Configuring IP Fabric for Media

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

Prerequisites

Cisco'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.

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

Guidelines and Limitations

The IP fabric for media solution has the following guidelines and limitations:

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

- All supported IP fabric for media platforms allows the sender or receiver end hosts to be connected to the spine.
- The IP fabric for media solution supports multiple border leafs per fabric.
- If you change the unicast bandwidth percentage, you must flap the fabric links for the new value to take effect.
- Only Layer 3 interfaces can be configured as NBM external links. If a Layer 3 interface is changed to a switch port, the NBM external link configuration is removed.
- When you configure a Layer 3 interface as an NBM external link, the interface flaps.
- If an RPF or any of the OIF interfaces cannot accommodate a bandwidth change, the flow is torn down. The next IGMP or PIM join will initiate flow stitching.
- When you change the flow policy (bandwidth) for groups with existing flows in the fabric, make the changes in the following order to reduce the impact on existing flows. Otherwise, oversubscription could occur, depending on the available bandwidth for the interfaces in use.
  1. Change from a lower to higher bandwidth: Modify the policy first on all last hop routers for the existing flows, then on all spine switches, and then on the rest of the switches.
  2. Change from a higher to lower bandwidth: Modify the policy first on all first hop routers for the existing flows, then on all spine switches, and then on the rest of the switches.
- Statistics are not available if you disable the NBM flow policer.
- During a failure, the PMN Flow Prioritization feature tries to recover priority flows where possible. By design, PMN Flow Prioritization does not bring down already established flows to accommodate priority flows.
- Beginning with Cisco Nexus Release 10.1(1) PMN Flow Prioritization with NBM is supported on Cisco Nexus 9300-FX3 platform switches.
- Beginning with Cisco NX-OS Release 10.1(2), PMN is supported on the N9K-X9624D-R2, and N9K-C9508-FM-R2 platform switches.
- Beginning with Cisco NX-OS Release 10.2(1q)F, PMN is supported on the N9K-C9332D-GX2B platform switches.
- For Cisco Nexus 9500 -R line cards, when configured in NBM Passive mode there will be increasing input discards and this has been determined to be expected and non-impacting.
- NBM running on a VXLAN enabled switch is not supported. Feature NBM may disrupt VXLAN underlay multicast forwarding.
- Beginning with Cisco NX-OS Release 10.3(1)F, the following PMN 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 NBM mode pim-active and NBM mode pim-passive on Cisco Nexus 9200, 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 nbm pim-active or nbm pim-passive mode.

  For example: If the parent port is part of NBM 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 NBM mode pim-active and NBM mode pim-passive.
- Beginning with Cisco NX-OS Release 10.3(2)F, NBM mode pim-active and NBM mode pim-passive can coexist on the same switch.
- From Cisco NX-OS Release 10.4(1)F, ISIS is supported with NBM.
- From Cisco NX-OS Release 10.4(1)F, NBM is supported on Cisco Nexus 9348GC-FX3 switch.
- From Cisco NX-OS Release 10.4(2)F, NBM 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 NBM 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 92348GC-X Platform Switches
  - Nexus 9300-EX/FX/FX2/FX3/H1 Platform Switches
  - Nexus 9300C/GX/GX2 Platform Switches
  - Nexus 9700-EX/FX/GX line cards
  - Nexus 9600-R/R2 line cards

Guidelines and Limitations for Host Policies

The following guidelines and limitations apply to host policies:

- Default host policies are configured automatically and are allowed by default.
- By default, all external receiver (PIM) and sender host policies are applied on the external links.
- Delete any custom NBM host policies before updating a default policy.

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

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

Note If you enter a wild card (0.0.0.0) for the host IP address for a local receiver host policy, 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 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 DCNM licen license, see the Cisco DCNM Installation Guide.

Upgrading to a Cisco NX-OS 9.x Release

Upgrading from a Cisco NX-OS 9.x Release

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

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

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

Step 3 Upgrade 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.

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

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

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

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

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

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

Step 7 Upgrade NDFC.

Step 8 Configure PIM and MSDP, if applicable.

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

Step 10 Configure NBM policies using the CLI or NDFC.

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

Step 12 Enable all ports facing the endpoints.

Setting Up the SNMP Server for 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.

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 NBM

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

- Spine-leaf topology
- Single modular switch

Configuring NBM for a Spine-Leaf Topology

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

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

Before you begin

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

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

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **feature nbm**
3. (Optional) [**no**] **nbm host-policy**
4. (Optional) {**sender** | **receiver** | **pim**}
5. (Optional) **default** {**permit** | **deny**}
6. (Optional) Enter one of the following commands:
   - For sender host policies: *sequence-number* **host** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
   - For local receiver host policies: *sequence-number* **host** *ip-address* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
   - For external receiver (PIM) host policies: *sequence-number* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}

7. (Optional) [**no**] **nbm reserve unicast fabric bandwidth** *value*
8. [**no**] **nbm flow asm range** [*group-range-prefixes*]
9. [**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**}
10. [**no**] **nbm flow dscp** *value*
11. (Optional) [**no**] **nbm flow policer**
12. [**no**] **nbm flow-policy**
13. [**no**] **policy** *policy-name*
14. (Optional) [**no**] **policer**
15. [**no**] **bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**}
16. [**no**] **dscp** *value*
17. [**no**] **ip group-range** *ip-address* **to** *ip-address*
18. (Optional) [**no**] **priority critical**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	[**no**] **feature nbm**
	Example:
	`switch(config)# feature nbm`
		Enables the NBM feature and PIM active mode, which allows the NBM fabric to form a multicast flow without assistance from an external controller.
		When you enter the **feature nbm** command, the following commands are also enabled automatically:
		• **nbm mode pim-active**
		• **ip multicast multipath nbm**
		• **ip pim prune-on-expiry**
		• **cdp enable**
		The **no** form of this command disables the following commands: **feature nbm**, **nbm mode pim-active**, **ip multicast multipath nbm**, and **ip pim prune-on-expiry**.
		Note If you disable NBM for Cisco Nexus 9504 and 9508 switches with -R line cards, you must configure these TCAM carving commands in the following order and then reload the switch. The recommended TCAM value is 2048.
		`hardware access-list tcam region ing-nbm 0`
		`hardware access-list tcam region redirect_v6 TCAM-size`

	Command or Action	Purpose
		Note If you want to configure an NBM VRF, see Configuring an NBM VRF for Active Flow Provisioning, on page 27.

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

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

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

Step 6	(Optional) Enter one of the following commands:
	• For sender host policies: *sequence-number* **host** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
	• For local receiver host policies: *sequence-number* **host** *ip-address* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
	• For external receiver (PIM) host policies: *sequence-number* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
	Example:
	`switch(config-nbm-host-pol-sender)# 10 host 101.1.1.3 group 229.1.1.1/32 deny`
	Example:
	`switch(config-nbm-host-pol-rcvr)# 40 host 100.1.1.1 source 145.1.1.1 group 234.1.1.1/32 deny`
	Example:
	`switch(config-nbm-host-pol-pim)# 50 source 101.1.1.1 group 235.1.1.1/32 deny`
		Specifies if the sender or receiver flows are to be permitted or denied.
		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 7	(Optional) [**no**] **nbm reserve unicast fabric bandwidth** *value* **Example:** `switch(config)# nbm reserve unicast fabric bandwidth 2`	Reserves a percentage of bandwidth on fabric ports for unicast flows. NBM flow management does not use this bandwidth for flow setup and reserves it on all fabric interfaces for the unicast traffic. The range is from 0 to 100 percent, and the default value is 0.
Step 8	[**no**] **nbm flow asm range** [*group-range-prefixes*] **Example:**	Programs the NBM ASM group range for *,G joins. The IGMP joins in this group range are expected to be V2 joins

	Command or Action	Purpose
	`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`	or (*, G) joins. You can configure up to 20 group ranges. The default is no configured group range. **Note** This command is needed only in a multispine deployment.
Step 9	[**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} **Example:** `switch(config)# nbm flow bandwidth 3000 mbps`	Configures the global NBM flow bandwidth in Kbps, Mbps, or Gbps. The minimum supported flow bandwidth is 200 Kbps. **Range** / **Default Value** 1 to 25,000,000 Kbps / 0 Kbps 1 to 25,000 Mbps / 0 Mbps 1 to 25 Gbps / 0 Gbps
Step 10	[**no**] **nbm flow dscp** *value* **Example:** `switch(config)# nbm flow dscp 10`	Configures the global NBM flow DSCP value. The range is from 0 to 63. If any of the flows do not match the NBM flow group range, the default flow DSCP is used for bandwidth management and flow setup.
Step 11	(Optional) [**no**] **nbm flow policer** **Example:** `switch(config)# no nbm flow policer`	Enables or disables the policer for all NBM flow policies. The policer is enabled by default.

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

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

Step 14	(Optional) [**no**] **policer** **Example:** `switch(config-nbm-flow-pol-attr)# no policer`	Enables or disables the policer for the specified NBM flow policy. By default, each source flow uses a policer on the source leaf (the first hop router). In a scenario where the number of multicast source flows exceeds the number of policers, the flow is not accepted by the source leaf. To override this behavior, you can disable the policer under the flow policy. For flows that match the flow policy where the policer is disabled, no policer resource is consumed.

	Command or Action	Purpose
		Note Use this command with caution as it could lead to an unprotected network, where a misbehaving endpoint could transmit more than what it is allowed. Use another method, such as an aggregate policer, to rate limit flows that have no policer programmed by NBM. For information on configuring an aggregate policer, see Configuring Shared Policers.
Step 15	[**no**] **bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} **Example:** `switch(config-nbm-flow-pol-attr)# bandwidth 10 mbps`	Configures the flow bandwidth in Kbps, Mbps, or Gbps for multicast groups matching this policy. The minimum supported flow bandwidth is 200 Kbps. **Range** / **Default Value** 1 to 25,000,000 Kbps / 0 Kbps 1 to 25,000 Mbps / 0 Mbps 1 to 25 Gbps / 0 Gbps
Step 16	[**no**] **dscp** *value* **Example:** `switch(config-nbm-flow-pol-attr)# dscp 10`	Configures the differentiated services code point (DSCP) value on the first-hop redundancy for flows matching the specified group range.

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

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

Example

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

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

switch(config)# show nbm host-policy applied sender all
```

```
Default Sender Policy: Allow
Applied WildCard host policies
Seq Num    Source     Group       Group Mask  Action
1100       0.0.0.0    224.1.1.1   32          Allow
Total Policies Found = 1

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

What to do next

Configuring PIM on Spine and Leaf Switches

Configuring MSDP on Spine Switches

Configuring Fabric and Host Interfaces

Configuring an NBM VRF, on page 27

Establishing a Flow (Optional)

Configuring PIM on Spine and Leaf Switches

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

Before you begin

Configure NBM for a spine-leaf topology.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

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

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

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

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

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

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

	Command or Action	Purpose
Step 10	**ip ospf passive-interface** **Example:** `switch(config-if)# ip ospf passive-interface`	Suppresses routing updates on the interface. This command overrides the router or VRF command mode configuration. OSPF runs passive on host-facing interfaces only. This configuration is needed only on endpoint interfaces and is not needed on fabric interfaces.
Step 11	**ip router ospf** *instance-tag* **area** *area-id* **Example:** `switch(config-if)# ip router ospf p1 area 0.0.0.0`	Enables OSPF on the interface.
Step 12	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on the interface.
Step 13	**ip igmp version** *number* **Example:** `switch(config-if)# ip igmp version 3`	Enables IGMPv3 packet support on endpoint interfaces only.
Step 14	**ip igmp immediate-leave** **Example:** `switch(config-if)# ip igmp immediate-leave`	Configures IGMP immediate leave on endpoint interfaces only.

Step 15	Configure an RP interface.
	Example:
	`switch(config)# interface loopback0`
	`  ip address 1.2.1.1/32`
	`  ip router ospf p1 area 0.0.0.0`
	`  ip pim sparse-mode`
		Make sure that the RP interface IP address is the same on each spine switch.
		Note Enter this configuration only on spine switches.

Configuring MSDP on Spine Switches

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

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

Before you begin

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

SUMMARY STEPS

1. **configure terminal**
2. Configure a loopback interface to establish an MSDP session between the spine switches.
3. **ip msdp originator-id** *interface*

4. **ip msdp peer** *peer-ip-address* **connect-source** *interface*
5. **ip msdp sa-policy** *peer-ip-address policy-name* **out**
6. **route-map** *policy-name* **permit** *sequence-number*
7. **match ip multicast group** *policy-name* **permit** *sequence-number*

DETAILED STEPS

	Command or Action	Purpose

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

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

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

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

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

Configuring Fabric and Host Interfaces

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

	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 1/49`
	`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.

	Command or Action	Purpose
Step 5	**ip pim sparse-mode** **Example:** `switch(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on this interface.
Step 6	**no shutdown** **Example:** `switch(config-if)# no shutdown`	Enables the interface.

Configuring a Layer 3 Host Interface

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

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

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.

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

Configuring a Layer 2 with SVI Host Interface

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

SUMMARY STEPS

1. **configure terminal**
2. **feature interface-vlan**
3. **vlan** *vlan-id*
4. **exit**
5. **vlan configuration** *vlan-id*
6. **ip igmp snooping**
7. **ip igmp snooping fast-leave**
8. **exit**
9. **interface vlan** *vlan-id*
10. (Optional) **ip igmp version 3**
11. **ip router ospf** *instance-tag* **area** *area-id*
12. **ip address** *ip-address*
13. **ip pim sparse-mode**
14. **ip pim passive**
15. **ip igmp suppress v3-gsq**
16. **no shutdown**
17. **exit**

18. **interface ethernet** *port/slot*
19. **switchport**
20. **switchport mode** {**access** | **trunk**}
21. **switchport** {**access** | **trunk allowed**} **vlan** *vlan-id*
22. **no shutdown**
23. **exit**

DETAILED STEPS

	Command or Action	Purpose

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

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

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

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

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

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.

	Command or Action	Purpose

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

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

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

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

Configuring NBM for a Single Modular Switch

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

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

Before you begin

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	[**no**] **feature nbm**
	Example:
	`switch(config)# feature nbm`
		Enables the NBM feature. The **no** form of this command disables this feature.
		Note If you disable NBM for Cisco Nexus 9504 and 9508 switches with -R line cards, you must configure these TCAM carving commands in the following order and reload the switch. The recommended TCAM value is 2048.
		`hardware access-list tcam region ing-nbm 0`
		`hardware access-list tcam region redirect_v6 TCAM-size`
		Note If you want to configure an NBM VRF, see Configuring an NBM VRF for Active Flow Provisioning, on page 27.

Step 3	[**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} **Example:**	Configures the global NBM flow bandwidth in Kbps, Mbps, or Gbps. The minimum supported flow bandwidth is 200 Kbps.

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td></td><td><pre>switch(config)# nbm flow bandwidth 150 mbps</pre></td><td><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></td></tr>
<tr><td>Step 4</td><td>(Optional) [no] nbm flow policer
Example:<pre>switch(config)# no nbm flow policer</pre></td><td>Enables or disables the policer for all NBM flow policies. The policer is enabled by default.</td></tr>
<tr><td>Step 5</td><td>[no] nbm flow-policy
Example:<pre>switch(config)# nbm flow-policy
switch(config-nbm-flow-pol)#</pre></td><td>Configures the flow bandwidth per flow.</td></tr>
<tr><td>Step 6</td><td>[no] policy policy-name
Example:<pre>switch(config-nbm-flow-pol)# policy 1.5gbps
switch(config-nbm-flow-pol-attr)#</pre></td><td>Configures the NBM flow policy. You can specify a maximum of 63 alphanumeric characters for the policy name.</td></tr>
<tr><td>Step 7</td><td>(Optional) [no] policer
Example:<pre>switch(config-nbm-flow-pol-attr)# no policer</pre></td><td>Enables or disables the policer for the specified NBM flow policy.
By default, each source flow uses a policer on the source leaf (the first hop router). In a scenario where the number of multicast source flows exceeds the number of policers, the flow is not accepted by the source leaf. To override this behavior, you can disable the policer under the flow policy. For flows that match the flow policy where the policer is disabled, no policer resource is consumed.
Note Use this command with caution as it could lead to an unprotected network, where a misbehaving endpoint could transmit more than what it is allowed. Use another method, such as an aggregate policer, to rate limit flows that have no policer programmed by NBM. For information on configuring an aggregate policer, see the 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 8</td><td>[no] bandwidth flow-bandwidth {kbps | mbps | gbps}
Example:<pre>switch(config-nbm-flow-pol-attr)# bandwidth 1500
 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.</td></tr>
</table>

<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 25,000,000 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></td></tr>
<tr><td>Step 9</td><td>[no] ip group ip-address
Example:
<pre>switch(config-nbm-flow-pol-attr)# ip group
228.0.0.15
switch(config-nbm-flow-pol-attr)# ip group
228.0.255.15</pre></td><td>Specifies the IP address for /32 multicast groups.</td></tr>
<tr><td>Step 10</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 group that is being configured.</td></tr>
<tr><td>Step 11</td><td>[no] ip group-range ip-address to ip-address
Example:
<pre>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</pre></td><td>Specifies the IP address range for multicast groups associated to this policy.</td></tr>
<tr><td>Step 12</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.</td></tr>
</table>

Example

The following example shows a sample configuration:

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

What to do next

Configuring an NBM VRF, on page 27

Establishing a Flow (Optional)

Configuring an NBM VRF

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

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

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

Note You must configure all VRFs in the same mode.

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

Configuring an NBM VRF for Active Flow Provisioning

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

Before you begin

Configure NBM.

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

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **nbm vrf** *vrf-name*
3. **nbm mode pim-active**
4. (Optional) [**no**] **nbm host-policy**
5. (Optional) {**sender** | **receiver** | **pim**}
6. (Optional) **default** {**permit** | **deny**}
7. (Optional) Enter one of the following commands:
   - For sender host policies: *sequence-number* **host** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
   - For local receiver host policies: *sequence-number* **host** *ip-address* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
   - For external receiver (PIM) host policies: *sequence-number* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}

8. (Optional) [**no**] **nbm reserve unicast fabric bandwidth** *value*
9. [**no**] **nbm flow asm range** [*group-range-prefixes*]
10. [**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**}
11. [**no**] **nbm flow dscp** *value*
12. (Optional) [**no**] **nbm flow reserve-bandwidth receiver-only**
13. (Optional) [**no**] **nbm flow policer**
14. [**no**] **nbm flow-policy**
15. [**no**] **policy** *policy-name*
16. (Optional) [**no**] **policer**
17. [**no**] **bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**}
18. [**no**] **dscp** *value*
19. [**no**] **ip group-range** *ip-address* **to** *ip-address*
20. (Optional) [**no**] **priority critical**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	[**no**] **nbm vrf** *vrf-name* **Example:** `switch(config)# nbm vrf nbm`	Creates an NBM VRF.
Step 3	**nbm mode pim-active** **Example:** `switch(config)# nbm mode pim-active`	Allows the NBM fabric to form a multicast flow without assistance from an external controller. **Note** You cannot disable PIM active mode for a custom NBM VRF. You can change the NBM VRF from PIM active mode to PIM passive mode but only if you first delete the custom configuration under the VRF. Otherwise, the following error appears: "NBM cannot be set to PIM-PASSIVE mode while custom config exists. Please delete all custom nbm config and retry."

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

Step 5	(Optional) {**sender** | **receiver** | **pim**}
	Example:
	`switch(config-nbm-host-pol)# sender`
	`switch(config-nbm-host-pol-sender)#`
		Configures the NBM host policy for a sender, local receiver, or external receiver (PIM).
		Note Before you update the default NBM host policy, you must first delete any custom host policies.

	Command or Action	Purpose
Step 6	(Optional) **default** {**permit** | **deny**} **Example:** `switch(config-nbm-host-pol-sender)# default permit`	Specifies the default action for the NBM host policy. All three types of host policies are allowed by default.

Step 7	(Optional) Enter one of the following commands:
	• For sender host policies: *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. NBM flow management does not use this bandwidth for flow setup and reserves it on all fabric interfaces for the unicast traffic. The range is from 0 to 100 percent, and the default value is 0.
Step 9	[**no**] **nbm flow asm range** [*group-range-prefixes*] **Example:** `switch(config)# nbm flow asm range 224.0.0.0/8 225.0.0.0/8 226.0.0.0/8 227.0.0.0/8`	Programs the NBM ASM group range for *,G joins. The IGMP joins in this group range are expected to be V2 joins or (*, G) joins. You can configure up to 20 group ranges. The default is no configured group range. **Note** This command is needed only in a multispine deployment.
Step 10	[**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} **Example:** `switch(config)# nbm flow bandwidth 3000 mbps`	Configures the global NBM flow bandwidth in Kbps, Mbps, or Gbps. The minimum supported flow bandwidth is 200 Kbps. **Range** / **Default Value** 1 to 25,000,000 Kbps / 0 Kbps 1 to 25,000 Mbps / 0 Mbps 1 to 25 Gbps / 0 Gbps

	Command or Action	Purpose
Step 11	[**no**] **nbm flow dscp** *value* **Example:** `switch(config)# nbm flow dscp 10`	Configures the global NBM flow DSCP value. The range is from 0 to 63. If any of the flows do not match the NBM flow group range, the default flow DSCP is used for bandwidth management and flow setup.
Step 12	(Optional) [**no**] **nbm flow reserve-bandwidth receiver-only** **Example:** `switch(config)# nbm flow reserve-bandwidth receiver-only`	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.
Step 13	(Optional) [**no**] **nbm flow policer** **Example:** `switch(config)# no nbm flow policer`	Enables or disables the policer for all NBM flow policies. The policer is enabled by default.

Step 14	[**no**] **nbm flow-policy**
	Example:
	`switch(config)# nbm flow-policy`
	`switch(config-nbm-flow-pol)#`
		Configures the flow bandwidth per flow.

Step 15	[**no**] **policy** *policy-name*
	Example:
	`switch(config-nbm-flow-pol)# policy nbmflow10`
	`switch(config-nbm-flow-pol-attr)#`
		Configures the NBM flow policy. You can specify a maximum of 63 alphanumeric characters for the policy name.

Step 16	(Optional) [**no**] **policer** **Example:** `switch(config-nbm-flow-pol-attr)# no policer`	Enables or disables the policer for the specified NBM flow policy. By default, each source flow uses a policer on the source leaf (the first hop router). In a scenario where the number of multicast source flows exceeds the number of policers, the flow is not accepted by the source leaf. To override this behavior, you can disable the policer under the flow policy. For flows that match the flow policy where the policer is disabled, no policer resource is consumed. **Note** Use this command with caution as it could lead to an unprotected network, where a misbehaving endpoint could transmit more than what it is allowed. Use another method, such as an aggregate policer, to rate limit flows that have no policer programmed by NBM. For information on configuring an aggregate policer, see the *Configuring Shared Policers* section in the *Configuring Policing* chapter of *Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide* on Cisco.com.

	Command or Action	Purpose
Step 17	[**no**] **bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} **Example:** `switch(config-nbm-flow-pol-attr)# bandwidth 10 mbps`	Configures the flow bandwidth in Kbps, Mbps, or Gbps for multicast groups matching this policy. The minimum supported flow bandwidth is 200 Kbps. **Range** / **Default Value** 1 to 25,000,000 Kbps / 0 Kbps 1 to 25,000 Mbps / 0 Mbps 1 to 25 Gbps / 0 Gbps
Step 18	[**no**] **dscp** *value* **Example:** `switch(config-nbm-flow-pol-attr)# dscp 10`	Configures the differentiated services code point (DSCP) value on the first-hop redundancy for flows matching the specified group range.

Step 19	[**no**] **ip group-range** *ip-address* **to** *ip-address*
	Example:
	`switch(config-nbm-flow-pol-attr)# ip group-range 224.19.10.1 to 224.19.255.1`
	`switch(config-nbm-flow-pol-attr)# ip group-range 224.20.10.1 to 224.20.255.1`
		Specifies the IP address range for multicast groups that are associated to this policy.

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

What to do next

Establishing a Flow (Optional)

Configuring an NBM VRF for Static Flow Provisioning

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

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

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

Before you begin

Configure NBM.

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	[**no**] **nbm vrf** *vrf-name* **Example:** `switch(config)# nbm vrf nbm`	Creates an NBM VRF.
Step 3	**nbm mode pim-passive** **Example:** `switch(config)# nbm mode pim-passive`	Allows the NBM fabric to form a multicast flow with assistance from an external controller.

What to do next

See the Cisco Nexus NX-API References for API details.

Configuring NBM Subinterface Type

Beginning with Cisco NX-OS Release 10.3(2)F, the subinterface with NBM 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 NBM 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 NBM interface configurations are supported with subinterface as well.

Note The **nbm bandwidth capacity** command is applicable only for the NBM 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

	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 NBM subinterface. Percentage range is 0-100, where 0 denotes no reservation for NBM bandwidth on this link. To unconfigure NBM 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 NBM flow definition or configuring IGMP static OIF. We recommend configuring an NBM flow definition.

Creating an NBM Flow Definition

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

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

Figure 1: Traffic from a Source to a Leaf

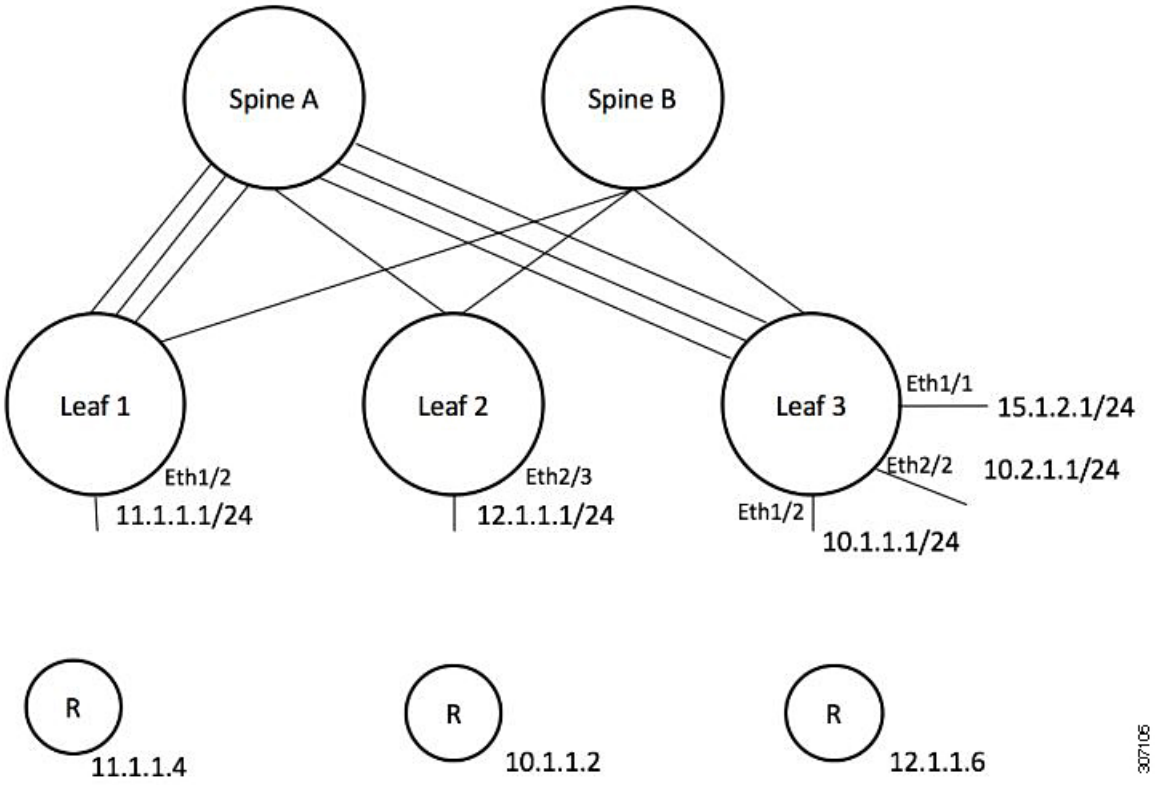
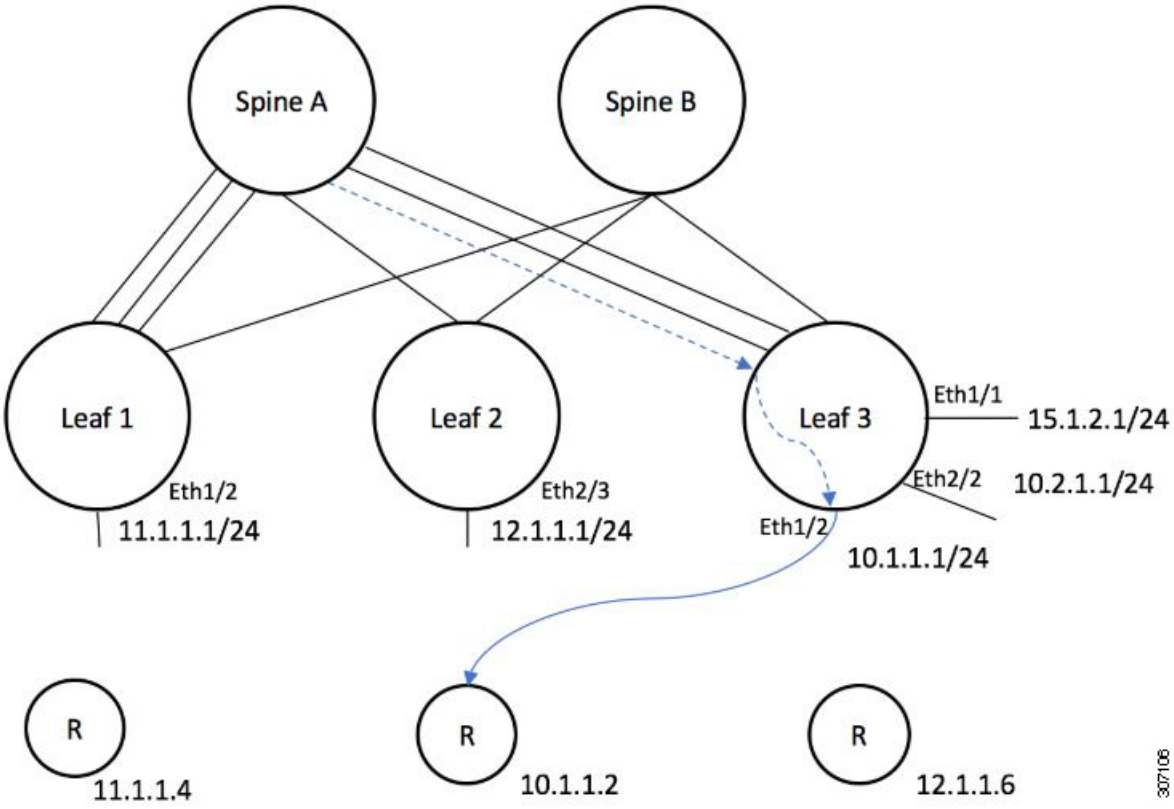


Figure 2: Traffic from the Leaf to a Receiver



Before you begin

Enable NBM.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

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

	Command or Action	Purpose

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

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

Example

The following example shows a sample configuration:

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

Configuring IGMP Static OIF

You can establish a flow by configuring a static IGMP OIF, but we recommend that you create an NBM flow definition rather than configuring static IGMP OIF.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**interface** *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

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

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

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **feature nbm**
3. **ip pim sparse mode**

4. **interface** *interface-type slot/port*
5. **nbm external-link**

DETAILED STEPS

	Command or Action	Purpose

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

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

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

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

Enabling Multicast and Unicast Flows (Optional)

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

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

	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:**	Creates an IP ACL and enters IP ACL configuration mode.

	Command or Action	Purpose
	`switch(config)# ip access-list pmn-ucast` `switch(config-acl)#`	

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

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

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

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

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

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

Step 9	**match access-group name** *acl-name* **Example:** `switch(config-cmap-qos)# match access-group name pmn-ucast`	Configures the traffic class by matching packets based on the ACL for unicast traffic.

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

Step 11	**class-map type qos match-any** *multicast-class-name* **Example:**	Creates a class map for multicast traffic and enters class-map configuration mode.

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

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

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

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

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

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

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

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

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

	Command or Action	Purpose

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

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

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

Example

Configuration example:

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

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

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

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

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

Verifying the NBM Configuration

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

Command	Description
show ip mroute *group-address*	Displays the IP multicast routing table for the specified group.
show nbm defaults [**vrf** {**all** | *vrf-name*}]	Displays the NBM default flow policy, host policies, and unicast fabric bandwidth.
show nbm flow-policy [*policy-name*] [**vrf** {**all** | *vrf-name*}]	Displays the multicast range, bandwidth, DSCP, and QoS for all configured custom flow policies or for a specific custom flow policy.
show nbm flows [[**group-based** [**group** *group-ip*] | **source** *source-ip* [**group** *group-ip*] | **group** *group-ip* [**source** *source-ip*] | **flow-policy** *pol-name* | **interface** *if-name*] [**all** | **active** | **inactive** | no-**receiver**] [**detail**] [**vrf** {*vrf-name* | **all**}]	Displays the active flows on the switch for all default and custom flow policies. Optional keywords can be added to narrow the output.
show nbm flows static [**vrf** {**all** | *vrf-name*}]	Displays the static flows for an NBM flow definition.
show nbm flows static group *group-address*	Displays the static flows for an NBM flow definition for the specified group.
show nbm flows statistics [**group-based** [**group** *group-ip*] | **source** *source-ip* [**group** *group-ip*] | **group** *group-ip* [**source** *source-ip*] | **flow-policy** *pol-name* | **interface** *if-name*] [**vrf** {**all** | *vrf-name*}]	Displays the NBM flow statistics. This command is valid on the first hop router where the senders are connected or on the switch where flows enter the fabric.
show nbm flows summary [**vrf** {**all** | *vrf-name*}]	Displays a summary of the NBM flows.
show nbm host-policy {**all** {**receiver external** | **receiver local** | **sender**} | **applied** {**receiver external** | **receiver local** {**all** | **interface** *type slot/port* | **wildcard**} | **sender** {**all** | **interface** *type slot/port* | **wildcard**}}} [**vrf** {**all** | *vrf-name*}]	Displays all NBM host policies or applied NBM host policies for external receivers (PIM), local receivers, or senders.
show nbm interface bandwidth	Displays the NBM interface bandwidth.
show running-config nbm	Displays the running configuration information for NBM.

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

For sample **show** command output, see Sample Output for Show Commands.

Clearing NBM Flow Statistics

To clear NBM 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 NBM 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 NBM 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

	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.

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

Example

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

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

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

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

```
----------------    --------------------    --------------------
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 NBM.