IPFM およびクラシック IPFM リリース 12.1.3

目次

新機能と更新情報

次の表は、この最新リリースまでの主な変更点の概要を示したものです。ただし、今リリースまでの変更点や新機能の一部は表に記載されていません。

リリース バージョン	特長	説明
NDFC リリース 12.1.3	再編成されたコンテンツ	このドキュメント内のコンテンツは元来 *『Cisco NDFC-Fabric Controller 構成ガイド』* または *『Cisco NDFC-SAN Controller 構成ガイド』* で提供されました。 リリース 12.1.3 以降、このコンテンツは現在、このドキュメントでのみ提供されており、これらのドキュメントでは提供されなくなっています。

IPFM ファブリック

このセクションでは、IP Fabric for Media（IPFM）に関連するファブリックの構成方法について説明します。IPFM ファブリック機能は、LAN ファブリックの一部です。IPFM ファブリック機能を有効にするには、**[設定（Settings）] > [機能管理（Feature Management）]** で LAN ファブリックの次の機能を有効にする必要があります。

- メディア向け IP ファブリック：メディア コントローラに対応するマイクロサービスを開始します。
- PTP モニタリング：必要に応じて有効にします。ただし、IPFM とは独立していますが、IPTP には PTP モニタリングが使用されます。
- パフォーマンス モニタリング：基本インターフェイス モニタリングを提供します。

Nexus Dashboard Fabric Controller バージョン 12.0.1a 以降、IPFM ファブリック テンプレートには次のタイプがあります。

- クラシック IPFM：クラシック IPFM ファブリック テンプレートを使用して、既存の IPFM ファブリックからスイッチを導入します。このテンプレートは、管理 VRF/インターフェイスやホスト名などの基本的なスイッチ構成のみをインポートできる外部または LAN クラシック ファブリックのように動作します。ファブリックの属性を読み取り/書き込みまたは読み取り専用に設定できます。読み取り専用ファブリックの場合は、モニタ モードを有効にします。このテンプレートは、クラシック IPFM および Generic_Multicast テクノロジーをサポートします。
- IPFM：IPFM テンプレートを使用して、Easy ファブリック管理で新しい IPFM ファブリックを作成し、IPFM ファブリックのアンダーレイ ネットワークを構築します。

IPFM Easy ファブリックは、グリーンフィールド展開のみをサポートします。

NDFC 展開に 35 を超えるスイッチがある場合は、3 ノード クラスタを展開することをお勧めします。開始する前に仮想 Nexus ダッシュボードクラスタを使用している場合は、テレメトリ用に永続的な IP アドレスおよび必要な設定が有効になっていることを確認してください。Cisco Nexus Dashboard Fabric Controller 導入ガイドを参照してください。

新規インストールの場合は、要件に応じて IPFM Easy ファブリックまたは IPFM クラシック ファブリックを選択できます。

IPFM ファブリックの作成

IPFM ファブリックを作成するには、次の手順を実行します。

1. 適切なテンプレートを使用して必要な IPFM ファブリックを作成し、パラメータを設定します。クラシック IPFM（Classic IPFM）テンプレートの詳細については、クラシック IPFM ファブリックの作成を参照してください。IPFM テンプレートの詳細については、IPFM ファブリックの作成を参照してください。
2. ファブリックにスイッチを追加し、スイッチのロールを設定します（IPFM ファブリックではスパインとリーフのみがサポートされます）。スイッチの追加、既存および新規スイッチの検出、ロールの割り当て、およびスイッチの導入の詳細については、LAN 動作モードのスイッチの追加を参照してください。

IPFM Easy ファブリックは、グリーンフィールド展開のみをサポートします。

3. ファブリックの **[ファブリックの概要（Fabric Overview）]** ウィンドウで、**[アクション（Actions）]** ドロップダウン リストから **[構成の再計算（Recalculate Config）]** を選択します。

   ドロップダウンリスト。次に、**[構成の展開（Deploy Configuration）]** ウィンドウで、**[展開（Deploy）]** ボタンをクリックして構成を展開します。詳細については、 LAN 動作モード設定のファブリックの概要の「ファブリックの概要」セクションを参照してください。

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

   IPFMクラシック ファブリック：ファブリックのインターフェイスを Nexus ダッシュボード ファブリック コントローラで管理する場合は、host_port_resync/Interface Config Resync を実行して、スイッチの移行プロセスを完了します。ホスト ポートの再同期の詳細については、アウトオブバンド スイッチ インターフェイス構成の同期の「アウトオブバンド スイッチ インターフェイス構成の同期」の項を参照してください。

   IPFM ファブリックを編集または削除する場合は、IPFM ファブリックの編集または IPFM ファブリックの削除を参照してください。

4. 必要に応じて既存のインターフェイスを編集します。詳細については、IPFM ファブリックのインターフェイスの編集を参照してください。新しい論理インターフェイスの詳細については、IPFM ファブリックのインターフェイスの作成を参照してください。

IPFM クラシック ファブリックの作成

ここでは、**[クラシック IPFM（Classic IPFM）]** テンプレートから IPFM クラシック ファブリックを作成する手順について説明します。
追加します。

1. **[LAN ファブリック（LAN Fabrics）]** ウィンドウで、**[アクション（Actions）]** ドロップダウン リストから **[ファブリックの作成（Create Fabric）]** を選択します。

   [ファブリックの作成（Create Fabric）] ウィンドウが表示されます。

   初めてログインしたときには、[LAN ファブリック（Lan Fabrics）] ウィンドウに IPFM ファブリックのエントリが表示されません。ファブリックが作成されると、[LAN ファブリック（Lan Fabrics）] ウィンドウに表示されます。
   閉じます。

2. **[ファブリックの作成（Create Fabric）]** ウィンドウで、ファブリック名を入力し、**[ファブリックの選択（Choose Fabric）]** をクリックします。

   [ファブリック テンプレートの選択（Select Fabric Template）] ウィンドウが表示されます。

3. **クラシック IPFM（Classic IPFM）** ファブリック テンプレートを検索またはスクロールして選択します。**[選択（Select）]** をクリックします。

   [ファブリックの作成（Create Fabric）] ウィンドウは次の要素を表示します。

   [ファブリック名（Fabric Name）]：入力したファブリック名を表示します。

   [テンプレートの選択（Pick Template）]：選択したテンプレートの型を表示します。テンプレートを変更するには、そのテンプレートをクリックします。**[ファブリック テンプレートの選択（Select Fabric Template）]** ウィンドウが表示されます。現在の手順を繰り返します。

   [全般パラメータ（General Parameters）]、**[詳細（Advanced）]**、および **[ブートストラップ（Bootstrap）]** タブ：IPFM クラシック ファブリックを作成するためのファブリック構成を表示します。

4. デフォルトでは、**[全般パラメータ（General Parameters）]** タブが表示されます。このタブのフィールドは次のとおりです。

   ファブリック テクノロジー（Fabric Technology）：ドロップダウンリストから次のいずれかのテクノロジーを選択します。

   - **クラシック IPFM**
   - **[Generic_Multicast]**

     ファブリック モニタ モード（Fabric Monitor Mode）：ファブリックのみをモニタし、構成を展開しない場合は、このチェックボックスをオンにします。

     Cisco NDFC リリース 12.1.2e から非ブロッキング マルチキャスト（NBM ）現用系とパッシブ VRF 両方を構成し、モニタリングできます。NBM パッシブ モードで NDFC は、IPFM ファブリックのモニタリングのみに参加されます。VRF モードを NBM パッシブに設定する以外

の構成には参加しません。

[NBM パッシブモードの有効化（Enable NBM Passive Mode）]：このチェックボックスをオンにすると、NBM モードが デフォルト VRF の IPFM パッシブ になります。

NBM モードを変更するために既存のファブリックを編集できません。

NBM モードを現用系からパッシブ、またはその逆に変更するには、ファブリックを削除して再作成する必要があります。

[パフォーマンス モニタリングの有効化（Enable Performance Monitoring）]：ファブリックのパフォーマンスをモニタリングするには、このチェックボックスをオンにします。

5. **[詳細（Advanced）]** タブをクリックします。このタブのフィールドは次のとおりです。

電源モード（Power Supply Mode）：適切な電源モードを選択します。

[AAA IP 認証の有効化（Enable AAA IP Authorization）]：AAA サーバーで IP 認証が有効になっている場合に、AAA IP 認証を有効にします。

NDFC をトラップ ホストとして有効にする（Enable NDFC as Trap Host）：Nexus ダッシュボード ファブリック コントローラをトラップ ホストとして有効にするには、このチェックボックスをオンにします。

[ブートストラップ スイッチの CDP の有効化（Enable CDP for Bootstrapped Switch）]：管理インターフェイスで CDP を有効にします。

[インバンド管理（Inband Mgmt）]：外部およびクラシック LAN ファブリックの場合、このノブを使用すると Nexus Dashboard Fabric Controller は、インバンド接続（スイッチ ループバック、ルーテッド、または SVI インターフェイス経由で到達可能）でのスイッチのインポートおよび管理が可能になり、またアウトオブバンド接続（つまり、スイッチ mgmt0 インターフェイス経由で到達可能）でのスイッチの管理が可能になります。

唯一の要件は、インバンド管理対象スイッチの場合、 Nexus ダッシュボード ファブリック コントローラから Nexus ダッシュボード データを介してスイッチに IP が到達可能であることです。インバンド管理を有効にした後、検出中に、インバンド管理を使用してインポートするすべてのスイッチの IP を指定し、最大ホップ数を 0 に設定します。

Nexus ダッシュボード ファブリック コントローラは、インバンド管理されたスイッチ IP が Nexus ダッシュボード データ インターフェイスを介して到達可能であるかを検証する事前チェックを行います。事前チェックをパスすると、 Nexus ダッシュボード ファブリック コントローラはインターフェイスが属する VRF に加えて、指定された検出 IP を持つそのスイッチ上のインターフェイスを検出し、学習します。

スイッチのインポート/検出のプロセスの一部として、この情報は Nexus ダッシュボード ファブリック コントローラに入力される目的のベースラインにキャプチャされます。詳細については、Configuring Inband Management, Inband POAP Management, and Secure POAP の「Inband Management in External Fabrics and LAN Classic Fabrics」の項を参照してください。

ヒント：	ブートストラップまたは POAP は、アウトオブバンド接続、つまりスイッチ mgmt0 を介して到達可能なスイッチでのみサポートされます。Nexus Dashboard Fabric Controller 上のさまざまな POAP サービスは通常、eth1 またはアウトオブバンド インターフェイスにバインドされます。Nexus Dashboard

Fabric Controller の eth0 / eth1 インターフェイスが同じ IP サブネットに存在するシナリオでは、POAP サービスは両方のインターフェイスにバインドされます。

[ファブリック自由形式（Fabric Freeform）]：この自由形式フィールドを使用して、外部ファブリックで検出されたすべてのデバイスに構成をグローバルに適用できます。

[AAA フリーフォームの設定（AAA Freeform Config）：AAA フリーフォームの設定を指定します。

6. **[ブートストラップ（Bootstrap）]** タブをクリックします。このタブのフィールドは次のとおりです。
[ブートストラップの有効化（NX-OS スイッチのみ）（Enable Bootstrap）（For NX-OS Switches Only））]：Cisco Nexus スイッチのみに対してブートストラップ機能を有効にするにはこのチェックボックスをオンにします。このチェックボックスをオンにすると、POAP の自動 IP 割り当てが有効になります。

   ブートストラップをイネーブルにした後、次の方法を使用して、POAP の自動 IP アドレス割り当てに対して DHCP サーバをイネーブルにできます。

   - **[外部 DHCP サーバー（External DHCP Server）]**：**[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]** および [*スイッチ管理 IP サブネット プレフィックス*（Switch Mgmt IP Subnet Prefix）] フィールド**に外部 DHCP サーバーに関する情報を入力します。**
   - **[ローカル DHCP サーバー（Local DHCP Server）]：[ローカル DHCP サーバー（Local DHCP Server）]** チェックボックスをオンにして、残りの必須フィールドに詳細を入力します。

     [ローカル DHCP サーバの有効化（Enable Local DHCP Server）]：ローカル DHCP サーバを介した自動 IP アドレス割り当ての有効化を開始するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、残りのすべてのフィールドが編集可能になります。

     DHCP バージョン（DHCP Version）：ドロップダウンリストから [DHCPv4] または [DHCPv6] を選択します。[DHCPv4] を選択すると、**[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]** フィールドは無効になります。DHCPv6 を選択すると、**[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）] は**無効になります。

     > Cisco Nexus Dashboard Fabric Controller の IPv6 POAP は、Cisco Nexus 7000 シリーズ スイッチではサポートされていません。Cisco Nexus 9000 および 3000 シリーズ
     >
     > スイッチは、スイッチが L2 隣接（eth1 またはアウトオブバンド サブネットは /64 である必要があります）である場合、またはいずれかの IPv6 / 64 サブネットに存在する L3 隣接である場合にのみ、IPv6 POAP をサポートします。 /64 以外のサブネット プレフィックスはサポートされていません。

     このチェックボックスをオンにしない場合、Nexus ダッシュボード ファブリック コントローラは自動 IP アドレス割り当てにリモートまたは外部DHCPサーバを使用します。

     [DHCP スコープ開始アドレス（DHCP Scope Start Address）] および**[DHCP スコープ終了**

アドレス（DHCP Scope End Address）]：スイッチ アウトオブバンド POAP に使用される IP アドレス範囲の最初と最後の IP アドレスを指定します。

[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]：スイッチの管理 VRF のデフォルト ゲートウェイを指定します。

[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]：スイッチの Mgmt0 インターフェイスのプレフィックスを指定します。プレフィックスは 8 ～ 30 の間である必要があります。

DHCP 範囲および管理デフォルト ゲートウェイ IP アドレスの仕様（DHCP scope and management default gateway IP address specification）**：管理デフォルト ゲートウェイ IP アドレスを 10.0.1.1 に、サブネット マスクを 24 に指定した場合、DHCP 範囲が指定したサブネット、10.0.1.2 ～ 10.0.1.254 の範囲内であることを確認してください。**

[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]：スイッチの Mgmt0 インターフェイスの IPv6 プレフィックスを指定します。プレフィックスは 64 ～ 126 の間である必要があります。このフィールドは DHCP の IPv6 が有効な場合に編集できます。

ブートストラップ自由形式の構成（Bootstrap Freeform Config）：（オプション）必要に応じて追加のコマンドを入力します。たとえば、AAA またはリモート認証関連の構成を使用している場合は、このフィールドにこれらの構成を追加してインテントを保存する必要があります。デバイスが起動すると、**[ブートストラップ自由形式の構成（Boostrap Freeform Config）]** フィールド**で定義されたインテントが含まれます。**

running-config をコピーして **[フリーフォーム構成（freeform config）]** フィールドに、NX-OS スイッチの実行設定と同様の、正しいインデントでコピーアンドペーストします。freeform config は running-config と一致する必要があります。*スイッチでのフリーフォーム構成エラーの解決方法については*、ファブリック スイッチでのフリーフォーム構成の有効化を参照してください。

[DHCPv4/DHCPv6 マルチ サブネット スコープ（DHCPv4/DHCPv6 Multi Subnet Scope）]：フィールドで 1 行に 1 つのサブネット スコープを入力するように指定します。このフィールドは、[*ローカル DHCP サーバーの有効化*（Enable Local DHCP Server）] チェックボックスを**オンにした後に編集できます。**

範囲のフォーマットは次のように定義される必要があります：

[DHCP スコープ開始アドレス、DHCP スコープ終了アドレス、スイッチ管理デフォルト ゲートウェイ、スイッチ管理サブネット プレフィックス（DHCP Scope Start Address, DHCP Scope End Address, Switch Management Default Gateway, Switch Management Subnet Prefix）]

たとえば、16.0.0.2, 10.6.0.9, 10.6.0.1, 24 です。

7. **[保存（Save）]** をクリックします。

IPFM クラシック ファブリックが作成され、**[LAN ファブリック（Lan Fabrics）]** ウィンドウのテーブルに表示されます。

次に行う作業：

ファブリックの作成後、[構成の再計算（Recalculate Config）] を実行し、スイッチに構成を行っ

てください。詳細については、 LAN 動作モード設定のファブリックの概要の「ファブリックの概要」セクションを参照してください。

その後必要に応じて、インターフェイスを編集または作成してください。詳細については、 IPFM ファブリック向けインターフェイスの構成を参照してください。

IPFM Easy ファブリックの作成

ここでは、[IPFM ファブリック（IPFM fabric）] テンプレートから IPFM Easy ファブリックを作成する手順について説明します。

1. **[LAN ファブリック（LAN Fabrics）]** ウィンドウで、**[アクション（Actions）]** ドロップダウン リストから **[ファブリックの作成（Create Fabric）]** を選択します。

   [ファブリックの作成（Create Fabric）] ウィンドウが表示されます。

   > ヒント： 初めてログインしたときには、[LAN ファブリック（Lan Fabrics）] テーブルにはまだエントリはありません。ファブリックが作成されると、**[LAN ファブリック（Lan Fabrics）]** ウィンドウに表示されます。

2. **[ファブリックの作成（Create Fabric）]** ウィンドウで、ファブリック名を入力し、**[ファブリックの選択（Choose Fabric）]** をクリックします。

   [ファブリック テンプレートの選択（Select Fabric Template）] ウィンドウが表示されます。

3. **IPFM** テンプレートを検索またはスクロールして選択します。**[選択（Select）]** をクリックします。

   [ファブリックの作成（Create Fabric）] ウィンドウは次の要素を表示します。

   [ファブリック名（Fabric Name）]：入力したファブリック名を表示します。

   [テンプレートの選択（Pick Template）]：選択したテンプレートの型を表示します。テンプレートを変更するには、そのテンプレートをクリックします。**[ファブリック テンプレートの選択（Select Fabric Template）]** 画面が表示されます。現在の手順を繰り返します。

   [全般パラメータ（General Parameters）]、**[マルチキャスト（Multicast）]**、**[プロトコル（Protocols）]**、**[詳細（Advanced）]**、**[管理性（Manageability）]**、および **[ブートストラップ（Bootstrap）]** タブ：IPFM Easy Fabric を作成するためのファブリック設定を表示します。

4. デフォルトでは、**[全般パラメータ（General Parameters）]** タブが表示されます。このタブのフィールドは次のとおりです。

   [ファブリックインターフェイスの番号付け（Fabric Interface Numbering）]：番号付き（ポイントツーポイント、つまり **p2p**）ネットワークのみをサポートします。

   [ファブリック サブネット IP マスク（Fabric Subnet IP Mask）]：ファブリック インターフェイスの IP アドレスのサブネット マスクを指定します。

   [ファブリック ルーティング プロトコル（Fabric Routing Protocol）]：ファブリック、OSPF、または IS-IS で使用される IGP。

   [ファブリック ルーティング ループバック ID（Fabric Routing Loopback Id）]：loopback0 は通常ファブリック アンダーレイ IGP ピアリングに使用されるため、ループバック インターフェイス ID は 0 と設定されます。有効な値の範囲は 0 ～ 1023 です。

   [手動ファブリック IP アドレス割り当て（Manual Fabric IP Address Allocation ）]：ファブリック IP アドレスの動的割り当てを無効にします。

   - デフォルトでは、Nexus Dashboard Fabric Controller. は定義されたプールから動的にアンダ

ーレイ IP アドレス リソース（ループバック、ファブリック インターフェイスなど）を割り当てます。このチェックボックスをオンにすると、割り当て方式が静的に切り替わり、動的 IP アドレス範囲フィールドの一部が無効になります。

- 静的割り当ての場合、REST API を使用してアンダーレイ IP アドレス リソースをリソース マネージャ（RM）に入力する必要があります。
- 詳細については、 *Cisco REST API Reference Guide*、*リリース 12.0.1a* を参照してください。スイッチをファブリックに追加した後、REST APIを呼び出してから **[保存して展開（Save & Deploy）]** オプションを使用する必要があります。
- 静的割り当てから動的割り当てに変更しても、現在の IP リソースの使用情況は維持されます。それ以後の IP アドレス割り当て要求のみが動的プールから取得されます。

[ファブリック ルーティング ループバック IP 範囲（Fabric Routing Loopback IP Range）]：プロトコル ピアリングのループバック IP アドレスの範囲を指定します。

[ファブリック サブネットIP範囲（Fabric Subnet IP Range）]：インターフェイス間のアンダーレイ P2P ルーティング トラフィックの IP アドレス。

[パフォーマンス モニタリングの有効化（Enable Performance Monitoring）]：ファブリックのパフォーマンスをモニタリングするには、このチェックボックスをオンにします。

5. **[マルチキャスト（Multicast）]** タブをクリックします。このタブのフィールドは次のとおりです。

Cisco NDFC リリース 12.1.2e から NBM 現用系とパッシブ VRF 両方を構成とモニタできます。NBM パッシブ モードで NDFC は、IPFM ファブリックのモニタリングのみに参加されます。VRF モードを NBM パッシブに設定する以外の構成には参加しません。

ROM のスイッチに VRF を展開することはできません。

[NBM パッシブモードの有効化（Enable NBM Passive Mode）]：このチェックボックスをオンにすると、NBM モードが pim-passive になります。NBM パッシブ モードを有効にすると、スイッチはすべての RP および MSDP 設定を無視します。これは必須のチェックボックスです。このチェックボックスをオンにすると、残りのフィールドとチェックボックスは無効になります。詳細については、 Cisco Nexus 9000 シリーズ NX-OS IP ファブリック メディア ソリューション ガイド、リリース 10.2(x) の スタティック フロー プロビジョニング向け NBM VRF の設定 セクションを参照してください。

パッシブ モードの VRF をインターフェイスに追加する場合は、**[IP PIM パッシブ（IP PIM Passive）]** コマンドを追加する必要があります。**[IP PIM パッシブ（IP PIM Passive）]** コマンドを追加するには、次の手順を実行します。

- **[ファブリックの概要（Fabric Overview）]** ウィンドウで、**[リンク（Links）] > [リンク（Links）]** を選択します。
- ポリシー **int_ipfm_intra_fabric_num_link** で適切なファブリックを選択し、**[アクション（Actions）] > [編集（Edit）] を選択します**。

  [リンク管理 - リンクの編集（Link Management- Edit Link）] ウィンドウが表示されます。

- **[全般パラメータ（General Parameters）]** タブで、[インターフェイス VRF（Interface VRF）] 名にデフォルトまたはデフォルト VRF を入力します。

6. **[詳細（Advanced）]** タブをクリックし、**[送信元 インターフェイス 自由形式構成（Source**

Interface Freeform Config）] および
[接続先 インターフェイス自由形式構成（Destination Interface Freeform Config）] フィールドに **[IP PIM パッシブ（IP PIM Passive）]** と入力します。

7. **[保存（Save）]** をクリックします。

NBM モードを変更するために既存のファブリックを編集できません。NBM モードを現用系からパッシブまたは、パッシブから現用系に変更するには、ファブリックを削除して再作成する必要があります。

[ASMの有効化（Enable ASM）] : (*,G)結合を送信する受信者を持つグループを有効に

するには、このチェックボックスをオンにします。このチェックボックスをオンにする

と、ASM 関連のセクションが有効になります。

[デフォルト VRF のための NBM フロー ASM グループ（SPT しきい値無限あり/なし）（NBM Flow ASM Groups for default VRF（w / wo SPT-Threshold Infinity））] : このセクションは、ASM 関連の情報で構成されます。

- セクションを縮小または展開するには、このセクションのタイトルの横にある展開矢印をクリックします。
- **[アクション（Actions）]** ドロップダウンリストを使用して、テーブル内の ASM グループを追加、編集、または削除します。
  - **[追加（Add）]** : **[項目の追加（Add Item）]** ウィンドウを開きます。**[項目の追加（Add Item）]** ウィンドウで、次の手順を実行します。
    a. フィールドに適切な値を入力し、次のようにチェックボックスをオンまたはオフにします。
      - [Group_Address] : **NBM フロー ASM グループ サブネットの IP アドレスを指定します。**
      - **[プレフィックス（Prefix）]** : ASM グループ サブネットのサブネット マスク長を指定します。サブネット マスク長の有効な値の範囲は 4 ～ 32 です。たとえば、239.1.1.0 / 25 はプレフィックス付きのグループ アドレスです。
      - **[Enable_SPT_Threshold]** : SPT しきい値の無限を有効にするには、このチェックボックスをオンにします。
    b. **[保存（Save）]** をクリックして、設定した NBM フロー ASM グループをテーブルに追加するか、**[キャンセル（Cancel）]** をクリックして値を破棄します。
  - **[編集（Edit）]** : グループアドレスの横にあるチェックボックスをオンにし、**[項目の編集（Edit Item）]** ウィンドウを開きます。編集項目を開き、ASM グループパラメータを編集します。**[保存（Save）] をクリックして**テーブルの値を更新するか、**[キャンセル（Cancel）]** をクリック**して値を破棄します。**
  - **[削除（Delete）]** : テーブルからASMグループを削除するには、グループ アドレスの横にあるチェックボックスをオンにし、このオプションを選択します。
- テーブルには、グループ アドレス、プレフィックス、および SPT 有効化しきい値の値が表示されます。

RP ループバック ID（RP Loopback Id） ：ファブリック アンダーレイでのマルチキャスト プロトコル ピアリングの目的で、ランデブー ポイント（RP）に使用されるループバック ID。有効な値の範囲は 0 ～ 1023 です。**ファブリック RP ループバック IP 範囲（Fabric RP Loopback IP Range）** ：RP ループバック IP アドレス範囲を指定します。

8. **[プロトコル（Protocols）]** タブをクリックします。

   このタブのフィールドは次のとおりです。

   ファブリック ルーティング プロトコル タグ（Fabric Routing Protocol Tag） ：ファブリックのルーティング プロセス タグを指定します。

   OSPF エリア ID（OSPF Area Id） ：OSPF がファブリック内で IGP として使用されている場合の OSPF エリア ID。

   > ヒント： [OSPF] または [IS-IS] 認証フィールドは、**[ファブリック ルーティング プロトコル（Fabric Routing Protoco）l]** フィールド（[全般パラメータ（General Parameters）]タブ）での選択に基づいて有効になります。

   [OSPF 認証を有効にする（Enable OSPF Authentication）]：OSPF 認証を有効にするには、このチェックボックスをオンにします。無効にするには、チェックボックスをオフにします。このフィールドを有効にすると、[OSPF 認証キー ID（OSPF Authentication Key ID）] および [OSPF 認証キー（OSPF Authentication Key）] フィールドが有効になります。

   [OSPF 認証キー ID（OSPF Authentication Key ID）]：キー ID が入力されます。

   [OSPF 認証キー（OSPF Authentication Key）]：OSPF 認証キーは、スイッチからの 3DES キーである必要があります。

   > ヒント： プレーン テキスト パスワードはサポートされていません。スイッチにログインし、暗号化キーを取得して、このフィールドに入力します。

   詳細については、 認証キーの取得の項を参照してください。

   [IS-IS レベル（IS-IS Level）]：このドロップダウン リストから IS-IS レベルを選択します。

   [IS-IS ネットワーク ポイントツーポイントの有効化（Enable IS-IS Network Point-to-Point）]：番号付きのファブリック インターフェイスでネットワーク ポイントツーポイントを有効にします。

   [IS-IS 認証の有効化（Enable IS-IS Authentication）]：IS-IS 認証を有効にするには、チェックボックスをオンにします。無効にするには、チェックボックスをオフにします。このフィールドを有効にすると、[IS-IS] 認証フィールドが有効になります。

   [IS-IS 認証キーチェーン名（IS-IS Authentication Keychain Name）]：キーチェーン名を入力します（例：CiscoisisAuth）。

   [IS-IS 認証キー ID（IS-IS Authentication Key ID） ：キー ID が入力されます。

   [IS-IS 認証キー（IS-IS Authentication Key）]：Cisco Type 7 暗号化キーを入力します。

   

   プレーン テキスト パスワードはサポートされていません。

   スイッチにログインし、暗号化キーを取得して、このフィールドに入力

   します。詳細については、認証キーの取得の項を参照してください。

   [PIM hello 認証の有効化（Enable PIM Hello Authentication）]：PIM hello 認証を有効にします。

[PIM Hello 認証キー（PIM Hello Authentication Key）]：PIM hello 認証キーを指定します。

9. **[詳細（Advanced）]** タブをクリックします。

   このタブのフィールドは次のとおりです。

   [イントラ ファブリック インターフェイス MTU（Intra Fabric Interface MTU）]：ファブリック内インターフェイスの MTU を指定します。この値は偶数にする必要があります。有効な値の範囲は 576 ～ 9216 です。これは必須フィールドです。

   [レイヤ 2 ホスト インターフェイス MTU（Layer 2 Host Interface MTU）]：レイヤ 2 ホストインターフェイスの MTU を指定します。この値は偶数にする必要があります。有効な値の範囲は 1500 ～ 9216 です。

   [電源モード（Power Supply Mode）]：ドロップダウンリストから、ファブリックのデフォルト モードとなる適切な電源モードを選択します。これは必須フィールドです。

   [ブートストラップ スイッチの CDP を有効にする（Enable CDP for Bootstrapped Switch）]：ブートストラップ スイッチの管理（mgmt0）インターフェイスで CDP を有効にします。デフォルトでは、ブートストラップ スイッチの場合、mgmt0 インターフェイスで CDP は無効にされています。

   [AAA IP 認証の有効化（Enable AAA IP Authorization）]：IP 認証がリモート認証サーバーで有効になっている場合に、AAA IP 認証を有効にします。これは、スイッチにアクセスできる IP アドレスを顧客が厳密に制御できるシナリオで Nexus ダッシュボード ファブリック コントローラ をサポートするために必要です。

   [NDFC をトラップ ホストとして有効化（Enable NDFC as Trap Host）]：SNMP トラップの接続先として Nexus ダッシュボード ファブリック コントローラを有効にするには、このチェックボックスをオンにします。通常、ネイティブHA Nexusダッシュボードファブリックコントローラの導入では、eth1 VIP IPアドレスがスイッチのSNMPトラップ宛先として設定されます。デフォルトでは、このチェックボックスは有効になっています。

   [精密時間プロトコル（PTP）の有効化（Enable Precision Time Protocol（PTP））]：ファブリック全体で PTP を有効にします。このチェックボックスをオンにした場合

   PTP はグローバルに、およびファブリック内インターフェイスで有効になります。また、**[PTP 送信元ループバック ID（PTP Source Loopback Id）]** および **[PTP ドメイン ID（PTP Domain Id）]** フィールドが編集可能になります。詳細については、高精度時間プロトコルの「Easy ファブリック向け高精度時間プロトコル」の項を参照してください。

   [PTP 送信元ループバック ID（PTP Source Loopback Id）]すべての PTP パケットの送信元 IP アドレスとして使用されるループバック インターフェイス ID ループバックを指定します。有効な値の範囲は 0 ～ 1023 です。PTP ループバック ID を RP ループバック ID と同じにすることはできません。そうした場合は、エラーが表示されます。PTP ループバック ID は、BGP ループバックまたは Nexus ダッシュボード ファブリック コントローラから作成されたユーザー定義ループバックと同じにすることができます。PTP ループバックが作成されていない場合は、自動的に作成されます。

   [PTP ドメイン ID]：単一のネットワーク上の PTP ドメイン ID を指定します。有効な値の範囲は 0 ～ 127 です。

   [PTP プロファイル（PTP Profile） ：リストから PTP プロファイルを選択します。PTP プロファ

イルは、ISL リンクでのみ有効になります。サポートされている PTP プロファイルは、IEEE-1588v2、SMPTE-2059-2、および AES67-2015 です。

[リーフの自由形式の設定（Leaf Freeform Config）]：リーフ、境界、および境界ゲートウェイの役割を持つスイッチに追加する必要がある CLI です。

[スパインの自由形式の設定（Spine Freeform Config）]：スパイン、境界スパイン、境界ゲートウェイ スパイン、および スーパー スパインのロールを持つスイッチに追加する必要がある CLI を追加します。

[ファブリック内リンクの追加設定（Intra-fabric Links Additional Config）]：ファブリック内リンクに追加する CLI を追加します。

10. **[管理性（Manageability）]** タブをクリックします。

    このタブのフィールドは次のとおりです。

    [DNS サーバー IP（DNS Server IPs）]：DNS サーバーの IP アドレス（v4/v6）のカンマ区切りリストを指定します。

    [DNS サーバー VRF（DNS Server VRFs）]：すべての DNS サーバーに 1 つの VRF を指定するか、DNS サーバーごとに 1 つの VRF を指定します。

    [NTP サーバー IP（NTP Server IPs）]：NTP サーバーの IP アドレス（v4/v6）のカンマ区切りリストを指定します。

    [NTP サーバー VRF（NTP Server VRFs）]：すべての NTP サーバーに 1 つの VRF を指定するか、NTP サーバーごとに 1 つの VRF を指定します。

    [Syslog サーバー IP（Syslog Server IPs）]：syslog サーバーの IP アドレスのカンマ区切りリスト（v4/v6）を指定します（使用する場合）。

    [Syslog サーバーの重大度（Syslog Server Severity）]：syslog サーバーごとに 1 つの syslog 重大度値のカンマ区切りリストを指定します。最小値は 0 で、最大値は 7 です。高いシビラティ（重大度）を指定するには、大きい数値を入力します。

    [Syslog サーバー VRF（Syslog Server VRFs）]：すべての syslog サーバーに 1 つの VRF を指定するか、syslog サーバーごとに 1 つの VRF を指定します。

    [AAA フリーフォームの設定（AAA Freeform Config）：AAA フリーフォームの設定を指定します。

    ファブリック設定で AAA 設定が指定されている場合は、**switch_freeform** PTI で、ソースが **UNDERLAY_AAA** で説明が **AAA Configurations** であるものが作成されます。

11. **[ブートストラップ（Bootstrap）]** タブをクリックします。

    このタブのフィールドは次のとおりです。

    [ブートストラップの有効化（Enable Bootstrap）]：ブートストラップ機能を有効にします。ブートストラップを使用すると、新しいデバイスを day-0 段階で簡単にインポートし、既存のファブリックに組み込むことができます。ブートストラップは NX-OS POAP 機能を活用します。

    ブートストラップを有効にした後、次のいずれかの方法を使用して、DHCP サーバーで IP アドレスの自動割り当てを有効にできます。

    - [外部 DHCP サーバー（External DHCP Server）]：**[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]** および **[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** フィールドに外部 DHCP サーバーに関する情報を入力します。
    - [ローカル DHCP サーバー（Local DHCP Server）]：**[ローカル DHCP サーバー（Local DHCP Server）]** チェックボックスをオンにして、残りの必須フィールドに詳細を入力します。

      [ローカル DHCP サーバの有効化（Enable Local DHCP Server）]：ローカル DHCP サーバを介した自動 IP アドレス割り当ての有効化を開始するには、このチェックボックスをオンにします。このチェックボックスをオンにすると、**[DHCP スコープ開始アドレス（DHCP Scope Start Address）]** および **[DHCP スコープ終了アドレス（DHCP Scope End Address）]** フィールドが編集可能になります。

      このチェックボックスをオンにしない場合、Nexus ダッシュボード ファブリック コントローラは自動 IP アドレス割り当てにリモートまたは外部DHCPサーバを使用します。

      [DHCP バージョン（DHCP Version）]：このドロップダウンリストから [DHCPv4] または [DHCPv6] を選択します。[DHCPv4] を選択すると、**[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]** フィールドは無効になります。DHCPv6 を選択すると、**[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** フィールドは無効になります。

      > ヒント：Cisco Nexus 9000 および 3000 シリーズ スイッチは、スイッチが L2 隣接（eth1 またはアウトオブバンド サブネットは /64 が必須）、またはスイッチがいくつかの IPv6 /64 サブネット内に存在する L3 隣接である場合にのみ、IPv6 POAP をサポートします。/64 以外のサブネット プレフィックスはサポートされていません。

      [DHCP スコープ開始アドレス（DHCP Scope Start Address）]：スイッチのアウトオブバンド POAP に使用する IP アドレス範囲の最初の IP アドレスを指定します。

      [DHCP スコープ終了アドレス（DHCP Scope End Address）]：スイッチのアウトオブバンド POAP に使用する IP アドレス範囲の最後の IP アドレスを指定します。

      [スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]：スイッチの管理 VRF のデフォルト ゲートウェイを指定します。

      [スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]：スイッチの Mgmt0 インターフェイスのプレフィックスを指定します。プレフィックスは 8 ～ 30

の間である必要があります。

DHCP 範囲および管理デフォルト ゲートウェイ IP アドレスの仕様（DHCP scope and management default gateway IP address specification）：管理デフォルト ゲートウェイ IP アドレスを 10.0.1.1 に、サブネット マスクを 24 に指定した場合、DHCP 範囲が指定したサブネット、10.0.1.2 ～ 10.0.1.254 の範囲内であることを確認してください。

[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]：スイッチの Mgmt0 インターフェイスの IPv6 プレフィックスを指定します。プレフィックスは 64 ～ 126 の間である必要があります。このフィールドは DHCP の IPv6 が有効な場合に編集できます。

DHCP 用です。

[AAA設定の有効化（Enable AAA Config）]：
デバイスの起動構成ポスト ブートストラップの一部としての **[管理性（Manageability）]** タブ。

[ブートストラップ フリーフォームの設定（Bootstrap Freeform Config）]：（オプション）必要に応じて追加のコマンドを入力します。たとえば、デバイスにプッシュするいくつかの追加の設定が必要であり、ポスト デバイス ブートストラップが使用可能である場合、このフィールドでキャプチャして要求のとおりに保存することが可能です。デバイスの起動後、**[ブートストラップ フリーフォームの構成（Bootstrap Freeform Config）]** フィールド**で定義された構成を含めることができます。**

running-config をコピーして **[フリーフォーム構成（freeform config）]** フィールドに、NX-OS スイッチの実行設定と同様の、正しいインデントでコピーアンドペーストします。freeform config は running-config と一致する必要があります。*スイッチでのフリーフォーム構成エラーの解決方法については*、ファブリック スイッチでのフリーフォーム構成の有効化を参照してください。

[DHCPv4/DHCPv6 マルチ サブネット スコープ（DHCPv4/DHCPv6 Multi Subnet Scope）]：フィールドで 1 行に 1 つのサブネット スコープを入力するように指定します。**[ローカル DHCP サーバーの有効化（Enable Local DHCP Server）]** チェックボックスをオンにすると、このフィールドは編集可能になります。

範囲のフォーマットは次のように定義される必要があります：

[DHCP スコープ開始アドレス、DHCP スコープ終了アドレス、スイッチ管理デフォルト ゲートウェイ、スイッチ管理サブネット プレフィックス（DHCP Scope Start Address, DHCP Scope End Address, Switch Management Default Gateway, Switch Management Subnet Prefix）]

たとえば、16.0.0.2, 10.6.0.9, 10.6.0.1, 24 です。

12. **[保存（Save）]** をクリックします。

IPFM Easy ファブリックが作成され、**[LAN ファブリック（Lan Fabrics）]** ウィンドウのテーブルに表示されます。

次に行う作業：

ファブリックの作成後、[構成の再計算（Recalculate Config）] を実行し、スイッチに構成を行ってください。詳細については、 LAN 動作モード設定のファブリックの概要の「ファブリックの概要」セクションを参照してください。

その後必要に応じて、インターフェイスを編集または作成してください。詳細については、 IPFM ファブリック向けインターフェイスの構成を参照してください。

認証キーの取得

3DES 暗号化 OSPF 認証キーの取得

1. スイッチに SSH 接続します。
2. 未使用のスイッチインターフェイスで、次を有効にします。

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

この例では、**ospfAuth** は暗号化されていないパスワードです。

このステップ 2 は、新しいキーを設定する場合に必要です。

3. パスワードを取得するには、**show run interface Ethernet1/1** コマンドを入力します。

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

md5 3 の後の文字のシーケンスは、暗号化されたパスワードです。

4. **[OSPF 認証キー（OSPF Authentication Key）]** フィールドの暗号化されたパスワードを更新します。

暗号化された IS-IS 認証キーの取得

キーを取得するには、スイッチにアクセスできる必要があります。

1. スイッチに SSH 接続します。
2. 一時キーチェーンを作成します。

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

この例では、**isisAuth** はプレーンテキスト パスワードです。これは、CLI が受け入れられた後に Cisco タイプ 7 パスワードに変換されます。

3. パスワードを取得するには、**show run | section "key chain"** コマンドを入力します。

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

key-string 7 の後の文字のシーケンスは、暗号化されたパスワードです。保存します。

4. [OSPF 認証キー（OSPF Authentication Key）] フィールドの暗号化されたパスワードを更新します。
5. ステップ 2 で行った不要な設定を削除します。

3DES 暗号化 BGP 認証キーの取得

1. スイッチに SSH 接続し、存在しないネイバーの BGP 構成を有効にします。

ヒント：	存在しないネイバー構成は、一時的な BGP パスワードを取得するためのネイバー構成です。

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

この例では、**bgpAuth** は暗号化されていないパスワードです。

2. パスワードを取得するには、show run bgp コマンドを入力します。サンプル出力：

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

パスワード 3 の後の文字のシーケンスは、暗号化されたパスワードです。

3. **[BGP 認証キー（BGP Authentication Key）]** フィールドの暗号化されたパスワードを更新します。
4. BGP ネイバー設定を削除します。

暗号化された BFD 認証キーの取得

1. スイッチに SSH 接続します。
2. 未使用のスイッチインターフェイスで、次を有効にします。

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

この例では、**cisco123** は暗号化されていないパスワードで、キー ID は **100** です。

このステップ 2 は、新しいキーを設定する場合に必要です。

3. キーを取得するには、**show running-config interface** コマンドを入力します。

```
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
```

BFD キー ID は **100** で、暗号化キーは **636973636F313233** です。

4. **[BFD 認証キー（BFD Authentication Key ID）]** フィールドと **[BFD 認証キー（BFD Authentication Key）]** フィールドのキー ID とキーを更新します。
フィールド。

IPFM ファブリックの編集

[LAN ファブリック（LAN Fabrics）] ウィンドウで、編集するファブリックを選択します。**[アクション（Actions）]** ドロップダウン リストから、**[ファブリックの編集（Edit Fabric）]** を選択します。必要に応じてテンプレートのフィールドを編集します[保存（Save）] をクリックします。

ヒント：	ファブリックの設定を変更したら、[構成の再計算（Recalculate Config）] を実行し、構成をスイッチに展開します。

IPFM ファブリックの削除

[LAN ファブリック（LAN Fabrics）] ウィンドウで、削除するファブリックを選択します。**[アクション（Actions）]** ドロップダウン リストから、**[ファブリックの削除（Delete Fabric）]** を選択します。ファブリックを削除するかどうかを確認するメッセージが表示されたら、**[確認（Confirm）]** をクリックします。

IPFM ファブリックのインターフェイス構成

Cisco Nexus Dashboard Fabric Controller Web UI では、ファブリック内の各スイッチに IPFM 外部リンクを設定できます。外部デバイスは、IPFM External-Link としてマーキングすることで、このインターフェイスを介してネットワークに接続できます。

ヒント：	Nexus Dashboard Fabric Controller のネットワーク オペレータ ロールを持つユーザーは、インターフェイス設定を保存、展開、展開解除、または編集できません。

NDFC リリース 12.0.1a 以降、IPFM ファブリックのインターフェイスは Nexus ダッシュボード ファブリック コントローラ インターフェイス マネージャによって管理されます。IPFM のデフォルトのインターフェイス ポリシーは **int_ipfm_l3_port** です。

インターフェイスが NBM 外部リンクおよびユニキャスト BW 設定で有効になった後に NBM VRF が NDFC から削除されると、次の問題が発生します。これが発生すると、影響を受けるインターフェイスは引き続き外部リンクと ucast BW を設定どおりに表示します。クリーンアップするには、次の手順を実行します。

1. **[ポリシー（Policies）]** タブで **[ポリシーの追加（Add Policy）]** を使用して、これらのインターフェイスの問題があるすべてのスイッチを選択します。
2. **host_port_resync** テンプレートを選択し、**[保存（Save）]** をクリックします。
3. **[再計算してデプロイ（Recalculate & Deploy）]** を選択します。これにより、スイッチ構成が NDFC と同期されます。
4. **[すべて再同期（Resync All）]** を選択します。

IPFM ファブリックの非ファブリック イーサネット インターフェイス ポリシー テンプレートは、**int_ipfm_l3_port**、**int_ipfm_access_host**、および **int_ipfm_trunk_host** です。

IPFM ファブリックのポート チャネル インター フェイス ポリシー テンプレートは、**int_ipfm_port_channel_access_host**、**int_ipfm_port_channel_trunk_host**、**int_ipfm_port_channel_access_member**、および **int_ipfm_port_channel_trunk_member** です。

IPFM ファブリックのスイッチ仮想インターフェイス（SVI）テンプレートは **int_ipfm_vlan** です。

IPFM ファブリックのインターフェイスの作成

ここでは、使用可能な IPFM ファブリック インターフェイス テンプレートから選択したテンプレートに基づいて、IPFM ファブリックの新しいインターフェイスを作成する手順について説明します。

IPFM ファブリックは V6 アンダーレイをサポートしません。

1. ファブリックの **[ファブリックの概要（Fabric Overview）]** ウィンドウに移動し、**[インターフェイス（Interfaces）]** タブをクリックします。
2. **[アクション（Actions）]** ドロップダウン リストから **[新しいインターフェイスの作成（Create new interface）]** を選択します。

[新しいインターフェイス（New Interfaces）] ウィンドウが表示されます。

3. IPFM のインターフェイス タイプとして、[ポートチャネル（Port Channel）]、[ループバック（Loopback）]、または [SVI] を選択します。
4. ドロップダウン リストからデバイスを選択します。ファブリックの一部であるスイッチ（スパインおよびリーフ）がドロップダウン リストに表示されます。
5. インターフェイス タイプの選択に基づいて、[ポートチャネル ID（Port Channel ID）]、[ループバック ID（Loopback ID）,または [VLAN ID] を入力します。
6. **[ポリシー未選択（No Policy Selected）]** リンクをクリックして、IPFM に固有のポリシーを選択します。**[アタッチするポリシーの選択（Select Attached Policy Template）]** ダイアログ ボックスで、必要なインターフェイス ポリシー テンプレートを選択し、**[保存（Save）]** をクリックします。
7. **[ポリシー オプション（Policy Options）]** 領域に適切な値を入力します。ポリシーに基づいて、それに応じた [ポリシーオプション（Policy Options）] フィールドが表示されることに注意してください。

   ◦ **[タイプ：ポートチャネル（Type - Port Channel）]**

   [ポートチャネル メンバー インターフェイス（Port Channel Member Interfaces）]：メンバー インターフェイスのリストを指定します（例：e1/5、eth1/7-9）。

   [ポートチャネル モード（Port Channel Mode）]：次のチャネル モード オプションとして、[オン（on）]、[アクティブ（active）]、または [パッシブ（passive）] のいずれかを選択します。

   [BPDU ガードの有効化（Enable BPDU Guard）]：スパニングツリー ブリッジ プロトコル データ ユニット（BPDU）ガードのオプションとして、次のいずれかを選択します。

   - true：bdpuguard を有効にします
   - false：bpduguard を無効にします
   - no：デフォルト設定に戻します。

   [ポート タイプ高速の有効化（Enable Port Type Fast）]：このチェックボックスをオンにすると、スパニングツリー エッジ ポートの動作が有効になります。

[MTU]：ポートチャネルまたはインターフェイスの最大伝送ユニット（MTU）を指定します。インターフェースでの MTU の有効な値の範囲は 576 ～ 9216 です。

[速度（SPEED）]：ポートチャネルの速度またはインターフェイスの速度を指定します。

[アクセス VLAN（Access Vlan）]：アクセス ポートの VLAN を指定します。

[トランク許可された VLAN（Trunk Allowed Vlans）]：次のいずれかの値を入力します。

- なし
- all
- VLANの範囲（1～200、500～2000、3000 など）

[PTP の有効化（Enable PTP）]：IPFM ファブリックのホスト インターフェイスの高精度時間プロトコル（Precision Time Protocol、PTP）を有効にします。詳細については、IPFM ファブリックの PTP 構成を参照してください。

[PTPプロファイル（PTP Profile）]：**ドロップダウン リストから PTP プロファイルとして [IEEE-1588v2]、[SMPTE-2059-2]**、または **[AES67-2015]** のいずれかを選択します。

[PTP VLAN（PTP Vlan）]：PTP が有効な場合のメンバー インターフェイスの PTP VLAN を指定します。

[ポートチャネルの説明（Port Channel Description）]：ポートチャネル

の説明を入力します。**[フリーフォームの設定（Freeform Config）]**：必要

に応じて、ポートチャネルの追加 CLI を入力します。**[ポートチャネルの有**

効化（Enable Port Channel）]：ポートチャネルを有効にするには、このチ

ェックボックスをオンにします。

- **[タイプ：ループバック（Type - Loopback）]**

[インターフェイス VRF（Interface VRF）]：インターフェイス VRF の名前を入力します。デフォルトの VRF の場合は **default** と入力します。

[ループバック IP（Loopback IP）]：ループバック インターフェイスの IPv4 アドレスを入力します。

[ループバック IPv6 アドレス（Loopback IPv6 address）]：VRFがデフォルト以外の場合、ループバック インターフェイスの IPv6 アドレスを入力します。デフォルトVRFの場合は、フリーフォームで IPv6 アドレスを追加します。

[ルートマップ タグ（Route-Map TAG）]：インターフェイス IP に関連付けられたルートマップ タグを入力します。

[インターフェイスの説明 (Interface Description)]：インターフェイスの説明を入力します。説明は最大 254 文字です。

[フリーフォームの設定（Freeform Config）]：必要に応じて、ループバック インターフェイスの追加 CLI を入力します。

[インターフェイスの有効化（Enable Interface）]：インターフェイスを有効にするには、このチェックボックスをオンにします。

- **[タイプ：SVI（Type - SVI）**

  [インターフェイス VRF（Interface VRF）]：インターフェイス VRF の名前を入力します。デフォルトの VRF の場合は **default** と入力します。

  [VLAN インターフェイス IP（VLAN Interface IP）]：VLAN インターフェイスの IP アドレスを入力します。

  [IP ネットマスク長（IP Netmask Length）]：IP アドレスで使用される IP ネットマスク長を指定します。有効な値の範囲は 1 ～ 31 です。

  [ルーティング TAG（Routing TAG）]：インターフェイス IP に関連付けられたルーティング タグを入力します。

  [MTU]：ポートチャネルまたはインターフェイスの最大伝送ユニット（MTU）を指定します。インターフェースでの MTU の有効な値の範囲は 576 ～ 9216 です。

[IP リダイレクトの無効化（Disable IP redirects）]：インターフェイスで IPv4 と IPv6 の両方のリダイレクトを無効にします。

[IPFM 外部リンク (IPFM External-Link)]：インターフェイスを外部ルーターに接続することを指定するには、このチェックボックスをオンにします。

[インターフェイスの説明 (Interface Description)]：インターフェイスの説明を入力します。説明は最大 254 文字です。

[フリーフォームの設定（Freeform Config）]：必要に応じて、VLAN インターフェイスの追加 CLI を入力します。

[インターフェイス管理状態（Interface Admin State）]：インターフェイスの管理状態を有効にするには、このチェックボックスをオンにします。

要件に基づいて、次のいずれかのボタンをクリックします。

- [保存 (Save)]：設定の変更を保存するには、**[保存 (Save)]** をクリックします。
- [プレビュー (Preview)]：**[プレビュー (Preview)]** をクリックすると、**[インターフェイス設定のプレビュー (Preview interfaces configuration)]** ウィンドウが開いて、詳細が表示されます。
- [展開 (Deploy)]：インターフェイスを設定するには、**[展開 (Deploy)]** をクリックします。

次に行う作業：

インターフェイスを編集する場合は、IPFM ファブリックのインターフェイスの編集を参照してください。

インターフェイスの準備ができたら、IPFM ファブリックを設定するためのポリシーを追加します。詳細については、IPFM ファブリックを構成するポリシーの追加を参照してください。

IPFM ファブリックのサブインターフェイスの作成

このセクションでは、IPFM ファブリックの新しいサブインターフェイスを作成する手順について説明します。

1. ファブリックの **[ファブリックの概要（Fabric Overview）]** ウィンドウに移動し、**[インターフェイス（Interfaces）]** タブをクリックします。
2. デバイスのリストからリーフまたはスパイン スイッチを選択し、**[アクション（Actions）] > [サブインターフェイスの作成（Create Subinterface）]** の順に選択します。

   [サブインターフェイスの作成（Create Subinterface）] ウィンドウが表示されます。
3. **[ポリシー未選択（No Policy Selected）]** リンクをクリックして、IPFM に固有のポリシーを選択します。
4. **[アタッチするポリシーの選択（Select Attached Policy Template）]** ダイアログ ボックスで、**int_ipfm_subif** ポリシー テンプレートを選択し、**[保存（Save）]** をクリックします。
5. **[ポリシー オプション（Policy Options）]** 領域に適切な値を入力します。ポリシーに基づいて、それに応じた [ポリシーオプション（Policy Options）] フィールドが表示されることに注意してください。

   - **[タイプ：ポートチャネル（Type - Port Channel）]**

     [ポートチャネル メンバー インターフェイス（Port Channel Member Interfaces）]：メ

ンバー インターフェイスのリストを指定します（例：e1/5、eth1/7-9）。

[ポートチャネル モード（Port Channel Mode）]：次のチャネル モード オプションとして、[オン（on）]、[アクティブ（active）]、または [パッシブ（passive）] のいずれかを選択します。

[BPDU ガードの有効化（Enable BPDU Guard）]：スパニングツリー ブリッジ プロトコル データ ユニット（BPDU）ガードのオプションとして、次のいずれかを選択します。

- true：bdpuguard を有効にします
- false：bpduguard を無効にします
- no：デフォルト設定に戻します。

[ポート タイプ高速の有効化（Enable Port Type Fast）]：このチェックボックスをオンにすると、スパニングツリー エッジ ポートの動作が有効になります。

[MTU]：ポートチャネルまたはインターフェイスの最大伝送ユニット（MTU）を指定します。インターフェースでの MTU の有効な値の範囲は 576 ～ 9216 です。

[速度（SPEED）]：ポートチャネルの速度またはインターフェイスの速度を指定します。

[アクセス VLAN（Access Vlan）]：アクセス ポートの VLAN を指定します。

[トランク許可された VLAN（Trunk Allowed Vlans）]：次のいずれかの値を入力します。

- なし
- all
- VLANの範囲（1～200、500～2000、3000 など）

[PTP の有効化（Enable PTP）]：IPFM ファブリックのホスト インターフェイスの高精度時間プロトコル（Precision Time Protocol、PTP）を有効にします。詳細については、IPFM ファブリックの PTP 構成を参照してください。

[PTPプロファイル（PTP Profile）]：**ドロップダウン リストから PTP プロファイルとして [IEEE-1588v2]、[SMPTE-2059-2]**、または **[AES67-2015]** のいずれかを選択します。

[PTP VLAN（PTP Vlan）]：PTP が有効な場合のメンバー インターフェイスの PTP VLAN を指定します。

[ポートチャネルの説明（Port Channel Description）]：ポートチャネル

の説明を入力します。**[フリーフォームの設定（Freeform Config）]**：必要

に応じて、ポートチャネルの追加 CLI を入力します。**[ポートチャネルの有**

効化（Enable Port Channel）]：ポートチャネルを有効にするには、このチ

ェックボックスをオンにします。

- **[タイプ：ループバック（Type - Loopback）]**

[インターフェイス VRF（Interface VRF）]：インターフェイス VRF の名前を入力します。デフォルトの VRF の場合は **default** と入力します。

[ループバック IP（Loopback IP）]：ループバック インターフェイスの IPv4 アドレスを入力します。

[ループバック IPv6 アドレス（Loopback IPv6 address）]：VRFがデフォルト以外の場合、ループバック インターフェイスの IPv6 アドレスを入力します。デフォルトVRFの場合は、フリーフォームで IPv6 アドレスを追加します。

[ルートマップ タグ（Route-Map TAG）]：インターフェイス IP に関連付けられたルートマップ タグを入力します。

[インターフェイスの説明 (Interface Description)]：インターフェイスの説明を入力します。説明は最大 254 文字です。

[フリーフォームの設定（Freeform Config）]：必要に応じて、ループバック インターフェイスの追加 CLI を入力します。

[インターフェイスの有効化（Enable Interface）]：インターフェイスを有効にするには、このチェックボックスをオンにします。

- **[タイプ：SVI（Type - SVI）**

  [インターフェイス VRF（Interface VRF）]：インターフェイス VRF の名前を入力します。デフォルトの VRF の場合は **default** と入力します。

  [VLAN インターフェイス IP（VLAN Interface IP）]：VLAN インターフェイスの IP アドレスを入力します。

  [IP ネットマスク長（IP Netmask Length）]：IP アドレスで使用される IP ネットマスク長を指定します。有効な値の範囲は 1 ～ 31 です。

  [ルーティング TAG（Routing TAG）]：インターフェイス IP に関連付けられたルーティング タグを入力します。

  [MTU]：ポートチャネルまたはインターフェイスの最大伝送ユニット（MTU）を指定します。インターフェースでの MTU の有効な値の範囲は 576 ～ 9216 です。

  [IP リダイレクトの無効化（Disable IP redirects）]：インターフェイスで IPv4 と IPv6 の両方のリダイレクトを無効にします。

[IPFM 外部リンク (IPFM External-Link)]：インターフェイスを外部ルーターに接続することを指定するには、このチェックボックスをオンにします。

[インターフェイスの説明 (Interface Description)]：インターフェイスの説明を入力します。説明は最大 254 文字です。

[フリーフォームの設定（Freeform Config）]：必要に応じて、VLAN インターフェイスの追加 CLI を入力します。

[インターフェイス管理状態（Interface Admin State）]：インターフェイスの管理状態を有効にするには、このチェックボックスをオンにします。

要件に基づいて、次のいずれかのボタンをクリックします。

- [保存 (Save)]：設定の変更を保存するには、**[保存 (Save)]** をクリックします。
- [プレビュー (Preview)]：**[プレビュー (Preview)]** をクリックすると、**[インターフェイス設定のプレビュー (Preview interfaces configuration)]** ウィンドウが開いて、詳細が表示されます。
- [展開 (Deploy)]：インターフェイスを設定するには、**[展開 (Deploy)]** をクリックします。

次に行う作業：

インターフェイスを編集する場合は、IPFM ファブリックのインターフェイスの編集を参照してください。

インターフェイスの準備ができたら、IPFM ファブリックを設定するためのポリシーを追加します。詳細については、IPFM ファブリックを構成するポリシーの追加を参照してください。

IPFM ファブリックの PTP 構成

Precision Time Protocol（PTP）は、コンピュータ ネットワーク全体でクロックを同期するために使用されるプロトコルです。インターフェイスの作成時に **[PTP の有効化（Enable PTP）]** チェックボックスをオンにすると、PTP はファブリック全体およびすべてのファブリック内インターフェイスで有効になります。IPFM ファブリックでサポートされる PTP プロファイルは、**IEEE-1588v2、SMPTE-2059-2、および AES67-2015 です**。

非ファブリック イーサネット インターフェイスのインターフェイスごとの PTP プロファイルについては、次の点に注意してください。

- 各非ファブリック イーサネット インターフェイスで PTP を有効化し、PTP プロファイルを選択する必要があります。
- PTP プロファイルは、ファブリック レベルのものとは異なる場合があります。
- 非ファブリック イーサネット インターフェイスで PTP を設定するには、ファブリック設定で PTP を有効にする必要があります。

ファブリック設定で PTP が無効になっている場合、PTP 設定はすべてのインターフェイス（ファブリック インターフェイスと非ファブリック インターフェイスの両方）から削除されます。

IPFM ファブリックの PTP モニタリングの詳細については、LAN 動作モード設定のスイッチの概要についての「PTP（モニタリング）」の項を参照してください。

IPFM ファブリック インターフェイスの編集

ここでは、既存の IPFM ファブリック インターフェイスのテンプレートを編集する手順について説明します。**[ポリシーオプション (Policy Options)]** 領域では、テンプレートを変更することや、編集可能なパラメータの値を編集することが

できます。

1. ファブリックの **[ファブリックの概要（Fabric Overview）]** ウィンドウに移動し、**[インターフェイス（Interfaces）]** タブをクリックします。
2. **[アクション (Actions)]** ドロップダウン リストから **[インターフェイスの編集 (Edit interface)]** を選択します。

   [インターフェイスの編集 (Edit interface)] ウィンドウが表示されます。

3. この手順は任意です。ポリシーを変更するには、ポリシー リンクをクリックし、IPFM に固有のポリシーを選択します。

   [アタッチするポリシーの選択 (Select Attached Policy Template)] ダイアログ ボックスで、必要なインターフェイス ポリシー テンプレートを選択し、**[保存 (Save)]** をクリックします。

4. **[ポリシーオプション (Policy Options)]** 領域で必要な値を編集します。ポリシーに基づいて、それに応じた [ポリシーオプション (Policy Options)] フィールドが表示されることに注意してください。パラメータの詳細については、IPFM ファブリックのインターフェイスの作成を参照してください。

   次のフィールドは int_ipfm_l3_port ポリシーに固有であることに注意してください。

   [IPFM ユニキャスト帯域幅パーセンテージ (IPFM Unicast Bandwidth Percentage)]：ユニキャスト トラフィック専用の帯域幅の割合を指定します。残りのパーセンテージは、マルチキャスト トラフィック用に自動的に予約されます。このフィールドを空白のままにすると、グローバル ユニキャストの帯域幅予約が適用されます。

   [IPFM 外部リンク (IPFM External-Link)]：インターフェイスを外部ルーターに接続することを指定するには、このチェックボックスをオンにします。

   [境界ルーター (Border Router)]：このチェックボックスをオンにすると、インターフェイスで境界ルーターの設定が有効になります。インターフェイスは PIM ドメインの境界です。

   [インターフェイスの説明 (Interface Description)]：インターフェイスの説明を入力します。説明は最大 254 文字です。

5. 要件に基づいて、次のいずれかのボタンをクリックします。
   - [保存 (Save)]：設定の変更を保存するには、**[保存 (Save)]** をクリックします。
   - [プレビュー (Preview)]：**[プレビュー (Preview)]** をクリックすると、**[インターフェイス構成のプレビュー (Preview interfaces configuration)]** ウィンドウが開いて、詳細が表示されます。
   - [展開 (Deploy)]：インターフェイスを設定するには、**[展開 (Deploy)]** をクリックします。

次に行う作業：

IPFM ファブリックを設定するためのポリシーを追加します。詳細については、 IPFM ファブリックを構成するポリシーの追加を参照してください。

IPFM ファブリックを構成するポリシーの追加

すべてのリーフまたはスパインで均一ではない設定の場合、IPFM ファブリックの設定を完了するのに役立つ追加のテンプレートが提供されます。

たとえば、9300 スイッチで NAT を有効にすると、**ipfm_tcam_nat_9300** ポリシーを作成して、スイッチに必要な NAT TCAM を設定できます。

テレメトリには ipfm_telemetry ポリシーを使用し、VRF 設定（routing、pim、asm）には ipfm_vrf ポリシーを使用します。

1. 使用するファブリックの **[ファブリックの概要（Fabric Overview）]** ウィンドウに移動し、**[ポリシー（Policies）]** タブをクリックします。
2. **[アクション（Actions）]** ドロップダウンリストから **[ポリシーの追加（Add Policy）]** を選択します。

   [ポリシーの作成（Create Policy）] ウィンドウを表示します。

3. **[スイッチの選択（Select Switches）]** フィールドの右矢印をクリックします。

   [スイッチの選択（Select Switches）] ダイアログボックスが表示されます。

4. 1 つ以上のスイッチを選択し、**[選択（Select）]** をクリックします。
5. **[ポリシーの作成（Create Policy）]** ウィンドウで **[テンプレートの選択（Choose Template）]** をクリックします。
6. [ポリシー テンプレートの選択（Select a Policy Template）] ダイアログ ボックスで、IPFM ファブリックに必要なテンプレート（ipfm_tcam_nat_9300 など）を選択します。[選択（Select）] をクリックします。
7. テンプレートの優先順位を入力します。有効な値の範囲は、1 ～ 1000 です。
8. TCAM 関連のフィールドに値を入力します。TCAM サイズを 256 単位で入力し、[保存（Save）] をクリックします。

IPFM ファブリックのポリシーの編集

IPFM ファブリック内の任意のスイッチのポリシーを編集できます。

1. 使用するファブリックの **[ファブリックの概要（Fabric Overview）]** ウィンドウに移動し、**[ポリシー（Policies）]** タブをクリックします。
2. テンプレートを検索します。
3. [アクション（Actions）] ドロップダウンリストからポリシーを選択し、[ポリシーの編集（Edit Policy）] を選択します。

   [ポリシーの編集（Edit Policy）] ウィンドウが表示されます。

4. 必要な変更を行って、**[保存（Save）]** をクリックします。

著作権

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

シスコおよびシスコのロゴは、シスコまたはその関連会社の米国およびその他の国における
商標または登録商標です。シスコの商標の一覧については、http://www.cisco.com/go/ trademarks を参照してください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。（1110R）。