IPFM and Classic IPFM, Release 12.2.1

Table of Contents

New and Changed Information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Release Version	Feature	Description
NDFC release 12.2.1	IGMP host proxy configuration	The Internet Group Management Protocol (IGMP) host proxy feature helps you connect a Protocol Independent Multicast (PIM)-enabled multicast network domain to a domain that does not understand PIM. This feature configures an interface as a proxy interface that proxies PIM join or prune requests that are received on the internal PIM network to IGMP join or leave requests. Enable the IGMP source group proxy in the Layer 3 port, **int_ipfm_l3_port** policy. You can filter by proxy groups, or you can add a new proxy group. For more information, see Editing an Interface for IPFM Fabrics.
NDFC release 12.2.1	IS-IS support added as a link-state IGP for an IPFM fabric template	This feature adds support for the Intermediate System-to-Intermediate System (IS-IS) link-state Interior Gateway Protocol (IGP) in an IPFM fabric template. You configure the IS-IS IGP when creating or editing an NDFC IPFM fabric template. NOTE: Once you create an IPFM fabric template, you cannot change the IGP unless you delete and then recreate the IPFM fabric template. IS-IS support is available only for an IPFM fabric template. For more information, see General Parameters and Protocols.
NDFC release 12.2.1	Extend support for up to 120 switches in a Classic IPFM fabric	This feature extends support for up to 120 switches in a Classic IPFM fabric. For more information on the verified scalability values for NDFC, see the Verified Scalability Guide for Cisco Nexus Dashboard Controller.

IPFM Fabrics

This section describes how to configure fabrics related to IP Fabric for Media (IPFM). The IPFM fabric feature is a part of LAN fabric. To enable the IPFM fabrics feature, you must have enabled the following features on the LAN Fabric in **Admin > System Settings > Feature Management**:

- IP Fabric for Media - Starts microservices corresponding to media controller.
- PTP Monitoring - Enable if required. However, PTP monitoring is used for IPFM though it is independent of IPFM.
- Performance Monitoring - Provides for base interface monitoring.

Beginning from Nexus Dashboard Fabric Controller version 12.0.1a, the IPFM fabric templates are of the following types:

- Classic IPFM - Use the Classic IPFM fabric template to bring in switches from an existing IPFM fabric. This template works like an external or Classic LAN Fabric where only basic switch configuration such as management VRF/interface, and hostname can be imported. You can set the attribute of the fabric to Read/Write or Read-only. For the Read-only fabric, enable the monitor mode. This template supports Classic IPFM and Generic_Multicast technologies.
- IPFM - Use the IPFM template to create a new IPFM fabric with Easy Fabric management and build an underlay network for the IPFM fabric.

> IPFM Easy Fabric supports only Greenfield deployments.

We recommend that you deploy a 3-node cluster if you've more than 35 switches in your NDFC deployment. If you are using a Virtual Nexus Dashboard Cluster before you begin, ensure that the Persistent IP address and required settings are enabled for telemetry. Refer to Cisco Nexus Dashboard Fabric Controller Deployment Guide.

For a fresh installation, you can choose either IPFM Easy Fabric or IPFM Classic Fabric, based on your requirement.

Creating IPFM Fabrics

Perform the following procedures to create IPFM fabrics:

1. Create the required IPFM Fabric using the appropriate templates and set the parameters. For more information about Classic IPFM template, see Creating a Classic IPFM Fabric. For more information about IPFM template, see Creating an IPFM Fabric.
2. Add switches to the fabric and set the switch roles (only spine and leaf are supported for IPFM Fabric). For more information about adding switches, discovering existing and new switches, assigning roles, and deploying switches, see Add Switches for LAN Operational Mode.

> - IPFM Easy Fabric supports only Greenfield deployments.
> - If you add a switch to an IPFM fabric that is configured in a non-monitor mode (Active NBM), the ongoing flows on that switch will be interrupted because NDFC deletes the existing switch DME configuration and then adds the intended DME configuration as part of the process of adding a switch. This is expected behavior.

3. In the **Fabric Overview** window of your fabric, choose **Recalculate Config** from the **Actions** drop-down list. Then, in the **Deploy Configuration** window, click the **Deploy** button to deploy the configuration. For more information, see the section "Fabric Overview" in About Fabric Overview for LAN Operational Mode Setups.

   IPFM Easy Fabric: The underlay config of each switch is calculated based on the fabric settings, switch role, and switch platform.

   IPFM Classic Fabric: If you choose to have Nexus Dashboard Fabric Controller manage the interfaces for your fabric, perform host_port_resync/**Interface Config Resync** to complete the migration process for the switch. For more information about host port resync, see the section "Out-of-Band Switch Interface Configurations" in About Fabric Overview for LAN Operational Mode Setups.

   If you want to edit or delete an IPFM fabric, see Editing an IPFM Fabric or Deleting an IPFM Fabric respectively.

4. Edit the existing interfaces as required. For more information, see Editing an Interface for IPFM Fabrics. For more information about any new logical interfaces, see Creating an Interface for IPFM Fabrics.

Creating a Classic IPFM Fabric

This document describes how to create a Classic IPFM fabric using the **Classic IPFM** fabric template.

1. Navigate to the **Manage > Fabrics** page.
2. Click **Actions > Create Fabric.**

   The **Create Fabric** page appears.

   > ℹ When you log in for the first time, the **Manage > Fabrics** page displays no entries for IPFM fabrics. After you create a fabric, the IPFM fabric displays on the **Manage > Fabrics** page.

3. Enter a unique name for the fabric in the **Fabric Name** field, then click **Choose Fabric**.

   A list of all available fabric templates are listed.

4. From the available list of fabric templates, choose the **Classic IPFM** template, then click **Select**.
5. Enter the necessary field values to create a fabric.

   The tabs and their fields in the screen are explained in the following sections. The fabric-level parameters are included in these tabs.

   - General Parameters
   - Advanced
   - Bootstrap

6. When you have completed the necessary configurations, click **Save**.
   - Click on the fabric to display a summary in the slide-in pane.
   - Click on the Launch icon to display the Fabric Overview.

General Parameters

The **General Parameters** tab is displayed by default. The fields in this tab are described in the following table.

Field	Description
Fabric Technology	Specifies IPFM fabric types. Options are: ▪ **Classic IPFM** ▪ **Generic _Multicast**
Fabric Monitor Mode	Check this check box to monitor the fabric only. No configuration is deployed. From Cisco NDFC release 12.1.2e, you can configure and monitor both Non-Blocking Multicast (NBM) active and passive VRFs. In NBM passive mode, NDFC monitors the IPFM fabric without configuring it, except if you configure VRF mode as NBM passive.

Field	Description
Enable NBM Passive Mode	Check this check box to enable NBM mode in IPFM passive mode for the default VRF. ℹ You cannot edit the existing fabric to change the NBM mode. You must delete and recreate the IPFM fabric to change the NBM mode from active to passive or vice versa.
Enable Performance Monitoring	Check this check box to enable performance monitoring. Ensure that you do not clear interface counters from the command-line interface of the switches. Clearing interface counters can cause the Performance Monitor to display incorrect data for traffic utilization. If you must clear the counters and the switch has both clear counters and clear counters snmp commands (not all switches have the clear counters snmp command), ensure that you run both the main and the Simple Network Management Protocol (SNMP) commands simultaneously. For example, you must run the clear counters interface ethernet slot/port command followed by the clear counters interface ethernet slot/port snmp command. This can lead to a one time spike.

What’s next: Complete the configurations in another tab if necessary, or click **Save** when you have completed the necessary configurations for this fabric.

Advanced

The fields in the **Advanced** tab are described in the following table. All of the fields are automatically populated based on Cisco-recommended best practice configurations, but you can update the fields if needed.

Field	Description
Power Supply Mode	Choose the appropriate power supply mode. Options are: - **ps-redundant** - **combined** - **insync-redundant**
Enable AAA IP Authorization	Enables authentication, authorization, and accounting (AAA) IP authorization, when **IP Authorization** is enabled in the remote authentication server. This is required to support Nexus Dashboard Fabric Controller in scenarios where customers have strict control of which IP addresses can have access to the switches.
Enable NDFC as Trap Host	Select this check box to enable Nexus Dashboard Fabric Controller as a Simple Network Management Protocol (SNMP) trap destination. Typically, for a native high-availability Nexus Dashboard Fabric Controller deployment, the eth1 VIP IP address is configured as an SNMP trap destination on the switches. By default, this check box is enabled.

Field	Description
Enable CDP for Bootstrapped Switch	Enables Cisco Discovery Protocol on the management (mgmt0) interface for a bootstrapped switch. By default, for bootstrapped switches, Cisco Discovery Protocol is disabled on the mgmt0 interface.
Inbound Mgmt	For external and Classic LAN fabrics, this knob enables Nexus Dashboard Fabric Controller to import and manage switches with inband connectivity (reachable over switch loopback, routed, or switch virtual interface (SVI) interfaces), in addition to management of switches with out-of-band connectivity (that is, reachable over the switch mgmt0 interface). The only requirement is that for inband-managed switches, there should be IP reachability from Nexus Dashboard Fabric Controller to the switches through the Nexus Dashboard data interface. After enabling inband management, during discovery, provide the IPs of all the switches to be imported using inband management and set the maximum hops to 0. Nexus Dashboard Fabric Controller has a precheck that validates that the inband-managed switch IPs are reachable over the Nexus Dashboard data interface. Once the precheck has passed, Nexus Dashboard Fabric Controller then discovers and learns about the interface on that switch that has the specified discovery IP in addition to the VRF that the interface belongs to. As part of the process of switch import/discovery, this information is captured in the baseline intent that is populated on the Nexus Dashboard Fabric Controller. For more information, see the section "Inband Management in External Fabrics and LAN Classic Fabrics" in Configuring Inband Management, Inband POAP Management, and Secure POAP. ℹ Bootstrap or PowerOn Auto Provisioning (POAP) is only supported for switches that are reachable over out-of-band connectivity, that is, over the switch mgmt0. The various POAP services on the Nexus Dashboard Fabric Controller are typically bound to the eth1 or out-of-band interface. In scenarios, where the Nexus Dashboard Fabric Controller eth0/eth1 interfaces reside in the same IP subnet, the POAP services are bound to both interfaces.
Fabric Freeform	You can apply configurations globally across all the devices discovered in the external fabric using this freeform field.
AAA Freeform Config	Specifies the AAA freeform configurations.

Bootstrap

The fields in the **Bootstrap** tab are described in the following table. Most of the fields are automatically populated based on Cisco-recommended best practice configurations, but you can update the fields if needed.

Field	Description
Enable Bootstrap (For NX-OX Switches Only)	Select this check box to enable the bootstrap feature. Bootstrap allows easy day-0 import and bring-up of new devices into an existing fabric. Bootstrap leverages the NX-OS POAP functionality. To add more switches and for POAP capability, chose the check box for **Enable Bootstrap** and **Enable Local DHCP Server**. After you enable bootstrap, you can enable the DHCP server for automatic IP address assignment using one of the following methods: ▪ External DHCP Server: Enter information about the external DHCP server in the **Switch Mgmt Default Gateway** and **Switch Mgmt IP Subnet Prefix** fields. ▪ Local DHCP Server: Enable the **Local DHCP Server** check box and enter details for the remaining mandatory fields.
Enable Local DHCP Server	Select this check box to initiate enabling of automatic IP address assignment through the local DHCP server. When you select this check box, the **DHCP Scope Start Address** and **DHCP Scope End Address** fields become editable. If you do not select this check box, Nexus Dashboard Fabric Controller uses the remote or external DHCP server for automatic IP address assignment.
DHCP Version	Select **DHCPv4** or **DHCPv6** from this drop-down list. When you select **DHCPv4**, the **Switch Mgmt IPv6 Subnet Prefix** field is disabled. If you select **DHCPv6**, the **Switch Mgmt IP Subnet Prefix** is disabled. ℹ Cisco Nexus Dashboard Fabric Controller IPv6 POAP is not supported with Cisco Nexus 7000 Series Switches. Cisco Nexus 9000 and 3000 Series Switches support IPv6-POAP only when switches are either Layer-2 adjacent (eth1 or out-of-band subnet must be a /64) or they are Layer 3 adjacent residing in some IPv6 /64 subnet. Subnet prefixes except /64 are not supported.
DHCP Scope Start Address and DHCP Scope End Address	Specifies the first and last IP addresses of the IP address range to be used for the switch out of band POAP.
Switch Mgmt Default Gateway	Specifies the default gateway for the management VRF on the switch.

Field	Description
Switch Mgmt IP Subnet Prefix	Specifies the prefix for the mgmt0 interface on the switch. The prefix should be between 8 and 30. *DHCP scope and management default gateway IP address specification*: If you specify the management default gateway IP address 10.0.1.1 and subnet mask 24, ensure that the DHCP scope is within the specified subnet, between 10.0.1.2 and 10.0.1.254. Cisco Nexus Dashboard Fabric Controller IPv6 POAP is not supported with Cisco Nexus 7000 Series Switches. Cisco Nexus 9000 and 3000 Series Switches support IPv6 POAP only when switches are either L2 adjacent (eth1 or out-of-band subnet must be a /64) or they are L3 adjacent residing in some IPv6 /64 subnet. Subnet prefixes except /64 are not supported.
DHCP scope and management default gateway IP address specification	If you specify the management default gateway IP address 10.0.1.1 and subnet mask 24, ensure that the DHCP scope is within the specified subnet, between 10.0.1.2 and 10.0.1.254.
Switch Mgmt IPv6 Subnet Prefix	Specifies the IPv6 prefix for the mgmt0 interface on the switch. The prefix should be between 64 and 126. This field is editable if you enable IPv6 for DHCP.
Enable AAA Config	Check this check box to include AAA configurations from the **Manageability** tab as part of the device startup configuration post bootstrap.
Bootstrap Freeform Config	(Optional) Enter additional commands as needed. For example, if you require some additional configurations to be pushed to the device and be available post device bootstrap, they can be captured in this field, to save the desired intent. After the devices boot up, they will contain the configuration defined in the **Bootstrap Freeform Config** field. Copy-paste the running-config to a **freeform config** field with correct indentation, as seen in the running configuration on the NX-OS switches. The freeform configuration must match the running configuration. For more information, see Enabling Freeform Configurations on Fabric Switches.
DHCPv4/DHCPv6 Multi Subnet Scope	Specifies the field to enter one subnet scope per line. This field is editable after you check the **Enable Local DHCP Server** check box. The format of the scope should be defined as: **DHCP Scope Start Address, DHCP Scope End Address, Switch Management Default Gateway, Switch Management Subnet Prefix** For example: 10.6.0.2, 10.6.0.9, 10.6.0.1, 24

What’s next: After creating the fabric, perform **Recalculate Config** and deploy the configuration to the switches. For more information, see the section " Fabric Overview" in About Fabric Overview for LAN Operational Mode Setups.

Then, edit or create an interface as appropriate. For more information, see Interface Configuration for

IPFM Fabrics.

Creating an IPFM Fabric

This document describes the procedure to create an IPFM fabric from the IPFM fabric template.

1. Choose **Fabric Controller**.
2. Click **Manage > Fabrics.**

   The **Manage > Fabrics** page appears.

   > When you log in for the first time, the **Manage > Fabrics** table has no entries. After you create a fabric, the fabric appears on the **Manage > Fabrics** page.

3. Click **Actions > Create Fabric.**

   The **Create Fabric** page appears.

4. Enter a unique name for the fabric in the **Fabric Name** field, and click **Choose Fabric**.
5. Click **Close**.

   The **Select Type of Fabric** dialog box appears.

6. From the available list of fabric templates, choose **IPFM**, then click **Select**.
7. In the **Pick Fabric** field, click on the fabric type if you want to select a different fabric type.

   The **Select Fabric Template** window appears.

8. Enter the necessary field values to create a fabric.

   The tabs and their fields in the screen are explained in the following sections. The fabric level parameters are included in these tabs.

   - General Parameters
   - Multicast
   - Protocols
   - Advanced
   - Manageability
   - Bootstrap

General Parameters

The **General Parameters** tab is displayed by default. The fields in this tab are described in the following table.

Field	Description
Fabric Interface Numbering	Supports only numbered, point-to-point, networks.
Fabric Subnet IP Mast	Specifies the subnet mask for the fabric interface IP addresses.

Field	Description
Fabric Routing Protocol	Specifies the Cisco Interior Gateway Routing Protocol (IGP) used in the fabric. Options are: - **OSPF** - Open Shortest Path First (OSPF) is an IGP designed for IP networks that supports IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets. - **IS-IS** - Integrated Intermediate System-to-Intermediate Systems (IS-IS) is a link-state IGP for propagating information required to build a complete network connectivity map on each participating device. The map is then used to calculate the shortest path to destinations.
Fabric Routing Loopback Id	Specifies that the loopback interface ID is populated as 0 since loopback0 is usually used for fabric-underlay IGP peering purposes. The valid value ranges are from 0 to 1023.
Manual Fabric IP Address Allocation	Check this check box to disable dynamic allocation of the fabric IP address. By default, Nexus Dashboard Fabric Controller allocates the underlay IP address resources (for loopbacks, fabric interfaces, and so on) dynamically from the defined pools. If you check the check box, the allocation scheme switches to static, and some of the dynamic IP address range fields are disabled. For static allocation, the underlay IP address resources must be populated into the Resource Manager (RM) using REST APIs. For more information, see the *Cisco REST API Reference Guide, Release 12.0.1a*. The REST APIs must be invoked after the switches are added to the fabric and before you use the **Save & Deploy** option. Changing from static to dynamic allocation keeps the current IP resource usage intact. Only future IP address allocation requests are taken from dynamic pools.
Fabric Routing Loopback IP Range	Specifies the range of loopback IP addresses for protocol peering.
Fabric Subnet IP Range	Specifies the IP addresses for the underlay point-to-point routing traffic between the interfaces.
Enable Performance Monitoring	Check this check box to monitor the performance of the fabric. Ensure that you do not clear interface counters from the command-line interface of the switches. Clearing interface counters can cause the **Performance Monitor** to display incorrect data for traffic utilization. If you must clear the counters and the switch has both clear counters and clear counters snmp commands (not all switches have the clear counters snmp command), ensure that you run both the main and the SNMP commands simultaneously. For example, you must run the clear counters interface ethernet slot/port command followed by the clear counters interface ethernet slot/port snmp command. This can lead to a one time spike.

What's next: Complete the configurations in another tab if necessary, or click **Save** when you have completed the necessary configurations for this fabric.

Multicast

From Cisco NDFC Release 12.1.2e, you can configure and monitor both Non-Blocking Multicast (NBM) active and passive VRFs. In NBM passive mode, NDFC is involved only in the monitoring of the IPFM fabric and not configuration except in setting up VRF mode as NBM passive.

- You cannot deploy a VRF on a switch in read-only memory (ROM).
- In NBM or regular multicast, both sender and receiver must be in the same fabric to display active flow.

The fields in this tab are described in the following table.

Field	Description
Enable NBM Passive Mode	Check this check box to enable NBM mode to Protocol Independent Multicast (PIM) passive mode. If you enable NBM passive mode, the switch ignores all rendezvous point (RP) and Multicast Source Discovery Protocol (MSDP) configurations. This is a mandatory check box. If you check this check box, the remaining fields and check boxes are disabled. For more information, see the Configuring an NBM VRF for Static Flow Provisioning section of the Cisco Nexus 9000 Series NX-OS IP Fabric for Media Solution Guide, Release 10.2(x). You must add the **IP PIM Passive** command when you add the VRF that is in passive mode to the interface. Perform the steps below to add the **IP PIM Passive** command: 1. On the **Fabric Overview** page, choose **Links > Links**. 2. Select the appropriate fabric with the policy **int_ipfm_intra_fabric_num_link** and choose **Actions > Edit**. The **Link Management - Edit Link** page appears. 3. On the **General Parameters** tab, enter the default VRF for the **Interface VRF** name. 4. Click the **Advanced** tab, enter **IP PIM Passive** on the **Source Interface Freeform Config** and **Destination Interface Freeform Config** fields. 5. Click **Save**. You cannot edit the existing fabric to change the NBM mode. You must delete and recreate the fabric to change the NBM mode from active to passive mode or vice versa.

Field	Description
Enable ASM	Check this check box to enable groups with receiver sending (*,G) joins. If you check this check box, the **Advanced Services Module** (ASM)-related section is enabled.
NBM Flow ASM Groups for default VRF (w/wo SPT-Threshold Infinity)	Specifies ASM-related information. 1. Click the expander arrow next to the title of this section to collapse or expand the section. 2. Use the **Actions** drop-down list to add, edit, or delete the ASM groups in the table. **Add** - Choose this option to open the **Add Item** dialog box. 3. In the **Add Item** dialog box, perform the following steps: a. Enter the appropriate values in the fields and check or clear the check box as follows: ▪ **Group_Address** - Specifies the IP address for the NBM flow ASM group subnet. ▪ **Prefix** - Specifies the subnet mask length for the ASM group subnet. The valid value for the subnet mask length ranges from 4 to 32. For example, 239.1.1.0/25 is the group address with the prefix. b. **Enable_SPT_Threshold**- Check this check box to enable the shortest path tree (SPT) threshold infinity. 4. Click **Save** to add the configured NBM flow ASM groups to the table or click **Cancel** to discard the values. 5. **Edit** - Check the check box next to the group address and then choose this option to open the **Edit Item** window. 6. Open the edit item and edit the ASM group parameters. 7. Click **Save** to update the values in the table or click **Cancel** to discard the values. 8. Check the **Delete** check box next to the group address and then choose this option to delete the ASM group from the table. The table displays the values for the group address, prefix, and the enabled-SPT threshold.

What's next: Complete the configurations in another tab if necessary, or click **Save** when you have completed the necessary configurations for this fabric.

Protocols

The fields in this tab are.

Field	Description
Fabric Routing Protocol Tag	Specifies the routing process tag for the fabric.
OSPF Area Id	Specifies the OSPF area ID, if OSPF is used as the IGP within the fabric. ℹ The **OSPF** or **IS-IS** authentication fields are enabled based on your selection in the **Fabric Routing Protocol** field in the **General Parameters** tab.
Enable OSPF Authentication	Check the check box to enable OSPF authentication. Clear the check box to disable it. If you enable this field, the **OSPF Authentication Key ID** and the **OSPF Authentication Key** fields get enabled.
OSPF Authentication Key ID	Indicates that the key ID is populated.
OSPF Authentication Key	Ensure that the OSPF authentication key is the Triple Data Encryption Standard (3DES) key from the switch. ℹ Plain-text passwords are not supported. Log in to the switch, retrieve the encrypted key, and enter it in this field. For more information, see the Retrieving the Authentication Key section for details.
IS-IS Level	Choose the IS-IS level. Available options are: · **level-1** · **level-2**
Enable IS-IS Network Point-to-Point	Enables network point-to-point on numbered fabric interfaces.
Enable IS-IS Authentication	Check the check box to enable IS-IS authentication. Clear the check box to disable it. If you enable this field, the **IS-IS Key ID** field is auto populated.
IS-IS Authentication Keychain Name	Specifies the name of the IS-IS key chain.
IS-IS Authentication Key ID	Specifies the IS-IS authentication key ID.

Field	Description
IS-IS Authentication Key	Specifies the encrypted IS-IS authentication key. Log in to the switch, retrieve the encrypted key, and enter it in this field. A plain-text password gets converted to a Cisco type 7 password. For more information, see the Retrieving the Encrypted IS-IS Authentication Key section for details.
Enable PIM Hello Authentication	Enables the PIM hello authentication.
PIM Hello Authentication Key	Specifies the PIM hello authentication key.

What's next: Complete the configurations in another tab if necessary, or click **Save** when you have completed the necessary configurations for this fabric.

Advanced

The fields in this tab are.

Field	Description
Intra Fabric Interface MTU	Specifies the maximum transmission unit (MTU) for the intra fabric interface. This value must be an even number. The valid values range from 576 to 9216. This is a mandatory field.
Layer 2 Host Interface MTU	Specifies the MTU for the Layer 2 host interface. This value must be an even number. The valid values range from 1500 to 9216.
Power Supply Mode	Choose the appropriate power supply mode that will be the default mode for the fabric from the drop-down list. This is a mandatory field.
Enable CDP for Bootstrapped Switch	Check this check box to enable the Cisco Discovery Protocol on the management (mgmt0) interface for a bootstrapped switch. By default, for bootstrapped switches, Cisco Discovery Protocol is disabled on the mgmt0 interface.
Enable AAA IP Authorization	Enables AAA IP authorization, when **IP Authorization** is enabled in the remote authentication server. This is required to support Nexus Dashboard Fabric Controller in scenarios where customers have strict control of which IP addresses can have access to the switches.

Field	Description
Enable NDFC as Trap Host	Check this check box to enable Nexus Dashboard Fabric Controller as an SNMP trap destination. Typically, for a native HA Nexus Dashboard Fabric Controller deployment, the eth1 VIP IP address will be configured as SNMP trap destination on the switches. By default, this check box is enabled.
Enable Precision Time Protocol (PTP)	Enables PTP across a fabric. When you select this check box, PTP is enabled globally and on intra fabric interfaces. Additionally, the **PTP Source Loopback Id** and **PTP Domain Id** fields are editable. For more information, see PTP Configuration for IPFM Fabrics.
PTP Source Loopback Id	Specifies the loopback interface ID loopback that is used as the source IP address for all PTP packets. The valid values range from 0 to 1023. ℹ The PTP loopback ID cannot be the same as the RP loopback ID. Otherwise, an error appears. The PTP loopback ID can be the same as the Border Gateway Protocol (BGP) loopback or user-defined loopback that is created from the Nexus Dashboard Fabric Controller. The PTP loopback will be created automatically if it is not created.
PTP Domain Id	Specifies the PTP domain ID on a single network. The valid values range from 0 to 127.
PTP Profile	Select a PTP profile from the list. The PTP profile is enabled only on Inter-Switch Links (ISL) links. The supported PTP profiles are IEEE-1588v2, SMPTE-2059-2, and AES67-2015.
Leaf Freeform Config	Adds CLIs that should be added to switches that have the **Leaf**, **Border**, and **Border Gateway** roles.
Spine Freeform Config	Adds CLIs that should be added to switches with a **Spine**, **Border Spine**, **Border Gateway Spine**, and **Super Spine** roles.
Intra-fabric Links Additional Config	Adds CLIs that should be added to the intra fabric links.

What’s next: Complete the configurations in another tab if necessary, or click **Save** when you have completed the necessary configurations for this fabric.

Manageability

The fields in this tab are.

Field	Description
DNS Server IPs	Specifies the comma-separated list of IP addresses (IPv4 or IPv6) of the Domain Name System (DNS) servers.
DNS Server VRFs	Specifies one VRF for all DNS servers or a comma-separated list of VRFs, one per DNS server.
NTP Server IPs	Specifies a comma-separated list of IP addresses (IPv4 or IPv6) of the NTP server.
NTP Server VRFs	Specifies one VRF for all NTP servers or a comma-separated list of VRFs, one per NTP server.
Syslog Server IPs	Specifies a comma-separated list of IP addresses (IPv4 or IPv6) IP address of the syslog servers, if used.
Syslog Server Severity	Specifies a comma-separated list of syslog severity values, one per syslog server. The minimum value is 0 and the maximum value is 7. To specify a higher severity, enter a higher number.
Syslog Server VRFs	Specifies one VRF for all syslog servers or a comma-separated list of VRFs, one per syslog server.
AAA Freeform Config	Specifies the AAA freeform Configurations. If AAA configurations are specified in the fabric settings, a **switch_freeform** Policy Template Instance (PTI) with a source as **UNDERLAY_AAA** and description as **AAAConfigurations** is created.

What’s next: Complete the configurations in another tab if necessary, or click **Save** when you have completed the necessary configurations for this fabric.

Bootstrap

The fields in this tab are.

Field	Description
Enable Bootstrap	Check this check box to enable the bootstrap feature. Bootstrap functionality allows easy day-0 import and bring-up of new devices into an existing fabric. Bootstrap functionality leverages the NX-OS PowerOn Auto Provisioning (POAP) functionality. After you enable bootstrap functionality, you can enable the DHCP server for automatic IP address assignment for POAP using one of the following methods: - **External DHCP Server** Enter information about the external DHCP server in the **Switch Mgmt Default Gateway** and **Switch Mgmt IP Subnet Prefix** fields. - **Local DHCP Server** Enable the **Local DHCP Server** check box and enter details for the remaining mandatory fields.
Enable Local DHCP Server	Check this check box to initiate enabling of automatic IP address assignment through the local DHCP server. When you check this check box, the **DHCP Scope Start Address** and **DHCP Scope End Address** fields become editable. If you do not check this check box, Nexus Dashboard Fabric Controller uses the remote or external DHCP server for automatic IP address assignment.
DHCP Version	Select **DHCPv4** or **DHCPv6** from this drop-down list. When you select **DHCPv4**, the **Switch Mgmt IPv6 Subnet Prefix** field is disabled. If you select **DHCPv6**, the **Switch Mgmt IP Subnet Prefix** field is disabled. ℹ Cisco Nexus 9000 and 3000 Series Switches support IPv6 POAP only when switches are either Layer 2 adjacent (eth1 or out-of-band subnet must be a /64) or they are Layer 3 adjacent residing in some IPv6 /64 subnet. Subnet prefixes except /64 are not supported.
DHCP Scope Start Address	Specifies the first IP address in the IP address range to be used for the switch out-of-band POAP.
DHCP Scope End Address-	Specifies the last IP address in the IP address range to be used for the switch out-of-band POAP.
Switch Mgmt Default Gateway	Specifies the default gateway for the management VRF on the switch.

Field	Description
Switch Mgmt IP Subnet Prefix	Specifies the prefix for the mgmt0 interface on the switch. The prefix should be between 8 and 30. *DHCP scope and management default gateway IP address specification* If you specify the management default gateway IP address 10.0.1.1 and subnet mask 24, ensure that the DHCP scope is within the specified subnet, between 10.0.1.2 and 10.0.1.254.
Switch Mgmt IPv6 Subnet Prefix	Specifies the IPv6 prefix for the mgmt0 interface on the switch. The prefix should be between 64 and 126. This field is editable if you enable IPv6 for DHCP.
Enable AAA Config	Check this check box to include an AAA configurations from the **Manageability** tab as part of the device startup configuration post bootstrap.
Bootstrap Freeform Config	(Optional) Enter additional commands as needed. For example, if you require some additional configurations to be pushed to the device and be available post device bootstrap, they can be captured in this field, to save the desired intent. After the devices boot up, they will contain the configuration defined in the **Bootstrap Freeform Config** field. Copy-paste the running configuration to a **freeform config** field with the correct indentation, as seen in the running configuration on the NX-OS switches. The **freeform config** must match the running configuration. For more information on resolving freeform configuration errors in switches, see the Enabling Freeform Configurations on Fabric Switches.
DHCPv4/DHCPv6 Multi Subnet Scope	Specifies the field to enter one subnet scope per line. This field is editable after you check the **Enable Local DHCP Server** check box. The format of the scope should be defined as:
DHCP Scope Start Address, DHCP Scope End Address, Switch Management Default Gateway, Switch Management Subnet Prefix	For example, 10.6.0.2,10.6.0.9,10.6.0.1,24

What's next: Complete the configurations in another tab if necessary, or click **Save** when you have completed the necessary configurations for this fabric.

The IPFM fabric is created and displayed in the table in the **Lan Fabrics** window.

Click on the fabric to display a summary in the slide-in pane.

After creating the IPFM fabric, perform **Recalculate Config** and deploy the configuration to the switches.

For more information, see the section "Fabric Overview" in the About Fabric Overview for LAN

Operational Mode Setups.

Edit or create an interface as appropriate. For more information, see Interface Configuration for IPFM Fabrics.

Retrieving the Authentication Key

Retrieving the 3DES Encrypted OSPF Authentication Key

1. SSH into the switch.
2. On an unused switch interface, enable the following:

   ```
   config terminal
       feature ospf
       interface Ethernet1/1
         no switchport
         ip ospf message-digest-key 127 md5 ospfAuth
   ```

   In the example, **ospfAuth** is the unencrypted password.

   > ℹ This Step 2 is needed when you want to configure a new key.

3. Enter the **show run interface Ethernet1/1** command to retrieve the password.

   ```
   Switch # show run interface Ethernet1/1
     interface Ethernet1/1
       no switchport
       ip ospf message-digest key 127 md5 3 sd8478f4fsw4f4w34sd8478fsdfw
       no shutdown
   ```

   The sequence of characters after **md5 3** is the encrypted password.

4. Update the encrypted password into the **OSPF Authentication Key** field.

Retrieving the Encrypted IS-IS Authentication Key

To get the key, you must have access to the switch.

1. SSH into the switch.
2. Create a temporary keychain.

   ```
   config terminal
     key chain isis
     key 127
     key-string isisAuth
   ```

In the example, **isisAuth** is the plaintext password. This will get converted to a Cisco type 7 password after the CLI is accepted.

3. Enter the **show run | section "key chain"** command to retrieve the password.

```
key chain isis
  key 127
     key-string 7 071b245f5a
```

The sequence of characters after key-string 7 is the encrypted password. Save it.

4. Update the encrypted password into the ISIS Authentication Key field.
5. Remove any unwanted configuration made in Step 2.

Retrieving the 3DES Encrypted BGP Authentication Key

1. SSH into the switch and enable BGP configuration for a non-existent neighbor.

> Non-existent neighbor configuration is a temporary BGP neighbor configuration for retrieving the password.

```
router bgp
  neighbor 10.2.0.2 remote-as 65000
  password bgpAuth
```

In the example, **bgpAuth** is the unencrypted password.

2. Enter the show run bgp command to retrieve the password. A sample output:

```
neighbor 10.2.0.2
  remote-as 65000
  password 3 sd8478fswerdfw3434fsw4f4w34sdsd8478fswerdfw3434fsw4f4w3
```

The sequence of characters after password 3 is the encrypted password.

3. Update the encrypted password into the **BGP Authentication Key** field.
4. Remove the BGP neighbor configuration.

Retrieving the Encrypted BFD Authentication Key

1. SSH into the switch.
2. On an unused switch interface, enable the following:

```
switch# config terminal
switch(config)# int e1/1
switch(config-if)# bfd authentication keyed-SHA1 key-id 100 key cisco123
```

In the example, **cisco123** is the unencrypted password and the key ID is **100**.

> This Step 2 is needed when you want to configure a new key.

3. Enter the **show running-config interface** command to retrieve the key.

```
switch# show running-config interface Ethernet1/1

interface Ethernet1/1
description connected-to- switch-Ethernet1/1
no switchport
mtu 9216
bfd authentication Keyed-SHA1 key-id 100 hex-key 636973636F313233
no ip redirects
ip address 10.4.0.6/30
no ipv6 redirects
ip ospf network point-to-point
ip router ospf 100 area 0.0.0.0
no shutdown
```

The BFD key ID is **100** and the encrypted key is **636973636F313233**.

4. Update the key ID and key in the **BFD Authentication Key ID** and **BFD Authentication Key** fields.

Editing an IPFM Fabric

In the **LAN Fabrics** window, select the fabric that you want to edit. From the **Actions** drop-down list, choose **Edit Fabric**. Edit the fields in the template as required. Click **Save**.

> After the fabric settings are changed, perform Recalculate Config, and deploy the configuration to the switches.

Deleting an IPFM Fabric

In the **LAN Fabrics** window, select the fabric that you want to delete. From the **Actions** drop-down list, choose **Delete Fabric**. When a message appears asking whether you want to delete the fabric, click **Confirm**.

Interface Configuration for IPFM Fabrics

Cisco Nexus Dashboard Fabric Controller Web UI allows you to configure IPFM External-Links for each switch in your fabric. The external device can connect to the network through this interface by marking it as IPFM External-Link.

> A user with the network operator role in Nexus Dashboard Fabric Controller cannot save, deploy, undeploy, or edit interface configs.

Beginning with NDFC Release 12.0.1a, Interfaces in IPFM fabrics are managed by the Nexus Dashboard Fabric Controller Interface Manager. The default interface policy for IPFM is **int_ipfm_l3_port**.

The following issues are seen when NBM VRF is deleted from NDFC after interface is enabled with NBM external-link and unicast BW setting. When this occurs, the affected interfaces continues to show external-link and ucast BW as set. Perform the following steps to cleanup:

1. Select all the switches that has these interface issues under **Policies** tab using **Add Policy**.
2. Choose **host_port_resync** template and click **Save**.
3. Select **Recalculate & Deploy**. This syncs switch configuration with NDFC.
4. Select **Resync All**.

The non-fabric ethernet interface policy templates for IPFM fabrics are **int_ipfm_l3_port**, **int_ipfm_access_host**, and **int_ipfm_trunk_host**.

The port channel interface policy templates for IPFM fabrics are **int_ipfm_port_channel_access_host**,**int_ipfm_port_channel_trunk_host**, **int_ipfm_port_channel_access_member**,and **int_ipfm_port_channel_trunk_member**.

The Switch Virtual Interface (SVI) template for IPFM fabrics is **int_ipfm_vlan**.

Creating an Interface for IPFM Fabrics

This section describes the procedure to create a new interface for an IPFM fabric based on the template that you have selected from the available IPFM fabric interface templates.

> IPFM fabrics do not support V6 underlay.

1. Navigate to the **Fabric Overview** window for your fabric and click the **Interfaces** tab.
2. Choose **Create new interface** from the **Actions** drop-down list.

   The **Create new interface** window appears.

3. Select either Port Channel, Loopback, or SVI as the interface type for IPFM.
4. Select a device from the drop-down list. The switches (spine and leaf) that are a part of the fabric are displayed in the drop-down list.
5. Enter the Port Channel ID, Loopback ID, or VLAN ID, based on your choice of the interface type.
6. Click the **No Policy Selected** link to select a policy that is specific to IPFM. In the **Select Attached**

Policy Template dialog box, choose the required interface policy template and click **Save**.

7. Enter the appropriate values in the **Policy Options** area. Note that the appropriate Policy Options fields are displayed based on the policy.

   - **Type - Port Channel**

     Port Channel Member Interfaces- Specify a list of member interfaces, for example, e1/5,eth1/7-9.

     Port Channel Mode- Select one of the following channel mode options: on, active, or passive.

     Enable BPDU Guard- Select one of the following options for spanning-tree Bridge Protocol Data Unit (BPDU) guard:

     - true - enables bdpuguard
     - false - disables bpduguard
     - no - returns to default settings

   Enable Port Type Fast- Select this check box to enable spanning-tree edge port behavior.

MTU- Specify the maximum transmission unit (MTU) for the Port Channel or the MTU for the interface. The valid value range for MTU for the interface is from 576 to 9216.

SPEED - Specify the port channel speed or the interface speed.

Access Vlan- Specify the VLAN for the access port.

Trunk Allowed Vlans- Enter one of the following values:

- none
- all
- vlan ranges, for example, 1-200, 500-2000, 3000)

  Enable PTP- Select this check box to enable Precision Time Protocol (PTP) for the host interface for the IPFM fabric. For more information about PTP, see PTP Configuration for IPFM Fabrics.

PTP Profile- Select a PTP profile from the drop-down list: **IEEE-1588v2**, **SMPTE-2059-2**, or **AES67-2015**.

PTP Vlan- Specifies the PTP vlan for member interface when PTP is enabled.

Port Channel Description- Enter description for the port channel.

Freeform Config- Enter additional CLI for the port channel if required.

Enable Port Channel- Select this check box to enable the port channel.

- **Type - Loopback**

Interface VRF- Enter the name of the interface VRF. Enter **default** for default VRF.

Loopback IP- Enter an IPv4 address for the loopback interface.

Loopback IPv6 address- Enter an IPv6 address for the loopback interface if the VRF is non-default.

For default VRF add the IPv6 address in the freeform.

Route-Map TAG- Enter the Route-Map tag associated with the interface IP.

Interface Description- Enter description for the interface. The maximum size limit is 254 characters.

Freeform Config- Enter additional CLI for the loopback interface if required.

Enable Interface- Select this check box to enable the interface.

- **Type - SVI**

  Interface VRF- Enter the name of the interface VRF. Enter **default** for default VRF.

  VLAN Interface IP- Enter IP address of the VLAN interface.

  IP Netmask Length- Specify the IP netmask length used with the IP address. The valid value range is from 1 to 31.

  Routing TAG- Enter the routing tag associated with the interface IP.

  MTU- Specify the maximum transmission unit (MTU) for the Port Channel or the MTU for the interface. The valid value range for MTU for the interface is from 576 to 9216.

  Disable IP redirects- Select this check box to disable both IPv4 and IPv6 redirects on the interface.

  IPFM External-Link- Select this check box to specify that the interface is connected to an external router.

  Interface Description- Enter description for the interface. The maximum size limit is 254 characters.

  Freeform Config- Enter additional CLI for the VLAN interface if required.

  Interface Admin State- Select this check box to enable admin state for the interface.

Based on your requirements, click one of the following buttons:

- Save - Click **Save** to save the configuration changes.
- Preview - Click **Preview** to open the **Preview interfaces configuration** window and view the details.
- Deploy - Click **Deploy** to configure the interfaces.

What to do next:

If you want to edit the interface, see Editing an Interface for IPFM Fabrics.

If your interface is ready, add a policy for configuring the IPFM fabric. For more information, see Adding a Policy for Configuring an IPFM Fabric

Creating a Sub-Interface for IPFM Fabrics

This section describes the procedure to create a new sub-interface for an IPFM fabric.

1. Navigate to the **Fabric Overview** window for your fabric and click the **Interfaces** tab.
2. Select a leaf or a spine switch from the list of devices and choose **Actions > Create Subinterface**.

   The **Create Subinterface** window appears.

3. Click the **No Policy Selected** link to select a policy that is specific to IPFM.
4. In the **Select Attached Policy Template** dialog box, choose the **int_ipfm_subif** policy template and click **Select**.
5. Enter the appropriate values in the **Policy Options** area. Note that the appropriate Policy Options fields are displayed based on the policy.

   - **Type - Port Channel**

     Port Channel Member Interfaces- Specify a list of member interfaces, for example, e1/5,eth1/7-9.

     Port Channel Mode- Select one of the following channel mode options: on, active, or passive.

     Enable BPDU Guard- Select one of the following options for spanning-tree Bridge Protocol Data Unit (BPDU) guard:

     - true - enables bdpuguard
     - false - disables bpduguard
     - no - returns to default settings

   Enable Port Type Fast- Select this check box to enable spanning-tree edge port behavior.

MTU- Specify the maximum transmission unit (MTU) for the Port Channel or the MTU for the interface. The valid value range for MTU for the interface is from 576 to 9216.

SPEED - Specify the port channel speed or the interface speed.

Access Vlan- Specify the VLAN for the access port.

Trunk Allowed Vlans- Enter one of the following values:

- none
- all
- vlan ranges, for example, 1-200, 500-2000, 3000)

  Enable PTP- Select this check box to enable Precision Time Protocol (PTP) for the host interface for the IPFM fabric. For more information about PTP, see PTP Configuration for IPFM Fabrics.

PTP Profile- Select a PTP profile from the drop-down list: **IEEE-1588v2**, **SMPTE-2059-2**, or **AES67-2015**.

PTP Vlan- Specifies the PTP vlan for member interface when PTP is enabled.

Port Channel Description- Enter description for the port channel.

Freeform Config- Enter additional CLI for the port channel if required.

Enable Port Channel- Select this check box to enable the port channel.

- **Type - Loopback**

Interface VRF- Enter the name of the interface VRF. Enter **default** for default VRF.

Loopback IP- Enter an IPv4 address for the loopback interface.

Loopback IPv6 address- Enter an IPv6 address for the loopback interface if the VRF is non-default. For default VRF add the IPv6 address in the freeform.

Route-Map TAG- Enter the Route-Map tag associated with the interface IP.

Interface Description- Enter description for the interface. The maximum size limit is 254 characters.

Freeform Config- Enter additional CLI for the loopback interface if required.

Enable Interface- Select this check box to enable the interface.

- **Type - SVI**

  Interface VRF- Enter the name of the interface VRF. Enter **default** for default VRF.

  VLAN Interface IP- Enter IP address of the VLAN interface.

  IP Netmask Length- Specify the IP netmask length used with the IP address. The valid value range is from 1 to 31.

  Routing TAG- Enter the routing tag associated with the interface IP.

  MTU- Specify the maximum transmission unit (MTU) for the Port Channel or the MTU for the interface. The valid value range for MTU for the interface is from 576 to 9216.

  Disable IP redirects- Select this check box to disable both IPv4 and IPv6 redirects on the interface.

  IPFM External-Link- Select this check box to specify that the interface is connected to an external router.

  Interface Description- Enter description for the interface. The maximum size limit is 254 characters.

  Freeform Config- Enter additional CLI for the VLAN interface if required.

  Interface Admin State- Select this check box to enable admin state for the interface.

Based on your requirements, click one of the following buttons:

- Save - Click **Save** to save the configuration changes.
- Preview - Click **Preview** to open the **Preview interfaces configuration** window and view the details.
- Deploy - Click **Deploy** to configure the interfaces.

What to do next:

If you want to edit the interface, see Editing an Interface for IPFM Fabrics.

If your interface is ready, add a policy for configuring the IPFM fabric. For more information, see Adding a Policy for Configuring an IPFM Fabric

PTP Configuration for IPFM Fabrics

The Precision Time Protocol (PTP) is a protocol used to synchronize clocks throughout a computer network. When creating an interface, if you enable the **Enable PTP** check box, PTP is enabled across the fabric and on all the intrafabric interfaces. The supported PTP profiles for IPFM fabrics are **IEEE-1588v2**, **SMPTE-2059-2**, and **AES67-2015**.

A few things to note about the per-interface PTP profile for nonfabric ethernet interfaces are as follows:

- You must enable PTP and select PTP profile on each nonfabric ethernet interface.
- PTP profile can be different from the fabric level one.
- PTP must be enabled in the fabric settings before PTP can be configured on a nonfabric ethernet interface.

If PTP is disabled from the fabric settings, the PTP config will be removed from all the interfaces, that is, both the fabric and nonfabric interfaces.

For more information about PTP monitoring for IPFM fabrics, see the section " PTP (Monitoring)" in About Switch Overview for LAN Operational Mode Setups.

Editing an Interface for IPFM Fabrics

This section describes the procedure to edit an existing IPFM fabric interface template. You can either change a template or edit the values for any of the editable parameters in the **Policy Options** area.

1. Navigate to the **Manage > Fabrics** page.
2. Double-click on a fabric to open **Fabric Overview**.
3. Click on the **Interfaces** tab.
4. Choose an **easyFabric_IPFM** fabric with an **int_ipfm_13_port** policy and an **Up** operational status.
5. Choose **Edit** from the **Actions** drop-down list.

   The **Edit interface(s)** page appears.

6. To change a policy in the **Policy** field, click the policy link and select a policy that is specific to an IPFM fabric.
7. In the **Select Attached Policy Template** dialog box, choose the required interface policy template and click **Save**.
8. Edit the required values in the **Policy Options** area.

   Note that the appropriate **Policy Options** fields are displayed based on the policy. For more information about the parameters, see Creating an Interface for IPFM Fabrics.

   The following fields are specific to the **int_ipfm_l3_port** policy and the subinterface

int_ipfm_subif policy:

Field	Description
IPFM Unicast Bandwidth Percentage	Specifies the dedicated percentage of bandwidth for unicast traffic. The remaining percentage is automatically reserved for multicast traffic. If you leave this field blank, NDFC IPMF uses a global unicast bandwidth reservation.
IPFM Bandwidth Capacity Percentage	Specifies the dedicated percentage of bandwidth for this interface. If you leave this field blank, NDFC IPMF uses a global unicast bandwidth reservation.
IPFM External-Link	Check this check box to specify that the interface is connected to an external router.
Border Router	Check this check box to enable the border router configuration on the interface. The interface is a boundary of a Protocol Independent Multicast (PIM) domain.
Interface Description	Enter a description for the interface. The maximum size limit is 254 characters.
Enable Host Source Group Proxy	Check this check box to enable an IGMP host proxy on the interface. The IGMP host proxy connects a PIM-enabled multicast network to a domain different from the PIM domain. For more information on configuring an IGMP source group proxy, see the Cisco Nexus 9000 Series NX-OX Multicast Routing Configuration Guide.
IGMP Host Source Group Proxy	You can filter by proxy groups, or you can add a new proxy group. From the **Actions** drop-down list, choose **Add**, **Edit**, **Delete**, or **Insert Above** for adding IGMP proxy groups. ℹ When policy groups are associated with an IGMP source group proxy, NDFC creates a route map for the corresponding interface. Use the switch-level **Deploy** option to provision the route map on a switch. Choose a group from the drop-down list to filter by IGMP proxy groups.

9. Ensure that you check the **Enable Interface** check box.
10. Choose from one of the following options depending on your configuration:
    - Click **Save** to save the configuration changes.
    - Click **Preview** to open the **Preview interfaces configuration** window and view the details.
    - Click **Deploy** to configure the interfaces.

What to do next:

Add a policy for configuring the IPFM fabric. For more information, see Adding a Policy for Configuring an IPFM Fabric.

Adding a Policy for Configuring an IPFM Fabric

For configuration that is not uniform for all leafs or spines, additional templates are provided to help you complete the configuration of an IPFM fabric.

For example, if you enable NAT on a 9300 switch, you can create an **ipfm_tcam_nat_9300** policy to configure the required NAT TCAM for the switch.

Use the ipfm_telemetry policy for telemetry and ipfm_vrf policy for VRF config (routing, pim, asm).

1. Navigate to the **Fabric Overview** window for your fabric and click the **Policies** tab.
2. Choose **Add Policy** from the **Actions** drop-down list.

   The **Create Policy** window appears.

3. Click the right arrow in the **Select Switches** field.

   The **Select Switches** dialog box appears.

4. Select one or more switches and click **Select**.
5. In the **Create Policy** window, click **Choose Template**.
6. In the **Select a Policy Template** dialog box, select the required template for IPFM fabric, for example, **ipfm_tcam_nat_9300**. Click **Select**.
7. Enter a priority for the template. The valid value ranges from 1 to 1000.
8. Enter the values in the TCAM-related fields. Make sure that you enter the TCAM size in increments of 256 and click **Save**.

Editing a Policy for an IPFM Fabric

You can edit a policy for any switch in the IPFM fabric.

1. Navigate to the **Fabric Overview** window for your fabric and click the **Policies** tab.
2. Search for the policy template.
3. Select the policy and choose **Edit Policy** from the **Actions** drop-down list.

   The **Edit Policy** window appears.

4. Make the required changes and click **Save**.

PTP Configuration for IPFM Fabrics

The Precision Time Protocol (PTP) is a protocol used to synchronize clocks throughout a computer network. When creating an interface, if you enable the **Enable PTP** check box, PTP is enabled across the fabric and on all the intrafabric interfaces. The supported PTP profiles for IPFM fabrics are **IEEE-1588v2**, **SMPTE-2059-2**, and **AES67-2015**.

A few things to note about the per-interface PTP profile for nonfabric ethernet interfaces are as follows:

- You must enable PTP and select PTP profile on each nonfabric ethernet interface.
- PTP profile can be different from the fabric level one.
- PTP must be enabled in the fabric settings before PTP can be configured on a nonfabric ethernet interface.

If PTP is disabled from the fabric settings, the PTP config will be removed from all the interfaces, that is, both the fabric and nonfabric interfaces.

For more information about PTP monitoring for IPFM fabrics, see the section "PTP (Monitoring)" in About Switch Overview for LAN Operational Mode Setups.

Copyright

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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 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/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017-2024 Cisco Systems, Inc. All rights reserved.