31.255.255.255

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

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

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

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

Verifying the IPFM Configuration

To display the IPFM 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 IPFM 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 [[**group** *group-ip*] | **source** *source-ip*] **priority** | **stitched** | **unstitched** [**all** | **critical** | **level** | **low**]] | [**vrf** {**all** | *vrf-name*}]]	Displays the static flows for an IPFM flow definition. You can add optional keywords to narrow the output.
show nbm flows static [**vrf** {**all** | *vrf-name*}]	Displays the static flows for an IPFM flow definition.
show nbm flows static group *group-address*	Displays the static flows for an IPFM 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 IPFM 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 IPFM 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 IPFM host policies or applied IPFM host policies for external receivers (PIM), local receivers, or senders.
show nbm interface bandwidth	Displays the IPFM interface bandwidth.
show running-config nbm	Displays the running configuration information for IPFM.

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 163.

Clearing IPFM Flow Statistics

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

clear nbm flow statistics
`switch# clear nbm flows statistics`
`Clearing all NBM flow statistics for all VRFs ...`
`Done.`
	Clears IPFM flow statistics for all VRFs.

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

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

Procedure

	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 interface on which you are enabling unicast PTP and enters the interface configuration mode.

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.

	Command or Action	Purpose
Step 8	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	Copies the running configuration to the startup configuration.

Example

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

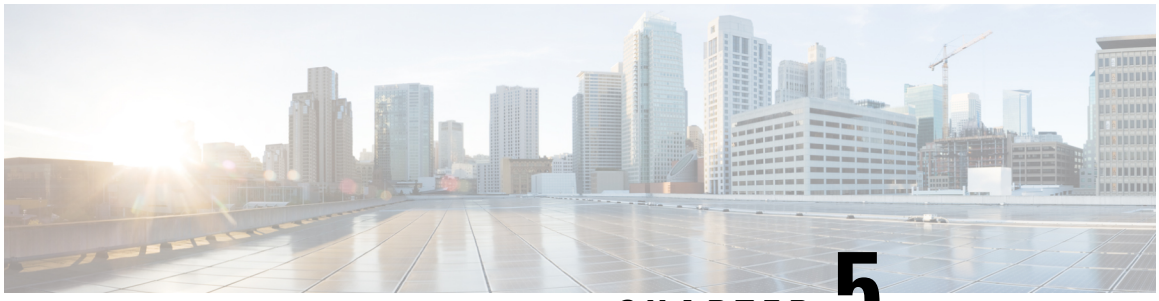
```
interface Ethernet1/1
  ptp transport ipv4 ucast master
    slave ipv4 81.0.0.2
  ptp ucast-source 81.0.0.1
  ip address 81.0.0.1/24
  ip router ospf 1 area 0.0.0.2
  no shutdown

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

show ptp counters interface eth1/1 ipv4 81.0.0.2
PTP Packet Counters of IP 81.0.0.2:
---------------------------------------------------------------
Packet Type                 TX                      RX
----------------    --------------------    --------------------
Announce                    9                       0
Sync                        70                      0
FollowUp                    70                      0
Delay Request               0                       18
Delay Response              18                      0
PDelay Request              0                       0
PDelay Response             0                       0
PDelay Followup             0                       0
Management                  0                       0
---------------------------------------------------------------
```

vPC Support

Beginning with Cisco NX-OS Release 10.3(1)F, vPC is supported with feature IPFM.



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 77
- Guidelines and Limitations for RTP Flow Monitoring, on page 77
- Configuring RTP Flow Monitoring, on page 78
- Displaying RTP Flows and Errors, on page 79
- Clearing RTP Flows, on page 81

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.

- On Cisco Nexus 9300-GX2, H2R, H1, and 9408 Series switches, multicast RTP flow monitoring with the optimization knob is not supported in the following scenarios:
  - when port-channels with PIM enabled are configured
  - when SVIs are configured
- These guidelines apply to RTP flow history entry management:
  - Use the command **flow rtp history** *value* to configure the desired maximum number of RTP errored flow history entries to be stored. This value acts as a guideline for the history buffer size.
  - Be aware that the actual number of stored entries shown by the **show flow rtp errors history** command may exceed the configured value due to internal system mechanisms. This behavior ensures that critical and recent RTP error events are comprehensively logged and retained for effective troubleshooting.

    For example, if you configure **flow rtp history 500**, you may observe more than 500 entries when running **show flow rtp errors history**.
- Beginning with Cisco NX-OS Release 10.6(1)F, DME operational objects are available for monitoring RTP flow-loss events through telemetry. For telemetry configuration and downgrade compatibility information, see Cisco Nexus 9000 Series NX-OS Programmability Guide.
- Beginning with Cisco NX-OS Release 10.6(2)F, RTP flow error checks are sampled at a 1-in-10 rate to limit update volume when scale reaches 16,000. Every tenth packet triggers an update to the RtpFlowLossNotifv4 or RtpFlowLossNotifv6 in the DME database.

  This feature is supported on Nexus 9300-FX/FX2/FX3/GX/GX2/H2R/H1 TOR switches

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

Procedure

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

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-channel500 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-channel500  2820074      199000      00:22:04
 PST Apr 07 2019
50::2        20::2  4151  30000  31999  Ethernet1/49/1   3058232      199000      00:21:16
 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
```

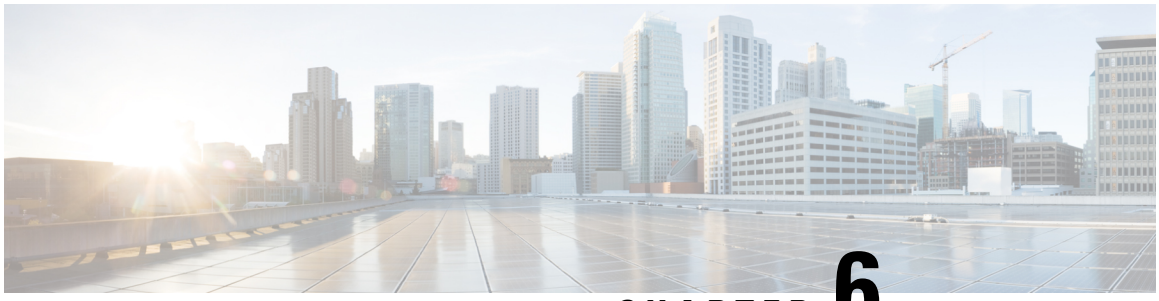
Note When an RTP flow is no longer in the “active-errored” state, the following syslog message appears:

```
%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:** `switch(config)# flow rtp timeout 100`	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 IPFM

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

- Multicast Service Reflection with IPFM, on page 83

Multicast Service Reflection with IPFM

Multicast Service Reflection with IPFM 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.

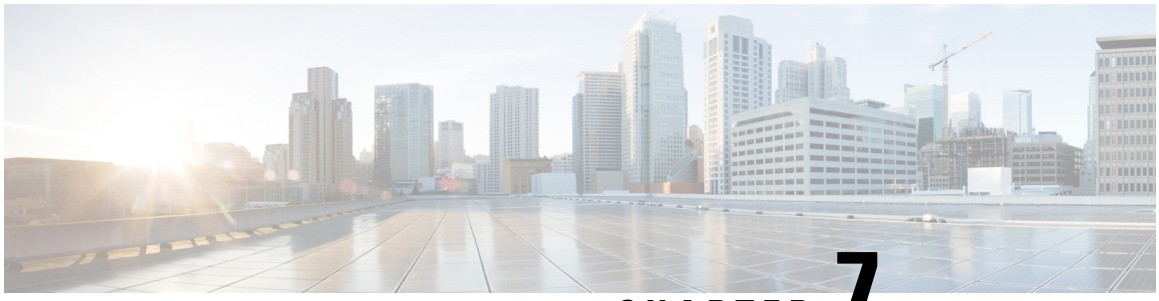
For more information and commands regarding the Multicast Service Reflection feature, see the Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide.

Note If IPFM 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 IPFM cannot support the requested translation.

Note Multicast Service Reflection with IPFM 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 IPFM is supported on Cisco Nexus 9300-FX3, Cisco Nexus C9316D-GX, Cisco Nexus C93600CD-GX, and Cisco Nexus C9364C-GX platform switches.



CHAPTER 7

Non-Blocking Multicast Service Reflection

- NAT Guidelines and Limitations, on page 85
- Multicast to Multicast Ingress NAT, on page 85
- Multicast to Multicast Egress NAT, on page 86
- Examples for ENAT PIM Passive, on page 86
- Multicast to Unicast NAT, on page 87
- Examples for MU NAT PIM Passive, on page 87
- Unicast to Multicast NAT, on page 88

NAT Guidelines and Limitations

The IPFM Service Reflection has the following guidelines and limitations:

- Beginning with Cisco NX-OS Release 10.2(3)F, Unicast to Multicast NAT, Multicast to Unicast NAT, Multicast to Multicast NAT, and Egress NAT are supported on non-default VRF.
- If NAT config is present, config rollback is not supported (and will fail).
- In some cases, service interface re-configuration will be rejected, and to change it, a specific sequence may be required. Also, after re-configuration, NAT rules may not recover automatically and additional actions are required.
- Beginning with Cisco NX-OS Release 10.3(2)F, NAT is supported with sub-interface with "feature nbm" enabled.
- Beginning with Cisco NX-OS Release 10.3(2)F, egress service reflection (egress multicast NAT, and multicast to unicast NAT) supports Post-NAT Source IP to be IP Address of an egress interface. This enhancement is supported for regular multicast, and for IPFM.

Multicast to Multicast Ingress NAT

The Ingress NAT allows translation of incoming (S,G) into a different source, group or both. All receivers inside the domain then can join the post translated flow. This feature is useful when multicast traffic:

- enters a network from a different domain with potentially overlapping address
- comes with an address that is not understood by applications in the network

The dynamic IGMP join or PIM join on a pre-translated route is not supported for ingress NAT.

Multicast to Multicast Ingress NAT works only in PIM active mode. The PIM passive mode is not supported.

Multicast to Multicast Egress NAT

The Egress NAT allows translating existing flow (S,G) to different source or group address on a per outgoing interface basis. This feature is useful for multicast distribution to external entities which may only accept a certain source or group address. It can also serve as a path to hide internal address space when flows are exposed to external entities.

The dynamic IGMP join or PIM join on a post-translated route is not supported for egress NAT.

Fault MO's are generated when there is a mismatch in bandwidth for pre-translated and post-translated flows.

In PIM-Passive mode, bandwidth management is done by an external controller for the flows and provisions both pre-translated and post-translated flows. The flow creation is made available through APIs.

Multicast to Multicast Egress NAT are supported in both PIM passive mode and active mode.

Examples for ENAT PIM Passive

Setting up the Service interface loopback1

```
URL:
{{ip}}/api/mo/sys/mrib/inst/dom-default/sr.json
Payload:
{ "mribServiceReflect": {
"attributes": {"status": "" },
"children": [
{
"mribSrcIntf": {
"attributes": {
"srcIntf": "lo1",
"status": ""
}
}
}
]
}
}
```

Setting up the NAT mode to Egress

```
URL:
{{ip}}/api/mo/sys/mrib/inst/dom-default/sr.json
Payload:
{"mribEgressMode": {"attributes": {"grpList": "225.0.0.0/8"}}}
```

Setting up the mapping interface

```
URL:
{{ip}}/api/mo/sys/mca/config/natsr/mappings.json
Payload:
{"mcaNatMapDefaultSif": {"attributes": {"domName": "default", "maxEnatReplications": "40",
 "siIfName": "eth1/2", "status": "" }}}
```

Setting up the SR rule:

```
URL:
{{ip}}/api/mo/sys/mrib/inst/dom-default/sr/rule.json
Payload:
{"mribSrRule": {"attributes": {"status": ""},
"children": [{"mribRule": {"attributes": {"postTransGrp": "226.1.1.1", "postTransSrc":
"57.1.1.2", "preTransGrp": "225.1.1.1", "preTransSrc": "47.1.1.2", "grpMasklen": 32,
"srcMasklen": 32, "udpsrcPort": "10003", "udpDestPort": "20003", "staticOif": "eth1/29/1"}}}
 ]
} }
```

Pre-NAT flow

```
URL:
{{ip}}/api/mo/sys/nbm/conf/flows.json
Payload:
{"nbmFlows": {"children": [{"nbmConfFlowsDom": {"attributes": {"name": "default", "status":
 ""},
"children": [ {"nbmConfFlow": { "attributes": {"group": "225.1.1.1", "source": "47.1.1.2",
 "ingressIf": "eth1/3" "policer": "ENABLED","bwKbps": "1000" "status": ""} } },
] }} ] } }
```

Post-NAT Flow

```
URL:
{{ip}}/api/mo/sys/nbm/conf/flows.json
Payload:
{"nbmFlows": {"children": [{"nbmConfFlowsDom": {"attributes": {"name": "default"},
"children": [ {"nbmConfFlow": {"attributes": {"group": "226.1.1.1", "source": "57.1.1.1",
"ingressIf": "loopback1", "bwKbps": 10000, "policer": "ENABLED", "status": "" },
"children": [{"nbmConfFlowIf": {"attributes": {"id": "eth1/29/1", "isLhr": "YES", "status":
 "" }}}]}}] }} ] } }
```

Multicast to Unicast NAT

Multicast to unicast NAT is used for hosting content to public cloud. The translation is required as the cloud may not support multicast. After translation, the Unicast packet gets routed as per unicast forwarding logic.

A similar use case is seen when connecting to different sites. If the core does not support multicast end to end, then the content is delivered as unicast to the different sites. The Border box translates multicast to unicast and delivers to different sites for consumption.

For MU NAT, IPFM will continue perform bandwidth management for pre-translated multicast flows. For the translated unicast flow, the outgoing interface will need to have unicast bandwidth reservation so that the translated unicast traffic will be sent without any disruption. IPFM will also publish the Flow operational MO to indicate the NAT relationship. Since, there are three re-circulations that occur internally for every unicast translation, one must make sure that only one third of the recirculation port bandwidth is assumed. In case of any congestion on the service-reflect map interface used for re-circulation, IPFM does not publish a Fault MO.

In PIM Passive mode, Controller will perform Bandwidth management and call Rest APIs to provision the pre-translated flow. IPFM will publish the flow operational MO to indicate the NAT relationship.

Examples for MU NAT PIM Passive

The following are the MUNAT Rest API calls and Payload information:

Configure Re-circ Interfaces

```
url: 172.28.249.173/api/mo/sys/mca/config/natsr/mappings.json?rsp-subtree=full
Payload:
{
"mcaNatMapDestPrefixSif": {
"attributes": {
"destPrefix": "112.10.3.0/24",
"domName": "default",
"maxEnatReplications": "40",
"siIfName": "eth1/15",
"status": ""
}
}
}
```

Service Reflect Rules

```
url: <ip_switch>/api/mo/sys/mrib/inst/dom-default/sr/rule.json?rsp-subtree=full
Payload:
{
"mribRule": {
"attributes": {
"grpMasklen": "32",
"postTransGrp": "112.3.3.51",
"postTransSrc": "11.1.1.3",
"preTransGrp": "225.10.1.50",
"preTransSrc": "112.3.1.2",
"srcMasklen": "32",
"staticOif": "unspecified",
"status": "",
"udpDestPort": "0",
"udpsrcPort": "0"
}
}
}
```

IPFM Flows

```
url: <ip_switch>/api/mo/sys/nbm/show/flows/dom-default.json?rsp-subtree=full
Payload:
{
"nbmConfFlow": {
"attributes": {
"bwKbps": "50000",
"group": "225.1.1.1",
"ingressIf": "eth1/2",
"policer": "ENABLED",
"source": "112.3.1.2",
"status": ""
}
}
}
```

Unicast to Multicast NAT

Unicast to Multicast NAT works in ingress translation mode. The multicast translated packet can be egress translated back to multicast. The destination address of the unicast packet should match the NAT source loopback interface secondary IP address.

The Unicast to Multicast NAT supports only 1:1 translation. If 1 to many translations is required, then you need to configure a 1:1 Unicast to Multicast NAT, and then configure 1 to many Multicast-to-Multicast NAT translations.

For Unicast to Multicast NAT, you must configure unicast bandwidth reservation on the port where the pre-translated unicast traffic arrives. This enables the multicast traffic on that port to not to consume all the port bandwidth. Using the bandwidth derived from the flow policy of the post-translated multicast group, IPFM installs policer on all the slices to police unicast flow. Since there is one re-circulation for every multicast translation, the recirculation port bandwidth must be same as the incoming port bandwidth.

IPFM publishes the flow operations MO to indicate the NAT relationship. IPFM does not publish a fault MO if there is a congestion on the service-reflect map interface that is used for re-circulation.



Note Flow priority to the subsequent Multicast to Multicast Translation flow cannot be assigned. This flow priority has to be set for Unicast to Multicast translation flow (parent flow).

Examples for Unicast to Multicast NAT PIM Active

The following are the examples for the Unicast to Multicast NAT in PIM Active mode:

UMNAT Flow

```
ip service-reflect destination 10.34.202.11 to 234.34.203.11 mask-len 32 source 10.30.17.11
 to 10.34.201.1 mask-len 32

other supporting config needed for above flow stitching are:
multicast service-reflect dest-prefix 234.34.203.0/24 map interface Ethernet1/6

NBM flow-policy config:
nbm flow-policy
policy umnat
    bandwidth 15000 kbps
    ip group-range 234.34.202.1 to 234.34.202.255
    ip group-range 234.34.203.1 to 234.34.203.255
```

Chained MMNAT Flow

```
ip service-reflect destination 234.34.203.11 to 234.34.253.11 mask-len 32 source 10.34.201.1
 to 10.34.202.111 mask-len 32 to-udp-src-port 25010 to-udp-dest-port 25310 static-oif
Ethernet1/56
ip service-reflect destination 234.34.203.11 to 234.34.253.11 mask-len 32 source 10.34.201.1
 to 10.34.202.111 mask-len 32 to-udp-src-port 25010 to-udp-dest-port 25510 static-oif
Ethernet1/55

other supporting config needed for above flow stitching are:

multicast service-reflect interface Ethernet1/56 map interface Ethernet1/3
multicast service-reflect interface all map interface Ethernet1/4

NBM flow-policy config:
nbm flow-policy
  policy ummnat1
    bandwidth 16000 kbps
    ip group-range 234.34.253.10 to 234.34.253.100
      priority critical
    ip group-range 234.34.253.101 to 234.34.253.255
switch# show ip mr sr umnat 10.30.17.11 10.34.202.11
IP Multicast Routing Table for VRF "default"

(10.30.17.11/32, 10.34.202.11/32)
  Translation:
    SR: (10.34.201.1/32, 234.34.203.11/32) udp src: 0, udp dst : 0
      Outgoing interface list: (count: 3)
```

```
        Ethernet1/56, uptime: 02:13:44, igmp
        Ethernet1/55, uptime: 02:13:44, igmp
        Ethernet1/60, uptime: 02:13:51, static
      Chained translations:
        SR: (10.34.202.111, 234.34.253.11) udp src: 25010 udp dst: 25310 OIF: Ethernet1/56
        SR: (10.34.202.111, 234.34.253.11) udp src: 25010 udp dst: 25510 OIF: Ethernet1/55

switch#

switch# show forwarding distribution multicast route group 234.34.203.11 source 10.34.201.1


  (10.34.201.1/32, 234.34.203.11/32), RPF Interface: Ethernet1/6.100, flags: EPrePstUM
    Upstream Nbr: 10.34.201.1, Stats State: NA
    Received Packets: 16964898 Bytes: 23784786996
    Number of Outgoing Interfaces: 6
    Outgoing Interface List Index: 1609
      Ethernet1/55
      Ethernet1/56
      Ethernet1/60
      Null0
        Type: NAT_EGR_RW
        Source IF: Ethernet1/6.100
        RW Group IP: 234.34.203.11
        RW Source IP: 10.34.201.1
        RW source L4 port: 0
        RW dest L4 port: 0
        Original Group IP: 10.34.202.11
        Original Source IP: 10.30.17.11

      Ethernet1/56
        Type: NAT_EGR_RW
        Source IF: Ethernet1/3.1
        RW Group IP: 234.34.253.11
        RW Source IP: 10.34.202.111
        RW source L4 port: 25010
        RW dest L4 port: 25310
        Original Group IP: 234.34.203.11
        Original Source IP: 10.34.201.1

      Ethernet1/55
        Type: NAT_EGR_RW
        Source IF: Ethernet1/4.1
        RW Group IP: 234.34.253.11
        RW Source IP: 10.34.202.111
        RW source L4 port: 25010
        RW dest L4 port: 25510
        Original Group IP: 234.34.203.11
        Original Source IP: 10.34.201.1

switch#

switch# show forwarding multicast route group 234.34.203.11 source 10.34.201.1

slot  1
=======


  (10.34.201.1/32, 234.34.203.11/32), RPF Interface: Ethernet1/6.100, flags:
    Received Packets: 17115724 Bytes: 23996245048
    Outgoing Interface List Index: 1609
    Number of next hops: 4
    oiflist flags: 16809984
```

```
  Outgoing Interface List Index: 0x649
    Ethernet1/55
    Ethernet1/56
    Ethernet1/60
    Null0
     Encap 216  (10.30.17.11, 10.34.202.11 -> 10.34.201.1, 234.34.203.11) L4(0,0)
SrcIf(Ethernet1/6.100) Flags(0x0)
    Ethernet1/56
    Encap 1002 (10.34.201.1, 234.34.203.11 -> 10.34.202.111, 234.34.253.11) L4(25010,25310)
 SrcIf(Ethernet1/3.1) Flags(0x0)
    Ethernet1/55
    Encap 1003 (10.34.201.1, 234.34.203.11 -> 10.34.202.111, 234.34.253.11) L4(25010,25510)
 SrcIf(Ethernet1/4.1) Flags(0x0)s#


switch# show forwarding multicast-sr internal-db
     Encap 216  (10.30.17.11, 10.34.202.11 -> 10.34.201.1, 234.34.203.11) L4(0,0)
SrcIf(Ethernet1/6.100) Flags(0x0)
    Encap 1002 (10.34.201.1, 234.34.203.11 -> 10.34.202.111, 234.34.253.11) L4(25010,25310)
 SrcIf(Ethernet1/3.1) Flags(0x0)
    Encap 1003 (10.34.201.1, 234.34.203.11 -> 10.34.202.111, 234.34.253.11) L4(25010,25510)
 SrcIf(Ethernet1/4.1) Flags(0x0)



NBM Show commands:
switch# show nbm flows group 234.34.203.11 source 10.34.201.1 detail

------------------------------------------------------------
 NBM Flows for VRF 'default'
------------------------------------------------------------

Active Source-Group-Based Flow(s) for Source 10.34.201.1 Group 234.34.203.11  :

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 Priority   Policy-name

   Rcvr-Num Rcvr-slot Unit    Num-Rcvrs    Rcvr-ifidx  IOD Rcvr-Intf  Nbr-Device

234.34.203.11   10.34.201.1     02:21:05   Lo34      not-available           0     N/A
ACTIVE       3   15.000   15.000   17    0     0    0   7 Yes     Yes LOW        umnat

          1         1    0            3    0x1a006e00   64 Eth1/56    not-available
          2         1    0            3    0x1a006c00   63 Eth1/55    not-available
          3         1    0            3    0x1a007600   68 Eth1/60
LEAF34-PMN-SOLN-SOUTHLAKE
switch#


switch# show nbm flows statis group 234.34.203.11 source 10.34.201.1

------------------------------------------------------------
 NBM Flow Statistics for VRF 'default'
------------------------------------------------------------

Source-Group-Based Flow Statistics for Source 10.34.201.1 Group 234.34.203.11  :

Mcast-Group      Src-IP           Uptime     Src-Intf  Packets        Bytes
Allow-Bytes       Drop-Bytes
234.34.203.11    10.34.201.1      02:21:27   Lo34      8413701        11779181400
11778445000       0
switch#
```

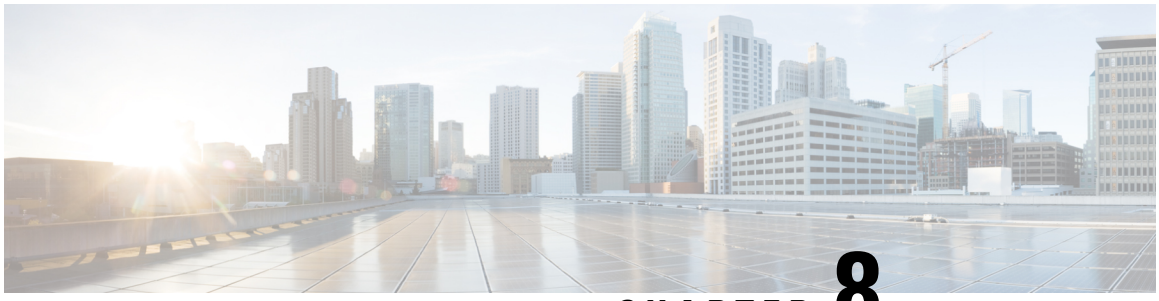
NBM Oper MO:


```
{
  "nbmNbmUmFlow": {
    "attributes": {
      "bucket": "3",
      "destination": "10.34.202.11",
      "dn": "sys/nbm/show/flows/dom-default/ums-[10.30.17.11]-umd-[10.34.202.11]",
      "modTs": "2021-11-30T11:34:55.213+00:00",
      "source": "10.30.17.11",
      "tStamp": "1638300895054"
    }
  }
}

{
  "nbmNbmFlow": {
    "attributes": {
      "bucket": "1",
      "bwKbps": "15000",
      "dn": "sys/nbm/show/flows/dom-default/s-[10.34.201.1]-g-[234.34.203.11]",
      "dscp": "0",
      "egressIfCount": "3",
      "flowPol": "umnat",
      "group": "234.34.203.11",
      "ingressIf": "335544354",
      "ingressIfName": "loopback34",
      "isFhr": "YES",
      "modTs": "2021-11-30T11:35:23.384+00:00",
      "policed": "YES",
      "priority": "LOW",
      "qid": "7",
      "source": "10.34.201.1",
      "tStamp": "1638300923224"
    },
    "children": [
      {
        "nbmOifList": {
          "attributes": {
            "dn":
"sys/nbm/show/flows/dom-default/s-[10.34.201.1]-g-[234.34.203.11]/oif-436237824",
            "modTs": "2021-11-30T11:35:35.387+00:00",
            "oif": "436237824",
            "oifName": "Ethernet1/60",
            "oifTstamp": "1638300935386",
            "origin": "PROTOCOL",
            "reporterIP": "10.34.60.1"
          }
        }
      },
      {
        "nbmOifList": {
          "attributes": {
            "dn":
"sys/nbm/show/flows/dom-default/s-[10.34.201.1]-g-[234.34.203.11]/oif-436235264",
            "modTs": "2021-11-30T11:35:42.436+00:00",
            "oif": "436235264",
            "oifName": "Ethernet1/55",
            "oifTstamp": "1638300942436",
            "origin": "PROTOCOL",
            "reporterIP": "10.34.55.11"
          }
        }
      },
```

```
      {
        "nbmOifList": {
          "attributes": {
            "dn":
"sys/nbm/show/flows/dom-default/s-[10.34.201.1]-g-[234.34.203.11]/oif-436235776",
            "modTs": "2021-11-30T11:35:42.437+00:00",
            "oif": "436235776",
            "oifName": "Ethernet1/56",
            "oifTstamp": "1638300942437",
            "origin": "PROTOCOL",
            "reporterIP": "10.34.56.11"
          }
        }
      },
      {
        "nbmUmIngNat": {
          "attributes": {
            "dn":
"sys/nbm/show/flows/dom-default/s-[10.34.201.1]-g-[234.34.203.11]/umng-pres-[10.30.17.11]-pred-[10.34.202.11]-postsp-[0]-postdp-[0]",

            "modTs": "2021-11-30T11:34:55.213+00:00",
            "postDPort": "0",
            "postSPort": "0",
            "preDestination": "10.34.202.11",
            "preSource": "10.30.17.11"
          }
        }
      }
    ]
  }
}
```



CHAPTER 8

Media Controller

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

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

Note

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

To bring up the devices from the basic configuration using POAP, you must define the templates and publish the POAP definition through Cisco NDFC **Web Client > Configure > Deploy > POAP Definitions**. For more information, see the *POAP Launchpad* section.

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

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

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

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

NX-OS Streaming Telemetry and NDFC

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

```
telemetry
  destination-profile
    use-vrf management
  destination-group 200
    ip address <dcnm-ip> port 50051 protocol gRPC encoding GPB
  destination-group 1500
  sensor-group 200
    data-source DME
    path sys/nbm/show/appliedpolicies depth unbounded
    path sys/nbm/show/stats depth unbounded
  sensor-group 201
    data-source DME
    path sys/nbm/show/flows depth 0 query-condition
    rsp-subtree-filter=eq(nbmNbmFlow.bucket,"1")&rsp-subtree=full
  sensor-group 202
    data-source DME
    path sys/nbm/show/flows depth 0 query-condition
    rsp-subtree-filter=eq(nbmNbmFlow.bucket,"2")&rsp-subtree=full
  sensor-group 203
    data-source DME
    path sys/nbm/show/flows depth 0 query-condition
    rsp-subtree-filter=eq(nbmNbmFlow.bucket,"3")&rsp-subtree=full
  sensor-group 204
    data-source DME
    path sys/nbm/show/flows depth 0 query-condition
    rsp-subtree-filter=eq(nbmNbmFlow.bucket,"4")&rsp-subtree=full
  sensor-group 205
    data-source DME
    path sys/nbm/show/endpoints depth unbounded
  sensor-group 300
    data-source NX-API
    path "show ptp brief"
    path "show ptp parent"
  sensor-group 301
    data-source NX-API
    path "show ptp corrections"
  sensor-group 500
    data-source NX-API
    path "show flow rtp details" depth 0
    path "show flow rtp errors active" depth 0
    path "show flow rtp errors history" depth 0
  sensor-group 400
    data-source DME
    path sys/nbm/show/faults depth unbounded
    path sys/nbm/show/notify depth unbounded
  subscription 201
    dst-grp 200
    snsr-grp 200 sample-interval 60000
    snsr-grp 201 sample-interval 30000
    snsr-grp 205 sample-interval 30000
  subscription 202
    dst-grp 200
    snsr-grp 202 sample-interval 30000
  subscription 203
    dst-grp 200
    snsr-grp 203 sample-interval 30000
  subscription 204
```

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

Scope in Media Controller

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

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

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

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

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

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

- Generic Multicast Monitoring, on page 97
- Topology, on page 100
- Host, on page 101
- Flow, on page 115
- RTP, on page 133
- Multicast NAT, on page 135
- Global, on page 147
- Config, on page 149
- NDFC Read-Only Mode for Media Controller, on page 158

Generic Multicast Monitoring

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

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

Enabling Generic Multicast Mode

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

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

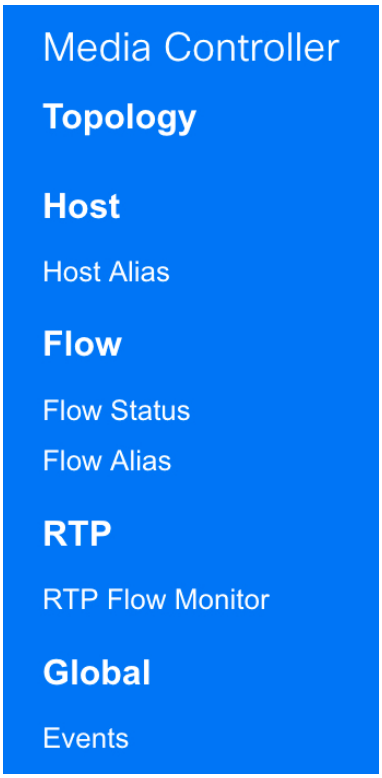


Note

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

Generic Multicast Menu

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



NX-OS Streaming Telemetry and NDFC (Generic Multicast)

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

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

Topology

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

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

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

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

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

Note

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

Quick Search

Enter the search string to highlight relevant devices.

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

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

Multicast Group

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

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

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

Show Panel > Bandwidth

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

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

The display format is *Transmitted-Received*.

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

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

Bandwidth Tracking on Host Facing Link

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



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

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

Host

The Host menu includes the following submenus:

Discovered Host

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

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

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

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

Host Alias



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

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

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

Table 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 NDFC.

Procedure

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

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

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

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

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

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

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

Edit Host Alias

Perform the following task to edit the host alias.

Procedure

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

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

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

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

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

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

Delete Host Alias

Perform the following task to delete the host alias.

Procedure

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

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

Step 2 Click **Delete**.

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

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

Import Host Alias

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

Procedure

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

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

Step 3 Click **Open**.

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

Export Host Alias

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

Procedure

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

A notification window appears.

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

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

Host Policies

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



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

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

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



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

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

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

Field	Description
Deployment	

Field	Description

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

Field	Description
	successfully deployed.

Table 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: • Sender • Receiver-External • Receiver-Local
Operation	Specifies if the operation of the host policy. The policy has the following operations: • Permit • Deny
Sequence #	Specifies the sequence number of the custom policy when the multicast range is selected.
Deployment Action	Specifies the action performed on the switch for that host policy. • **Create**—The policy is deployed on the switch. • **Delete**—The policy is undeployed from the switch.
Deployment Status	Specifies if the deployment is successful, failed or the policy is not deployed.
Last Updated	Specifies the date and time at which the host policy was last updated. The format is `Day MMM DD YYYY HH:MM:SS Timezone`.

This section contains the following:

Add Host Policy

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

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

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

Procedure

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

The **Host Policies** window is displayed.

Step 2 Click the **Add** icon.

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

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

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

  Note
  When **Receiver IP** in a receiver host policy is a wildcard (* or 0.0.0.0), **Sender IP** also has to be a wildcard (* or 0.0.0.0).
- **Multicast**: Specifies the multicast IP Address for the host policy. Note that you can specify wildcard for this IP address by specifying the * (asterisk) symbol in this field. This will translate to 224.0.0.0/4. If you specify a wildcard

IP address for **Sender IP** and **Receiver IP** fields, the Multicast Group is always required, that is, you cannot specify multicast as * or 0.0.0.0.

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

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

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

Edit Host Policy

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

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

Procedure

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

The **Host Policies** window is displayed.

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

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

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

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

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

Click **Cancel** to discard the changes.

Delete Host Policy

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

Note You can delete only user-defined Host Policies.

Procedure

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

The **Host Policies** window is displayed.

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

You can select more than one host policy to delete.

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

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

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

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

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

Import Host Policy

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

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

Procedure

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

The **Host Policies** window is displayed.

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

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

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

Step 4 Click **Open**.

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

Export Host Policy

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

Procedure

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

The **Host Policies** window is displayed.

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

A notification window appears.

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

Step 4 Click **OK**.

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

Policy Deployment

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

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

Deploy Selected Policies

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

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

Deploy All Custom Policies

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

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

Undeploy Selected Custom Policies

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

Undeploy All Custom Policies

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

Note You cannot undeploy the default configured policies.

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

Redo All Failed Custom Policies

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

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

Deployment History

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

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

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

Deployment History table shows the following fields.

Table 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 *Day MMM DD YYYY HH:MM:SS Timezone*.
Failed Reason	Species why the policy was not successfully deployed.

Applied Host Polices

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

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

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

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

Flow

The Flow menu includes the following submenus:

Flow Status

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

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

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

Multicast NAT Visualization

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

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

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

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

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

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

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

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

Fields and Descriptions

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

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

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

Table 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	Specifies reason for the inactive flow. Cisco NDFC determines the inactive flow if both the sender and receiver mroute exists with any of the following combinations. • Receiver IIF is null • Receiver OIF is null • Sender IIF is null • Sender OIF is null In this scenario, the switch will not have any fault reason. Therefore, there is no fault reason for such inactive flows.
Field Specific for Generic Multicast Mode	
Receiver Interface IP	Specifies the IP address of the receiver interface joining the group.

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

Table 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.

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

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

Table 13: Receiver Only Tab

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

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

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

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

Note Cisco NDFC holds the Flow statistics values in the NDFC server internal memory. Therefore, after a NDFC Restart or HA switch over, the Flow statistics won't show previously collected values. However, you can see the Flow statistics that are collected after the server Restart or HA switch over.

If the new flow joins before the uplinks between the switches that are detected in NDFC, a message BW_UNAVAIL appears. This is resolved after the uplinks between the switches are detected by NDFC after discovery of the devices.

Flow Alias

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

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

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

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

Table 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 NDFC Web UI, perform the following steps:

Procedure

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

The **Flow Alias** window is displayed.

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

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

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

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

Click **Cancel** to discard.

Edit Flow Alias

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

Procedure

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

The **Flow Alias** window is displayed.

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

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

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

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

Click **Cancel** to discard the changes.

Delete Flow Alias

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

Procedure

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

The **Flow Alias** window is displayed.

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

You can select more than one flow alias to delete.

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

The flow alias is deleted.

Export Flow Alias

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

Procedure

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

The **Flow Alias** window is displayed.

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

A notification window appears.

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

Step 4 Click **OK**.

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

Import Flow Alias

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

Procedure

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

The **Flow Alias** window is displayed.

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

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

Step 4 Click **Open**.

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

Flow Policies

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

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

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

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

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

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

Table 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** • You cannot delete the default flow policies. • Undeploy policies from all switches before deleting them from NDFC.
Delete All	Allows you to delete all the flow policies at a single instance. **Note** Undeploy policies from all switches before deleting them from NDFC.
Import	Allows you to import flow policies from a CSV file. **Note** After import, all policies imported from a CSV file are applied to all managed switches automatically.
Export	Allows you to export flow policies to a CSV file.

Field	Description
Deployment	

Field	Description

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

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

Table 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	Specified if the flow policy is deployed successfully or failed.
Deployment Action	Specifies the action that is performed on the switch for that host policy. • **Create**—The policy is deployed on the switch. • **Delete**—The policy is undeployed from the switch.
In Use	Specifies if the flow policy is in use or not.
Policer	Specifies whether the policer for a flow policy is enabled or disabled. **Note** In adding or editing a flow policy, the default policer state is **Enabled**.
Last Updated	Specifies the date and time at which the flow policy was last updated. The format is `Day MMM DD YYYY HH:MM:SS Timezone`.

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

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

This section contains the following:

Add Flow Policy

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

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

Procedure

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

The **Flow Policies** window is displayed.

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

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

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

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

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

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

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

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

The flow priority is used during the following scenarios:

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

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

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

Click **Cancel** to discard the changes.

Edit Flow Policy

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

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

SUMMARY STEPS

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

DETAILED STEPS

Procedure

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

The **Flow Policies** window is displayed.

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

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

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

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

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

The flow priority is used during the following scenarios:

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

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

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

Click **Cancel** to discard the changes.

Delete Flow Policy

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

Procedure

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

The **Flow Policies** window is displayed.

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

You can select more than one flow policy to delete.

Note
You cannot delete the default policies.

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

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

Import Flow Policy

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

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

SUMMARY STEPS

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

DETAILED STEPS

Procedure

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

The **Flow Policies** window is displayed.

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

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

Step 4 Click **Open**.

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

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

Export Flow Policy

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

Procedure

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

The **Flow Policies** window is displayed.

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

A notification window appears.

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

Step 4 Click **OK**.

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

Policy Deployment

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

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

Deploy Selected Policies

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

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

Deploy All Custom Policies

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

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

Undeploy Selected Custom Policies

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

Undeploy All Custom Policies

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



Note You cannot undeploy the default configured policies.



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

Redo All Failed Custom Policies

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

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

Deployment History

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

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

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

Deployment History table shows the following fields.

Table 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.

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

Static Flow

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

Table 18: Static Flow Operations

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

Table 19: Static Flow Field and Description

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

Adding Static Flow

Procedure

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

Step 2 Click the **Add** icon.

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

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

Group: Specifies the multicast group.

Source: Specifies the source IP address.

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

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

Click **Cancel** to discard it.

Deleting Static Flow

Procedure

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

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

RTP

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

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

RTP Flow Monitor

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



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

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

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

The description of the fields in these tabs are:

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

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

Active

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

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

Packet Drop

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

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

Flow Topology

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

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

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

The switches experiencing packet drops are circled in red.

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

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

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

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

Drop History

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

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

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

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

Multicast NAT

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

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

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

Prerequisites

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

  Here is an example to configure the loopback interface:

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

ip service-reflect source-interface loopback10
```

- TCAM memory carving must be completed.

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

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

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

NAT Modes

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

Table 20: NAT Modes Operations

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

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

Table 21: NAT Mode Field and Description

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

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

Adding a NAT Mode

Procedure

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

Step 2 Click the **Add** icon.

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

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

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

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

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

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

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

Deleting a NAT Mode

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

Procedure

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

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

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

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

Egress Interface Mappings

Table 22: Egress Interface Mappings Operations

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

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

Table 23: Egress Interface Mappings Field and Description

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

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

Adding Egress Interface Mapping

Procedure

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

Step 2 Click the **Add** icon.

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

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

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

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

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

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

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

Click **Cancel** to discard it.

Editing Egress Interface Mapping

Procedure

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

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

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

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

Click **Cancel** to discard it.

Deleting Egress Interface Mapping

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

Procedure

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

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

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

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

NAT Rules

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

Table 24: NAT Rules Operations

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

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

Table 25: NAT Rules Field and Description

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

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

Adding NAT Rule

Procedure

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

Step 2 Click the **Add** icon.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Click **Cancel** to discard it.

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

Deleting NAT Rule

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

Procedure

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

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

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

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

Border Router Config

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

Table 26: Border Router Config Operations

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

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

Table 27: Border Router Config Field and Description

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

Deploying Border Router Config

Procedure

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

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

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

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

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

Global

The Global menu includes the following submenus:

Events



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

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

The IPFM Events table is updated real-time.

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

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

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

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

Copying Switch Running Configuration to Start-up Configuration

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

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

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

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

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

Realtime Notifications

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

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

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

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

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

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

Threshold Notifications

NDFC generates threshold notifications in the following scenarios:

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

The notification is deleted when the condition is resolved.

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

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

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

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

Config

The Config menu includes the following submenus:

Setting Up the SNMP Server for NDFC

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

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

Procedure

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

Step 2 For an Inband environment, use the `pmn_telemetry_snmp` CLI template that is packaged along with the Cisco NDFC Application, to configure more SNMP settings on the switch. For more information, see Switch Global Config, on page 152.

AMQP Notifications

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

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

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

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

   ```
   AMQP_POLL_TIME=5
   ```

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

   appmgr restart dcnm—for Standalone deployment

   appmgr restart ha-apps—for Native HA deployment

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

AMQP Notification Components

- **Routing Key**

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

- **Routing Key Format**

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

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

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

- **Message Properties**

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

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

Property	Value
message_id	Message ID

- **Notification Body**

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

Switch Global Config

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

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

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

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

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

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

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

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

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

AMQP Notifications

As Cisco NDFC uses Telemetry to fetch data from the Fabric, the flow status and AMQP notifications may not reflect the current state in real time. It periodically checks new events and generate appropriate notification.

Also, flows are no longer limited to a single spine and may take N or W or M shape. Host policies are applied based on the switch interface configuration and not just-in-time (JIT). All these architecture changes influence current AMQP messages and trigger time. By default, poll interval is set to 2 minutes. For more information, see AMQP Notifications, on page 150.

Unicast Bandwidth Reservation

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

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

Reserve Bandwidth to Receiver Only

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

ASM Range

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

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

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

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

Table 28: Operations on the Global Config screen

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

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

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

Table 29: Deployment History Field and Description

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

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

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

Interface Configs

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

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

Note A user with the network operator role in NDFC cannot save, deploy, undeploy, or edit interface configs.

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

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

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

2. In the WAN Links column, from the drop-down list, choose **Yes** or **No** to designate the interface as a WAN link.
3. Click **View All Deployed Interfaces** to view the Switch Name, Switch IP Address, and Interface Name which is configured as a WAN link or reserved the bandwidth. You can choose an appropriate filter to view the deployed interfaces.
4. In the **Unicast BW %** column, you can configure the interface to allot a dedicated percentage of bandwidth to unicast traffic. The remaining percentage is automatically reserved for multicast traffic. Enter a numeric value or the default **n/a** value in this column for an interface.

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

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

Table 30: WAN Links Table Field and Description

Field	Description
Status	Specifies if the WAN links or unicast bandwidths are deployed or undeployed on the selected switch.
History	Click this link to view the deployment history. For description about the fields that appear on this page, see the table below.
Interface Name	Specifies the interface which is connected as a WAN link to the end device and this interface will be in Layer 3.

Field	Description
Admin Status	An up arrow depicts that the status is up. A down arrow implies that the status is down.
Oper Status	An up arrow depicts that the operational state of the interface is up. A down arrow implies that the status is down.
WAN Links	From the drop-down, list you can choose to designate this interface as a WAN link. • Select **Yes** to configure the interface as a WAN link. • Select **No** to remove the interface as a WAN link.
Unicast BW %	Specifies the dedicated percentage of bandwidth to the unicast traffic. The remaining percentage is automatically reserved for the multicast traffic. The default value is **n/a**.
Deployment Status	Specifies if the interface is deployed or not.

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

Table 31: Deployment History Field and Description

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

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

NDFC Read-Only Mode for Media Controller

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

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

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

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

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

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

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

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

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

Host Policies - NDFC Read-Only Mode

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

Table 32: Host Policies Table Field and Description

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

Field	Description
Host Role	Specifies the host device role. The host device role is one of the following: • Sender • Receiver-External • Receiver-Local
Operation	Specifies if the operation of the host policy. The policy has the following operations: • Permit • Deny
Last Updated	Specifies the date and time at which the host policy was last updated. The format is *Day MMM DD YYYY HH:MM:SS Timezone*.

Flow Policies - NDFC Read-Only Mode

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

Table 33: Flow Policies Table Field and Description

Field	Description
Policy Name	Specifies the flow policy name.
Multicast IP Range	Specifies the multicast IP address for the traffic.
Bandwidth	Specifies the bandwidth that is allotted for the traffic.
QoS/DSCP	Specifies the Switch-defined QoS Policy.
Policer	Specifies whether the policer for a flow policy is enabled or disabled.
Last Updated	Specifies the date and time at which the flow policy was last updated. The format is *Day MMM DD YYYY HH:MM:SS Timezone*.

Switch Global Config - Read-Only Mode

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

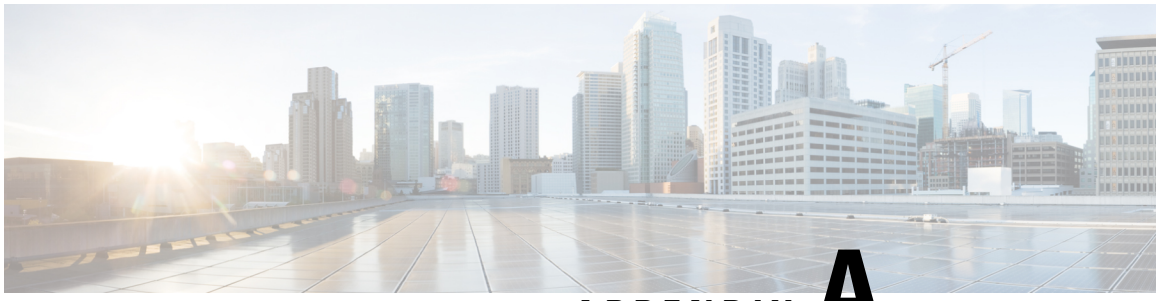
WAN Links - Read-Only Mode

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

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

Table 34: WAN Links Table Field and Description

Field	Description
Interface Name	Specifies the interface which is connected as a WAN link to the end device.
Admin Status	An up arrow depicts that the status is up. A down arrow implies that the status is down.
Oper Status	An up arrow depicts that the operational state of the interface is up. A down arrow implies that the status is down.
WAN Links	From the drop-down, list you can choose to designate this interface as a WAN link. • Select **Yes** to configure the interface as a WAN link. • Select **No** to remove the interface as a WAN link.
Deployment Status	Specifies if the interface is deployed as a WAN link or not.



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 163
- Sample Show Command Output (Single Modular Switches), on page 178

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)
```

```
 ----------------------------------------

  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    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    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    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:

```
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       | 21.7.1.2        |
| 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
 ------------------------------------------------------------------------
```

```
| 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     pol2
```

```
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
```

```
-------------------------------------------------------------------

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
 ------------------------------------------------------
```

```
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
```

```
 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** *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
------------------------------------------------------------------------
------------------------------------------------------------------------
```

```
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         | 1000000         | Yes
|                 |                 | None            |                                                 |
|                 |                 |                 |                 |
| 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
```

```
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 Nexus Dashboard Fabric Controller. In controller-based deployments, statistics are available in the Nexus Dashboard Fabric 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
  bandwidth 123 kbps
  dscp 10
  ip group-range 237.1.1.0 to 238.1.1.0
policy POL_A
policy flow
policy nbm1_1
  bandwidth 1000000 kbps
  dscp 11
  ip group-range 224.1.0.1 to 224.1.255.255
  ip group-range 225.1.0.1 to 225.1.255.255
```



INDEX

B

bandwidth **37, 53, 59**

C

class **69–72**
class-map type qos match-all **69, 71**
class-map type qos match-any **69, 71**
clear flow rtp detail **81**
clear nbm flow statistics **74**

D

default deny **35, 57**
default permit **35, 57**
dscp **38, 59**

E

egress-host **65**
egress-interface **65**

F

feature interface-vlan **48**
feature nbm **34, 52, 68**
feature netflow **79**
flow priority **38, 54, 59**
flow rtp timeout **81**

H

host **36, 57**

I

interface vlan **48–49**
ip access-list **69–70, 79**
ip address **39–40, 45–49**
ip flow rtp **79**
ip group **54**
ip group-range **38, 54, 59**
ip igmp immediate-leave **39, 41, 46–47**
ip igmp snooping **48–49**
ip igmp snooping fast-leave **48–49**
ip igmp suppress v3-gsq **48, 50**
ip igmp version **39, 41**
ip igmp version 3 **46–49**
ip ospf passive-interface **39–40, 46–47**
ip pim passive **48, 50**
ip pim rp-address **39**
ip pim sparse-mode **39, 41, 45–48, 50, 68**
ip pim spt-threshold infinity group-list **39–40**
ip pim ssm range none **39–40**
ip router ospf **39–40, 45–49**
ipv6 flow rtp **79**

M

master ipv4 **75**
match access-group name **69, 71**
match ip multicast group **39–40**

N

nbm external-link **68**
nbm flow asm range **36, 57**
nbm flow bandwidth **36, 52, 57**
nbm flow dscp **36, 58**
nbm flow reserve-bandwidth receiver-only **58**
nbm flow-definition **65**
nbm flow-policy **37, 53, 58**
nbm host-policy **35, 56**
nbm mode pim-active **56**
nbm mode pim-passive **61**
nbm reserve unicast fabric bandwidth **36, 57**
nbm vrf **56, 61**
no nbm flow policer **37, 53, 58**
no policer **37, 53, 58**
no shutdown **45–48, 50–51**

P

permit **69–70**
pim **35, 57**
policy **37, 53, 58**
policy-map type qos **69, 71**

priority level 38, 54, 60
ptp transport ipv4 ucast master 75
ptp ucast-source 75

R

receiver 35, 57
route-map 39–40

S

sender 35, 57
service-policy type qos input 70, 72
set qos-group 69–72
show flow rtp details 80
show flow rtp errors active 80
show flow rtp errors history 80
show ip mroute 73
show nbm defaults 73
show nbm flow-policy 73
show nbm flows 73
show nbm flows static 73
show nbm flows static group 73
show nbm flows statistics 74
show nbm flows summary 74
show nbm host-policy 74
show nbm interface bandwidth 74
show ptp brief 75
show ptp counters interface ethernet 76
show running-config nbm 74
slave ipv4 75
source 36, 57
stage-flow 65
switchport 48, 50
switchport access vlan 48, 51
switchport mode 48, 50
switchport trunk allowed vlan 48, 51

V

vlan configuration 48–49