メディア用 Cisco Nexus 9000 シリーズ NX-OS IP ファブリック ソリューション ガイド、リリース 10.6(x)

最終更新：2026 年 2 月 3 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに

この前書きは、次の項で構成されています。

対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

表記法

コマンドの説明では、次の表記法を使用しています。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y | z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の `screen` フォント	ユーザが入力しなければならない情報は、太字のスクリーンフォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコ（<>）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、 へご連絡ください。ご協力をよろしくお願いいたします。

通信、サービス、およびその他の情報

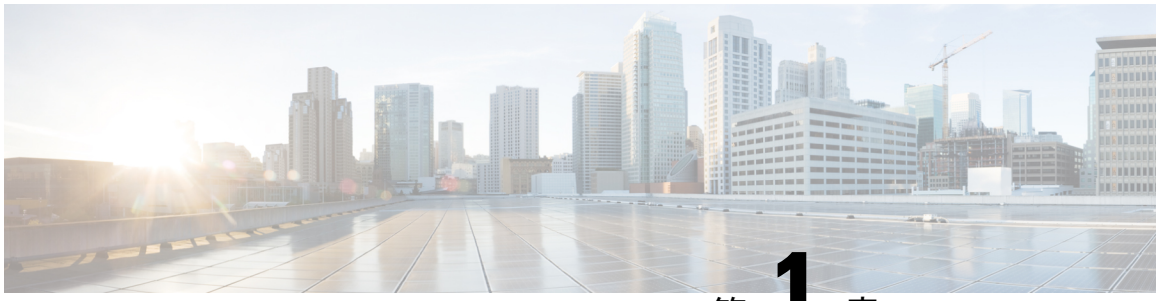
- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。

- 重要な技術によって求めるビジネス成果を得るには、Cisco Services [英語] にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

Cisco Bug Search Tool（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

はじめに



第 1 章

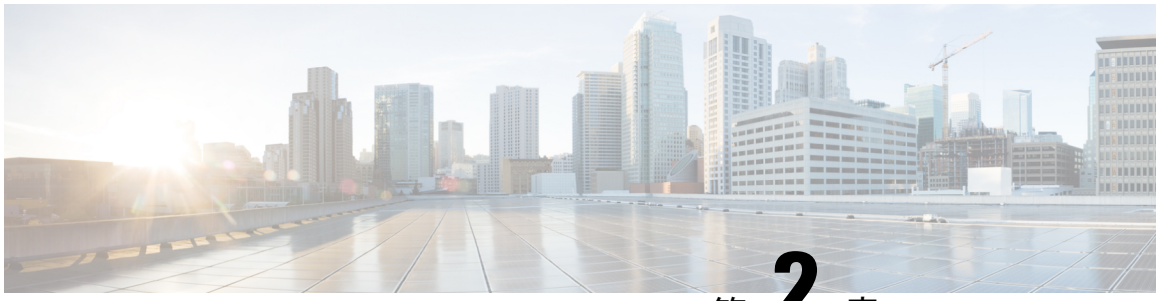
新機能と更新情報

新機能および変更情報

表 *1* : 新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
拡張された障害と通知のペイロード構造	新しい障害カテゴリとペイロード構造による高度なフロー分析により、トラフィック フローの正確なトラブルシューティングと最適化を実現。	10.6(1)F	IPFM クリティカル イベントの拡張ペイロード （9 ページ） 拡張された障害と通知のペイロード構造 （11 ページ）

新機能および変更情報



第 2 章

Cisco のメディア ソリューション向け IP ファブリックの概要

この章には、メディア ソリューション向けのシスコの IP ファブリックに関する情報が含まれています。

ライセンス要件

Cisco NX-OS を動作させるには、機能とプラットフォームの要件に従って適切なライセンスを取得し、インストールする必要があります。

- 基本（Essential）ライセンスとアドオンライセンスが、さまざまな機能セットに使用できます。
- ライセンスは、製品および購入オプションに応じて、永続的、一時的、または評価用のものがあります。
- 高度な機能を使用するには、基本ライセンス以外の追加の機能ライセンスが必要です。
- 高度な機能を使用するには、基本ライセンス以外の追加ライセンスが必要です。
- ライセンスの適用と管理は、デバイスのコマンドライン インターフェイス（CLI）を介して行われます。

ライセンスのタイプとインストール手順の詳細については、『*Cisco NX-OS* ライセンシング ガイド』および『*Cisco NX-OS* ライセンシング オプション ガイド』を参照してください。

サポートされるプラットフォーム

Nexus スイッチ プラットフォーム サポート マトリックスには、次のものがリストされています。

- サポートされている Cisco Nexus 9000 および 3000 スイッチ モデル
- NX- OS ソフトウェア リリース バージョン

プラットフォームと機能の完全なマッピングについては、『Nexus スイッチプラットフォーム サポート マトリックス』を参照してください。

メディア ソリューション向け IP ファブリックの概要

現在、放送業界では、シリアル デジタル インターフェイス (SDI) ルータと SDI ケーブルを使用してビデオと音声のトラフィックを転送しています。SDI ケーブルは、単一の単方向信号のみを伝送できます。その結果、多くのケーブルが必要になり、多くの場合、長距離にわたって引き伸ばされ、SDI ベースのインフラストラクチャを拡張または変更することが難しくなり、時間がかかります。

メディア ソリューション向けのシスコの IP ファブリックは、SDI ルータから IP ベースのインフラストラクチャへの移行を支援します。IP ベースのインフラストラクチャでは、1 本のケーブルで複数の双方向トラフィック フローを伝送でき、物理インフラストラクチャを変更することなく、さまざまなフロー サイズをサポートできます。

メディア ソリューションの IP ファブリックは、柔軟なスパインおよびリーフ アーキテクチャまたは単一のモジュラ スイッチ トポロジで構成されます。このソリューションでは、Cisco Nexus 9000 シリーズ スイッチを IP Fabric for Media アルゴリズム（インテリジェント トラフィック管理アルゴリズム）とともに使用し、Nexus ダッシュボード ファブリック コントローラ（NDFC） の有無にかかわらず使用します。オープン API を使用して、Cisco Nexus Dashboard Fabric Controller （NDFC） はさまざまなブロードキャスト コントローラと統合できます。このソリューションは、信頼性が高く (ゼロ ドロップ マルチキャスト)、視認性が高く、安全性が高く、可用性の高いネットワークを提供します。

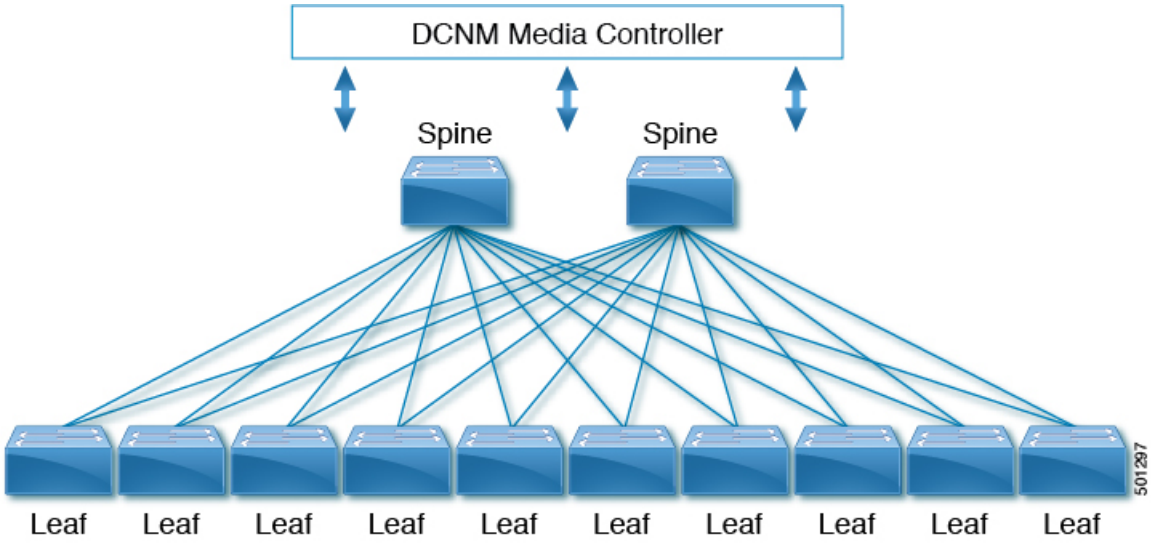
導入タイプ

メディア ソリューション向けのシスコの IP ファブリックは、次のタイプの展開をサポートしています。

- スパイン リーフ トポロジ-IP スタジオで一般的に見られる大規模な展開向けの柔軟なアーキテクチャ。
- シングル モジュラー スイッチ — フローの可視性、セキュリティ、監視などの機能を提供するコントローラーを備えた、固定展開に適したアーキテクチャ。

スパインリーフ トポロジ

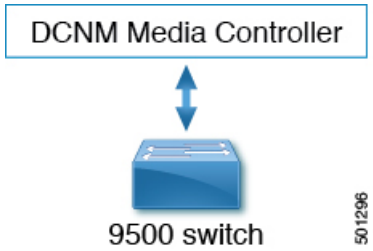
シスコのメディア ソリューション向け IP ファブリックは、複数のスパインおよびリーフ スイッチで構成されるスパインリーフ トポロジをサポートします。トポロジは、1 種類のリーフ スイッチの使用を含め、リーフ スイッチの任意の組み合わせをサポートします。



メディア ソースとレシーバはリーフ スイッチに接続し、レシーバーはメディア トラフィックを受信するためにリーフ スイッチへの IGMP 参加要求を開始します。

単一のモジュラ スイッチ トポロジ

メディア ソリューション向けのシスコの IP ファブリックは、1 つの Cisco Nexus 9500 シリーズ スイッチで構成される単一のモジュラ スイッチ トポロジをサポートします。



メディア ソリューション コンポーネントの IP ファブリック

Cisco Nexus 9000 シリーズ スイッチ

次の Cisco Nexus 9000 シリーズ スイッチは、IP ファブリックを介してビデオおよび音声トラフィックを転送するために使用されます。

Cisco Nexus 9000 シリーズ スイッチ	ポートの数とサイズ	トポロジにおける役割*
Cisco Nexus 9336C-FX2 スイッチ	36 x 40/100-Gbps ポート	スパインリーフ トポロジのスパインまたはリーフ
Cisco Nexus 9348GC-FXP スイッチ	48 x 100-Mbps/1-Gbps ポート	スパインリーフ トポロジのリーフ
Cisco Nexus 93108TC-FX スイッチ	48 x 10-Gbps ポート	スパインリーフ トポロジのリーフ
Cisco Nexus 93180YC-FX スイッチ	48 x 10/25-Gbps ポート	スパインリーフ トポロジのリーフ
Cisco Nexus 93216TC-FX2 スイッチ	96 x 1/10-Gbps ポート	スパインリーフ トポロジのリーフ
Cisco Nexus 93240YC-FX2 スイッチ	48 x 10/25-Gbps ポート	スパインリーフ トポロジのリーフ
Cisco Nexus 93360YC-FX2 スイッチ	96 x 10/25-Gbps ポート	スパインリーフ トポロジのリーフ
以下のライン カードを搭載した Cisco Nexus 9504 および 9508 スイッチ • N9K-X9636C-R • N9K-X9636C-RX • N9K-X9636Q-R （注） N9K-X96136YC-R ライン カードはサポートされていません。	36 x 40/100 Gbps ポート（N9K-X9636C-R ライン カード用） 36 x 40/100 Gbps ポート（N9K-X9636C-RX ライン カード用） 36 x 40 Gbps ポート（N9K-X9636Q-R ライン カード用）	スパイン リーフ トポロジのスパインまたは単一のモジュラ スイッチのスパイン

Cisco Nexus 9000 シリーズ スイッチ	ポートの数とサイズ	トポロジにおける役割*
Cisco Nexus 9316D-GX スイッチ	400/100 Gbps QSFP-DD ポート x 16	スパインリーフ トポロジのリーフ
Cisco Nexus 9364C-GX スイッチ	64 x 100/40-Gbps Quad Small Form-Factor Pluggable（QSFP28）ポート	スパインリーフ トポロジのリーフ
Cisco Nexus 93600CD-GX スイッチ	100/40 Gbps Quad Small Form-Factor Pluggable（QSFP28）ポート x 28、400/100 Gbps QSFP-DD ポート x 8	スパインリーフ トポロジのリーフ
Cisco Nexus 93180YC-FX3S スイッチ	48 個の 25/50/100 ギガビット イーサネット SFP28 ポート（ポート 1 ～ 48）および 6 個の 10/25/40/50/100 ギガビット QSFP28 ポート（ポート 49 ～ 54）	スパインリーフ トポロジのリーフ
Cisco Nexus 93180YC-FX3	1/10/25 Gbps ファイバ ポート x 48、40/100 Gbps QSFP28 ポート x 6	スパインリーフ トポロジのリーフ
Cisco Nexus 93108TC-FX3P	100M/1/2.5/5/10 Gbps BASE-T ポート x 48 40/100 Gbps Quad Small Form-Factor Pluggable 28（QSFP28）ポート x 6	スパインリーフ トポロジのリーフ
Cisco Nexus 9348GC-FX3	10M/100M/1 Gbps BASE-T ポート X 48 10/25 Gbps SFP28 ポート X 4 40/100 Gbps Quad Small Form-Factor Pluggable 28（QSFP28）ポート X 2	スパインリーフ トポロジのリーフ
N9K-X9624D-R2 ライン カード	24 個の 400G QSFP-DD ポートを備えたラインカード（8 スロット シャーシでのみ使用）	スパインリーフ トポロジのスパインまたはリーフ
Cisco Nexus 9508-FM-R2 ライン カード	400G ライン カード用ファブリック モジュール（8 スロット シャーシでのみ使用）	スパインリーフ トポロジのスパインまたはリーフ

Cisco Nexus 9000 シリーズ スイッチ	ポートの数とサイズ	トポロジにおける役割*
Cisco Nexus 9364D-GX2A スイッチ	40/100/400G QSFP-DD ポート X 64 1/10G SFP+ ポート X 2	スパインリーフ トポロジのスパインまたはリーフ スイッチ
Cisco Nexus 9348D-GX2A スイッチ	40/100/400G QSFP-DD ポート X 48 1/10G SFP+ ポート X 2	スパインリーフ トポロジのスパインまたはリーフ スイッチ
Cisco Nexus 9332D-GX2B スイッチ	40/100/400G QSFP-DD ポート X 32 1/10G SFP+ ポート X 2	スパインリーフ トポロジのスパインまたはリーフ スイッチ
次のライン カードを搭載した Cisco Nexus 9808 スイッチ： Cisco Nexus X9836DM-A Cisco Nexus 9808-FM-A	40/100/400G QSFP-DD ポート X36（8スロットのシャーシでのみ使用） Nexus 9808 用ファブリック モジュール	スパイン リーフ トポロジのスパインまたは単一のモジュラ スイッチのスパイン
Cisco Nexus 9332D-H2R	32 ポート 400G QSFP-DD ポート	スパインリーフ トポロジのリーフ
Cisco Nexus 9364C-HX スイッチ	64 x 40/100-Gbps QSFP28 ポート	スパインリーフ トポロジのスパインまたはリーフ
Cisco Nexus 93400LD-GX2A スイッチ	32 x 400-Gbps ポートおよび 16 x 100-Gbps QSFP-DD/QSFP28 ポート	スパインリーフ トポロジのスパインまたはリーフ
Cisco Nexus 9804 スイッチ	4スロットモジュラ型シャーシ（ポートと機能はラインカードによって異なります）	スパインリーフ トポロジのスパインまたはリーフまたは単一のモジュラ スイッチ
Cisco Nexus 9408 スイッチ	8スロットモジュラ型シャーシ（ポートと機能はラインカードによって異なります）	スパインリーフ トポロジのスパインまたはリーフまたは単一のモジュラ スイッチ
Cisco Nexus 9364C-GX スイッチ	100/40 Gbps QSFP28 ポート x 64	スパインリーフ トポロジのリーフ
Cisco Nexus 9336C-SE1 スイッチ	36 x 40/100-Gbps QSFP28 ポート	スパインリーフ トポロジのスパインまたはリーフ

*役割は、各スイッチがサポートするポート速度を考慮して、最も意味のあるファブリック内の場所を示します。スイッチが使用できる役割自体に制限はありません。

NDFC と IPFM

オープン API を通じて、Nexus Dashboard Fabric Controller （NDFC）とメディア対応 IP ファブリック（IPFM） は、ブロードキャスト コントローラとシームレスに統合し、IP ベースのインフラストラクチャのすべてのメリットとともに、同様のオペレータ ワークフローを提供します。NDFC with IPFM 機能は、メディア ネットワーク用に設計された定義済みテンプレートを使用して IP ファブリックを設定できる直感的な GUI を備えています。

NDFC と IPFM を使用すると、次のことが行えます。

- 個々のホストにセキュアな汎用ポリシーまたはマルチキャスト固有のポリシーを設定し、その役割に基づいてホストを許可または拒否します。
- 複数のホストおよびフローに対してセキュアなマルチキャスト固有のポリシーを構成します。
- トラフィック フローと帯域幅使用率を表示して、ファブリック内の問題領域 (リンク障害やオーバーサブスクリプションなど) を特定します。
- フロー分析を使用して、ビット レートを測定および保存し、個々のトラフィック フローの詳細を表示します。
- ファブリックで実行されたアクションの監査ログを表示します。

IPFM クリティカル イベントの拡張ペイロード

Cisco NX-OSリリース 10.6(1)F 以降、拡張機能により、より詳細でユーザー フレンドリな障害および通知情報が提供され、ネットワークの可視性と運用上のインサイトを向上させることができます。これにより、ネットワークの問題をより迅速に識別して解決できます。主要な改善点は次のとおりです。

- 障害の理由と解決策を明確化します。
- キー情報が、以前は識別名（DN）に埋め込まれていましたが、ペイロードに個別の属性として含まれるようになりました。この属性が含まれます：
  - **source**：送信元 IP アドレス
  - **group:** マルチキャスト グループ IP アドレス
  - **faultCode**： 障害を識別するコード。
  - **vrf**：仮想ルーティングおよび転送（VRF）インスタンス。

  この変更によって、DN を解析してこれらの値を抽出する必要がなくなり、より直接的な情報へのアクセス方法が提供されます。
- ネットワーク管理およびモニタリング インターフェイスでのスイッチの重要なイベントの表示の改善。

新しい障害カテゴリとペイロード構造を備えたフロー分析の機能拡張により、ネットワークの動作に関するより詳細で実用的ビューが提供されます。これにより、より正確なトラブルシューティングとトラフィックフローの最適化が可能になります。

- 新しい障害カテゴリでは、障害状態をより具体的に分類できます。これにより、管理者は問題の原因と性質を迅速に特定できます。
- 拡張ペイロードの faultReason 属性と faultResolution 属性は、障害の明確な説明とそれを解決するための具体的な手順を提供します。
- 新しい通知カテゴリでは、ネットワーク イベントに関するより詳細な情報が提供されます。これにより、管理者は潜在的な問題をプロアクティブに特定し、パフォーマンスに影響が出る前にトラフィック フローを最適化できます。
- 新しい通知カテゴリでは、ネットワーク イベントに関するより詳細な情報が提供されます。これにより、管理者は潜在的な問題をプロアクティブに特定し、トラフィック フローを最適化するための適切なアクションを実行できます。

（注） Cisco NX-OSリリース 10.6(1)F 以降、レガシーの障害および通知出力は廃止。サブスクライバと統合は、すべての障害および通知の管理対象オブジェクト（MO）の拡張された名前と値の属性ペアを提供する、拡張された JSON ペイロード構造を使用する必要があります。自動統合またはモニタリング ツールが適宜更新されていることを確認します。

ペイロード構造：新旧の比較

次の例では、フロー障害のペイロード構造に対する変更が強調表示されています：

拡張前	拡張後

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

拡張された障害と通知のペイロード構造

Cisco NX-OSリリース 10.6(1)F 以降、新しい障害カテゴリとNotification（通告）カテゴリにより、ネットワークのトラブルシューティングと最適化のためのより明確で有用な情報が提供されます。次のセクションでは、新しい障害および通知管理対象オブジェクト（MO）と、それらの拡張ペイロード構造の例について詳しく説明します。

障害 MO

拡張された障害管理対象オブジェクト（MO）は、さまざまなネットワークの問題に関する詳細で分類された情報を提供し、より正確なトラブルシューティングと迅速な解決を可能にします。これらのMOは、さまざまなタイプの障害に関する詳細な情報を提供するように設計されています。障害 MO は次のとおりです。

- フロー エラー

  帯域幅不足やポリサー リソースの枯渇など、特定のマルチキャスト フローに関連する問題を示します。

- 送信者エラー

ポリシーの拒否や接続の問題など、送信元デバイスまたはエンドポイントに起因する問題を報告します。

- レシーバーの障害

  フローの配信を妨げる帯域幅の不十分や設定の問題など、受信者に影響を与える状態を強調表示します。

- PIM パッシブ入力障害

  VRF コンテキストまたはインターフェイスの構成ミスなど、フローの入力（着信）インターフェイスに関連する障害を特定します。

- PIM パッシブ出力障害

  無効なインターフェイス IP や VRF の不一致など、フローの出力（発信）インターフェイスの障害に関連します。

通知 MO

新しい通知管理対象オブジェクト（MO）は、ネットワークイベントと動作状態に関するきめ細かい情報を提供するため、管理者が潜在的な問題をプロアクティブに特定し、パフォーマンスに影響を与える前にトラフィック フローを最適化するのに役立ちます。通知 MO は次のとおりです：

- インターフェイス レベルの使用 MO：

  入力インターフェイスと出力インターフェイスの帯域幅使用率に関する通知を提供し、インターフェイス使用状況の正常性をモニタリングします。

  - 出力イベント

    出力インターフェイスの帯域幅使用量がクリティカルしきい値に達したか、超えた場合に通知します。

  - 入力イベント

    入力インターフェイスの帯域幅使用量がクリティカルしきい値に達したか、超えた場合に通知します。

- フローレートのイベント MO

  フローのレートが構成済みのしきい値を下回った場合、または上回った場合を示します。

- フローでプロビジョニングされた MO

  新しいフローがネットワークで正常にプロビジョニングされたときに確認します。

- NAT イベント MO:

  NAT 固有の帯域幅または変換状態の問題に関連するイベントを提供します。

  - オーバーサブスクリプション イベント

NAT 前の帯域幅の使用量の累積が NAT 後の帯域幅容量を超えた場合にアラートを発行します。

- 帯域幅不一致イベント

  プレ NAT フロー帯域幅とポスト NAT フロー帯域幅の間に不一致がある場合に信号で通知されます。

フロー障害

nbmFlowFaults 管理対象オブジェクトは、帯域幅やポリサーの問題など、特定のフローに関連する障害に関する情報を提供します。

```
"nbmFlowFaults": {

    "attributes": {

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

        "faultCode": "2076",

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

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

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

         "group": "233.1.4.255",

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

        "source": "47.20.20.9",

        "tStamp": "1743518104080",

         "vrf": "default"

}
```

次の表に、フロー障害コード、その理由、および推奨される解決策を示します。

障害コード	障害の理由（Fault Reason）	障害解決
3051	送信者が使用できる帯域幅がありません	帯域幅の構成を確認し、必要に応じて変更してください。
3201	リモートでフロー拒否	参加しているアップストリーム スイッチを再確認してください。
3202	リモートで拒否されたフロー（外部リンク）	参加しているアップストリーム スイッチを再確認してください。

障害コード	障害の理由（Fault Reason）	障害解決
3376	帯域幅の競合により、優先順位の高いフローの影響を受けます	きめ細かいフロー優先順位設定の影響
3126	送信者は到達不能です	送信者 IP のユニキャスト ルーティング テーブルを確認してください
3176	PIM が有効化されていない	PIMを構成してください
3151	PIM/ IGMP ホストプロキシが有効になっていません	PIM/ IGMP ホストプロキシを設定してください
3152	PIM/ IGMP ホストプロキシが有効になっていません（外部リンク）	PIM/ IGMP ホストプロキシを設定してください

送信者エラー

nbmSenderFaults 管理対象オブジェクトは、ホストポリシーの拒否やリソース制限など、メディア送信者から発生した障害に関する情報を提供します。

```
"nbmSenderFaults": {

    "attributes": {

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


       "faultCode": "2001",

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

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

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


         "group": "227.10.10.1",

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

          "senderEndpoint": "47.20.20.9",

          "tStamp": "1743517513635",

          "vrf": "default"

}
```

次の表に、送信者障害コード、その理由、および送信者障害タイプに推奨される解決策のリストを示します。

障害コード	障害の理由（Fault Reason）	障害解決
2001	送信者ホスト ポリシーによる拒否	送信者ホスト ポリシーの構成を確認し、必要に応じて変更します
2002	送信者ホスト ポリシーによる拒否（外部リンク）	送信者ホスト ポリシーの構成を確認し、必要に応じて変更します
2051	送信者が使用できる帯域幅がありません	帯域幅の構成を確認し、必要に応じて変更してください。
2052	送信者が使用できる帯域幅がありません（外部リンク）	帯域幅の構成を確認し、必要に応じて変更してください。
2076	ポリサー リソースがすべて消費されました。構成された TCAM の最大値に達しました	必要に応じて TCAM 構成を確認します。
2077	ポリサー リソースがすべて消費され（外部リンク）、設定されたTCAM最大値に達しました	必要に応じて TCAM 構成を確認します。
2377	ポリサーが使用できないため、優先順位の高いフローの影響を受けます	きめ細かいフロー優先順位設定の影響
2101	一致するポリシーが見つかりません	このグループのフローポリシーと帯域幅を定義してください
2151	PIM/ IGMP ホストプロキシが有効になっていません	PIM/ IGMP ホストプロキシを設定してください
2152	PIM/ IGMP ホストプロキシが有効になっていません（外部リンク）	PIM/ IGMP ホストプロキシを設定してください
2351	ing-nbm リージョンに TCAM が割り当てられていません	TCAM 構成を再確認してください
2352	外部入力インターフェイスの ing-nbm リージョンに TCAM が割り当てられていません	TCAM 構成を再確認してください

レシーバーの障害

nbmReceiverFaults 管理対象オブジェクトは、帯域幅制限や接続の問題など、メディア受信者に関連する障害に関する情報を提供します。


```
"nbmReceiverFaults": {

     "attributes": {

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


          "faultCode": "1026",

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


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

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


          "group": "227.10.10.1",

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

          "receiverEndpoint": "47.20.10.1",

          "receiverInterface": "Ethernet1/47.1",

          "source": "47.20.20.9",

          "tStamp": "1743517666801",

          "vrf": "default"

}
```


次の表に、受信者障害コード、その理由、および受信者障害タイプに推奨される解決策のリストを示します。

障害コード	障害の理由（Fault Reason）	障害解決
1026	現在レシーバーで使用できる帯域幅がありません	レシーバーをスティッチングする必要がある場合は、フロー ポリシーを確認してください

PIM パッシブ入力障害

nbmFlowIngressFaults 管理対象オブジェクトは、 VRF コンテキストの問題や無効なインターフェイス構成など、メディア フローの入力インターフェイスに関連する障害に関する情報を提供します。


```
"nbmFlowIngressFaults": {
                "attributes": {
```

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

                "faultCode": "4230",
              "faultDn": "sys/nbm/conf/flows/dom-default/s-[47.20.20.9]-g-[230.1.0.1]",

                "faultReason": "IIF is not part of valid VRF context",
               "faultResolution": "Update VRF context on IIF if needed, then delete and
 re-add DN in fault",
                "group": "230.1.0.1",
                "ingressif": "null0_iif",
                "modTs": "2025-04-01T15:07:15.248+00:00",
                "source": "47.20.20.9",
                "tStamp": "1743520035248",
                "vrf": "default"
                }
```


次の表に、PIM パッシブ入力の障害コード、その原因、および PIM パッシブ入力の障害タイプに推奨される解決策のリストを示します。

障害コード	障害の理由（Fault Reason）	障害解決
4226	IIF の無効なインターフェイス IP	インターフェイスの IP アドレスを構成してから、 RPF を未指定に設定して検証します
4230	IIF が有効な VRF コンテキストの一部ではありません	必要に応じて IIF で VRF コンテキストを更新し、その後障害が発生した DN を削除して再度追加します
4251	入力インターフェイスの VRF コンテキストがシャットダウンされました	VRF コンテキストを有効にしてから、障害が発生した DN を削除して再度追加します
4276	入力インターフェイスの mroute clear コマンドが開始されました	障害が発生した DN を削除て再度追加します
4076	ポリサー リソースがすべて消費されました構成された TCAM の最大値に達しました	必要に応じて TCAM 構成を確認します
4228	インターフェイスIP（IIF）の VRFコンテキストが変更されました	必要に応じてインターフェイスの VRF 設定を元に戻してから、障害のある DN を削除して再度追加します
4232	RPF に PIM/IGMP ホストプロキシ設定がありません	インターフェイスでPIM/IGMP ホストプロキシを設定した後、障害が発生したDNを削除して再度追加してください

PIM パッシブ出力障害

nbmFlowEgressFaults 管理対象オブジェクトは、無効なインターフェイス IP アドレスや構成エラーなど、メディア フローの出力インターフェイスに関連する障害に関する情報を提供します。


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

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


次の表に、PIM パッシブ出力の障害コード、その原因、および PIM パッシブ出力の障害タイプに推奨される解決策のリストを示します。

障害コード	障害の理由（Fault Reason）	障害解決
4227	OIF の無効なインターフェイス IP	インターフェイスの IP アドレスを構成してから、障害が発生した DN を削除して再度追加する
4229	OIF が有効な VRF コンテキストの一部ではありません	必要に応じて OIF で VRF コンテキストを更新し、その後障害が発生した DN を削除して再度追加する
4231	出力インターフェイスに OIF-PIM 構成がない	インターフェイスで PIM を構成した後、障害が発生した DN を削除して再度追加する
4252	発信インターフェイスの VRF コンテキストがシャットダウンされています	VRF コンテキストを有効にしてから、障害が発生した DN を削除して再度追加します
4277	出力インターフェイスの mroute clear コマンドが開始されました	障害が発生した DN を削除して再度追加する

インターフェイスの使用率

出力イベント： nbmEgressEvent

nbmEgressEvent管理対象オブジェクトは、出力インターフェイスでの帯域幅使用率などのインターフェイス レベルの使用状況に関する情報を提供します。


```
"nbmEgressEvent": {

                "attributes": {

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

                "egressinterface": "Eth1/47.2",

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

                "notifyCode": "5301",

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

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

                "tStamp": "1743667956338",

                "vrf": "vrf_pmn1"

                }
```


次の表に、出力イベントタイプに対する通知コードとそれに対応する理由の一覧を示します。

通知コード	理由
5301	クリティカル：出力帯域幅使用率が 90 %以上です

入力イベント： nbmIngressEvent

nbmIngressEvent管理対象オブジェクトは、入力インターフェイスでの帯域幅使用率などのインターフェイス レベルの使用状況に関する情報を提供します。


```
"nbmIngressEvent": {

                "attributes": {

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

                "ingressinterface": "Eth1/42.1",

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

                "notifyCode": "5302",

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

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

                "tStamp": "1743668171366",
```

```
                "vrf": "vrf_pmn1"

                }
```

次の表に、入力イベント タイプに対する通知コードとそれに対応する理由のリストを示します。

通知コード	理由
5302	クリティカル：入力帯域幅使用率が 90 %以上です

フロー レートのイベント M0

nbmEvent

nbmEvent 管理対象オブジェクトは、フロー レートが構成されたしきい値を下回った場合やしきい値を超えた場合など、フロー レート イベントに関する情報を提供します。

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

次の表に、フロー レート イベント タイプに対する通知コードとそれに対応する理由の一覧を示します。

通知コード	理由
5303	レートが構成されているフロー ポリシーの 100% を超えています。
5304	レートが構成されているフロー ポリシーの 60% 未満です。

フロー プロビジョニングされたイベント

nbmFlowEvent

nbmFlowEvent 管理対象オブジェクトは、フローが正常にプロビジョニングされたときなどのフロー プロビジョニング イベントに関する情報を提供します。

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

                "egressinterface": "Lo1",
```

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


次の表に、フロープロビジョニングされたイベントのタイプに対する通知コードとそれに対応する理由の一覧を示します。

通知コード	理由
5201	正常にフロー プロビジョニングされました。

NAT イベント

オーバーサブスクリプション イベント

nbmInatOversubscriptionEvent 管理対象オブジェクトは、 NAT前の累積帯域幅がNAT後の帯域幅を超えた場合などのNATオーバーサブスクリプション イベントに関する情報を提供します。


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

                "group": "226.1.1.1",
                "modTs": "2025-04-01T14:19:04.393+00:00",
                "notifyCode": "5305",
              "notifyDn": "vrf:default-post_s-[51.51.51.51]-post_g-[226.1.1.1]-ingress",

               "reason": "Oversubscription: cumulative pre-NAT bandwidth is higher than
 post-NAT bandwidth from the respective flow policies",
                "source": "51.51.51.51",
                "tStamp": "1743517144393",
                "vrf": "default"
                }
                }
```


次の表に、NAT オーバーサブスクリプション イベント タイプの通知コードとそれに対応する理由のリストを示します。

通知コード	理由
5305	オーバーサブスクリプション：NAT 前の累積帯域幅が、それぞれのフローポリシーのNAT 後の帯域幅よりも大きい

帯域幅不一致イベント

nbmEnatBandwidthmismatchEvent 管理対象オブジェクトは、 NAT前のフロー帯域幅とNAT後のフロー帯域幅の間に不一致がある場合などの NAT 帯域幅不一致イベントに関する情報を提供します。

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

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

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


次の表に、 NAT 帯域幅不一致イベント タイプの通知コードとそれに対応する理由のリストを示します。

通知コード	理由
5307	変換前および変換後のフロー帯域幅の不一致

失敗のハンドリング（Failure Handling）

Cisco のメディア ソリューション向け IP ファブリックは、決定論的な障害処理をサポートしています。

リンクまたはスイッチの障害時に、十分な帯域幅が利用可能であれば、影響を受けるフローは代替リンクに移動されます。SMPTE 2022-7 では、エンドポイントに冗長性が構築されているため、リンクまたはスイッチの障害が本番トラフィックに影響を与えることはありません。

Cisco NX-OS リリース 10.6(1)F では、より詳細で実用的障害情報を提供する障害処理の拡張機能が導入されています。これにより、管理者は障害情報を効果的に理解し、障害の根本原因を特定し、好みのネットワーク管理ツールを使用して適切な修復手順を実装できます。

メディア ソリューション向け IP ファブリックの利点

メディア ソリューション向けのシスコの IP ファブリックには、次の利点があります。

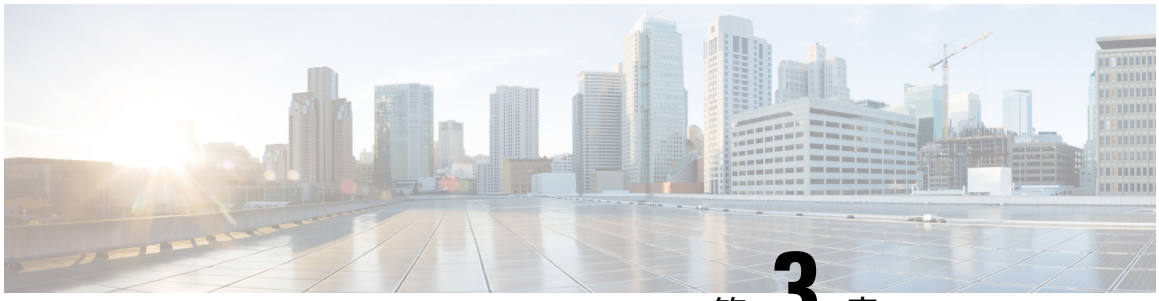
- 専用ハードウェア (SDI ルータ) を汎用スイッチング インフラストラクチャに置き換えます。
- 最大 100 Gbps のポート速度で、さまざまなタイプとサイズのブロードキャスト機器エンドポイントをサポートします。

- 4K および 8K ウルトラ HD を含む最新のビデオ テクノロジをサポートします。
- 水平にスケーリングします。より多くの容量が必要な場合は、リーフ スイッチを追加して、より多くのエンドポイントをサポートできます。
- パケット損失ゼロ、超低遅延、最小限のジッタを備えた確定的なネットワークを提供します。
- すべてのメディア ソースとレシーバを同期できます。
- リーフとスパインの間のリンクに障害が発生したときに、受信側にトラフィックを送信する決定論的な障害処理を提供します。
- ポストプロダクション作業のためのライブ トラフィック フローとファイル ベースのトラフィック フローの共存をサポートします。
- 向上したネットワーク セキュリティを提供します。
- リンクのオーバーサブスクリプションを防止するノンブロッキング ネットワーク設計を提供します。
- 既存のオペレータ ワークフローを変更する必要はありません。

関連資料

関連項目	マニュアル タイトル
Cisco NDFC	Cisco Nexus Dashboard Fabric Controller インストー プグレード ガイド Cisco DCNM オンライン ヘルプ
Cisco Nexus Dashboard	Cisco Nexus Dashboard
Cisco NX-OS リリース情報	メディア リリース ノート向け Cisco Nexus 9000 シ IP ファブリック
Cisco NX-OS ソフトウェア アップグレード	『Cisco Nexus 9000 Series NX-OS Software Upgrad Guide』
IGMP スヌーピングと PIM	『Cisco Nexus 9000 Series NX-OS Multicast Routing Guide』
メディア スケーラビリティ数の IP ファブリック	『Cisco Nexus 9000 Series NX-OS Verified Scalabili
NX-API REST	Cisco Nexus 3000 and 9000 Series NX-API REST SDK API Reference （Cisco Nexus 3000 および 9000 シ REST SDK ユーザ ガイドと API リファレンス）

関連項目	マニュアル タイトル
OSPF	『Cisco Nexus 9000 シリーズ NX-OS ユニキャスト ル設定ガイド』
PTP	『Cisco Nexus 9000 Series NX-OS System Management Guide』
QoS	『Cisco Nexus 9000 Series NX-OS Quality of Service Co Guide』
TCAM カービング	『Cisco Nexus 9000 Series NX-OS Security Configuratio
VLANs	『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Co Guide』



第 3 章

メディア向け IP ファブリックの設定

この章では、メディア ネットワーク用の IP ファブリックを設定する方法について説明します。

IP ファブリックに必要なリーフ スイッチの数とタイプの決定

IP ファブリックに必要なリーフ スイッチの数とタイプは、ブロードキャスト センターのエンドポイントの数とタイプによって異なります。

必要なリーフ スイッチの数を判断するには、次の手順に従ってください。

1. ブロードキャスト センターのエンドポイント（カメラ、マイクなど）の数を数えます（たとえば、360 の 10 Gbps エンドポイントと 50 の 40 Gbps エンドポイント）。
2. ブロードキャスト センターのエンドポイントのタイプに基づいて、必要なリーフ スイッチのタイプを決定します。
   - 10 Gbps エンドポイントの場合、Cisco Nexus 93108TC-FX、93216TC-FX2、93180YC-FX リーフ スイッチを使用します。
   - 25 Gbps エンドポイントの場合、Cisco Nexus 93180YC-FX、93240YC-FX2、または 93360YC-FX2 リーフ スイッチを使用します。
   - 40 Gbps エンドポイントの場合、Cisco Nexus 9336C-FX2 リーフ スイッチを使用します。
   - 100 Gbps エンドポイントの場合、Cisco Nexus 9336C-FX2 リーフ スイッチを使用します。
3. 各リーフ スイッチがサポートするエンドポイントとアップリンクの数に基づいて、必要なリーフ スイッチの数を決定します。

（注） 次の表のアップリンクとダウンリンクの数は推奨値です。特定のポートをアップリンクまたはホスト側リンクとして使用するための技術的な制限はありません。

表 *2:* リーフ スイッチごとにサポートされるエンドポイントとアップリンク

リーフ スイッチ	エンドポイントキャパシティレポート	アップリンク容量
Cisco Nexus 9336C-FX2 スイッチ	25 x 40 Gbps エンドポイント	10 x 100 Gbps (1000 Gbps) アップリンク
Cisco Nexus 9348GC-FXP スイッチ	48 x 1 Gbps/100 Mbps エンドポイント	2 x 100 Gbps（200 Gbps）アップリンク
Cisco Nexus 93108TC-FX スイッチ	48 x 1/10 Gbps エンドポイント	6 x 100 Gbps（600 Gbps）アップリンク
Cisco Nexus 93180YC-FX スイッチ	48 x 10/25 Gbps エンドポイント	6 x 100 Gbps（600 Gbps）アップリンク
Cisco Nexus 93216TC-FX2 スイッチ	96 x 1/10 Gbps エンドポイント	12 x 40/100 Gbps (1200 Gbps) アップリンク
Cisco Nexus 93240YC-FX2 スイッチ	48 x 10 Gbps エンドポイント	12 x 100 Gbps（1200 Gbps）アップリンク
Cisco Nexus 93360YC-FX2 スイッチ	96 x 10/25-Gbps エンドポイント	12 x 40/100 Gbps (1200 Gbps) アップリンク

4. （スパイン スイッチに向かう）アップリンク帯域幅が（エンドポイントに向かう）ダウンストリーム帯域幅以上であることを確認してください。

   1. 次の式を使用して、アップリンク帯域幅を決定します。

      ```
      リーフ スイッチあたりのアップリンク容量 x リーフ スイッチの数 = アップリンク帯域幅
      ```

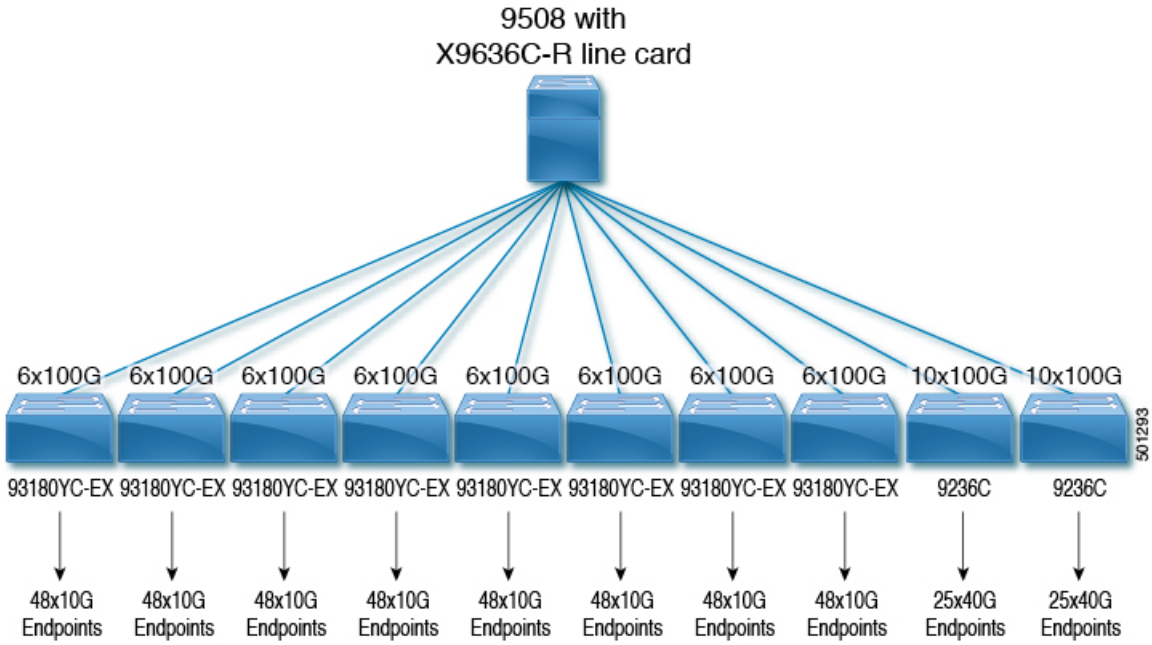
   2. 次の式を使用して、ダウンストリーム帯域幅を決定します。

      ```
      リーフ スイッチあたりのエンドポイント容量 x リーフ スイッチの数 = ダウンストリーム帯域幅
      ```

5. アップリンク帯域幅の合計がダウンストリーム帯域幅の合計以上である場合、トポロジは有効です。達成可能なフローの数を決定できるようになりました。アップリンク帯域幅がダウンストリーム帯域幅より小さい場合は、アップストリーム帯域幅がダウンストリーム帯域幅以上になるまでトポロジを修正します。

   PIM 双方向 RP 構成が利用可能な IPFM 帯域幅を利用するため、IPFM フローは予想される帯域幅をすべて利用することはできません。IPFM 帯域幅を増やすには、**PIM 双方向 RP** 構成を削除します。

次の図は、Cisco Nexus 9508 スパイン スイッチと N9K-X9636C-R ライン カードを使用したトポロジの例を示しています。



IP ファブリックで達成可能なフロー数を決定します。

次の式を使用して、IP ファブリックで可能なフローの数を決定します。

総帯域幅 ÷ フロー サイズ = 達成可能なフローの数

フロー サイズは設定可能であり、通常、ブロードキャスト センターで使用されるビデオ テクノロジーのタイプに基づいています。

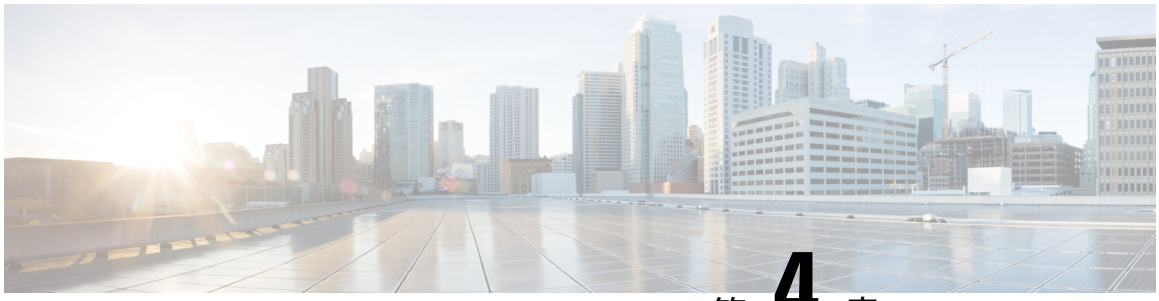
表 *3:* ビデオ テクノロジーあたりのフロー サイズ

テクノロジー	フロー サイズ
HD ビデオ	1.5 Gbps (1500 Mbps)
3G HD ビデオ	3Gbps（3000Mbps）
4K ウルトラ HD ビデオ	12 Gbps (12,000 Mbps)
8K ウルトラ HD ビデオ	48 Gbps (48,000 Mbps)

次に例を示します。

7200 Gbps の合計帯域幅 ÷ 1.5 Gbps フロー サイズ (HD ビデオの場合) = 4800 の可能なフロー

IP ファブリックで達成可能なフロー数を決定します。



第 4 章

メディア用の IP ファブリックの構成

この章では、メディア ソリューション用のシスコの IP ファブリックに Cisco Nexus 9000 シリーズ スイッチを設定する方法について説明します。

前提条件

メディア ソリューション向けのシスコの IP ファブリックには、次の前提条件があります。

（注） Cisco Nexus 9800 スイッチの場合、TCAM カービング構成は必要ありません。

- -R ライン カードを備えた Cisco Nexus 9504 および 9508 スイッチの場合、これらの TCAM カービング コマンドを次の順序で設定してから、スイッチをリロードします。

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

- 他のすべてのスイッチでは、これらの TCAM カービング コマンドを次の順序で設定してから、スイッチをリロードします。

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

- 互換性のある Cisco NX-OS および Nexus Dashboard Fabric Controller（NDFC）リリースをインストールします。NDFC のインストール手順については、ご使用の NDFC リリースの

『Cisco Nexus Dashboard Fabric Controller インストールおよびアップグレード ガイド』を参照してください。

互換性のあるリリースとサポートされているスイッチの詳細については、Nexus Dashboard Fabric Controller ソフトウェアおよびハードウェア互換性マトリックス（旧 DCNM）を参照してください。

注意事項と制約事項

メディア ソリューション向けの IP ファブリックには、次の注意事項と制約事項があります。

- リーフ スイッチの数は、使用されるアップリンクの数と、スパイン スイッチで使用可能なポートの数によって異なります。
- IPFM を有効にする前に、スイッチでアクティブなフローがないことを確認してください。アクティブなフローがある場合は、フローをオフにするか、IPFM を設定した後にスイッチをリロードします。
- エンドポイントへのレイヤ 3 ルーテッド ポートを使用することをお勧めします。
- レイヤ 2 ポートを介して接続された SVI およびエンドポイントを備えた -R ライン カードを使用する単一モジュラ スイッチ配置では、フローの最大数は 2000 です。
- -R ライン カードを備えた Cisco Nexus 9504 および 9508 スイッチの場合、IPFM には 6 つのファブリック モジュールが必要です。
- ノンブロッキング パフォーマンスを確保するには、各リーフ スイッチからのアップリンク帯域幅が、エンドポイントに提供される帯域幅以上である必要があります。
- 可能であれば、エンドポイントを異なるリーフ スイッチに分散させて、すべてのリーフ スイッチで送信元と受信者が均等に分散されるようにします。
- 可能であれば、障害に備えてアップリンクをオーバープロビジョニングすることをお勧めします。
- ベスト プラクティスとして、/30 マスクでエンドポイントに向かうレイヤ 3 ポートを使用します。1 つの IP アドレスをエンドポイントに割り当て、別の IP アドレスをスイッチ インターフェイスに割り当てます。
- このソリューションは、IGMPv2 および IGMPv3 の参加と、PIM Any Source Multicast（ASM）および PIM Source-Specific Multicast（SSM）をサポートします。複数の送信元が ASM 範囲内の同じマルチキャスト グループにトラフィックを送信している場合、ファブリックの帯域幅は 1 つのフローのみに対応します。オーバーサブスクリプションが発生する可能性があるため、複数の送信者が ASM 範囲内の同じマルチキャスト グループにトラフィックを送信しないように注意してください。SSM 範囲では、さまざまなソースが同じグループに送信でき、ファブリックの帯域幅はフローごとに考慮されます。
- 統計は、送信側が接続されているスイッチでのみ使用できます。

- IPFM は、拡張 ISSU ではサポートされていません。メディア セットアップの IP ファブリックで **noboot mode lxc** コマンドを使用しないでください。
- リソースを節約するために、**service-policy type qos** コマンドを使用するときは統計を無効にすることをお勧めします。
- メディア ソリューションの IP ファブリックは、外部リンク上の IGMP および PIM エンドポイントが帯域幅管理される受信側の帯域幅管理をサポートします。
- メディア ソリューションの IP ファブリックは、DSCP およびフロー帯域幅の動的フローポリシーの変更をサポートします。
- メディア プラットフォームでサポートされているすべての IP ファブリックにより、送信側または受信側のエンド ホストをスパインに接続できます。
- メディア ソリューションの IP ファブリックは、ファブリックごとに複数のボーダー リーフをサポートします。
- ユニキャスト帯域幅のパーセンテージを変更する場合は、新しい値を有効にするためにファブリック リンクをフラップする必要があります。
- IPFM 外部リンクとして構成できるのは、レイヤ 3 インターフェイスのみです。レイヤ 3 インターフェイスがスイッチ ポートに変更されると、IPFM 外部リンク構成が削除されます。
- レイヤ 3 インターフェイスを IPFM 外部リンクとして構成すると、インターフェイスがフラップします。
- RPF または OIF インターフェイスのいずれかが帯域幅の変更に対応できない場合、フローは破棄されます。次の IGMP または PIM 参加により、フロー スティッチングが開始されます。
- ファブリック内の既存のフローを持つグループのフロー ポリシー (帯域幅) を変更する場合は、既存のフローへの影響を軽減するために、次の順序で変更を行います。そうしないと、使用中のインターフェースで使用可能な帯域幅に応じて、オーバーサブスクリプションが発生する可能性があります。
  1. より低い帯域幅からより高い帯域幅への変更: 最初に既存のフローのすべてのラスト ホップ ルータでポリシーを変更し、次にすべてのスパイン スイッチで、次に残りのスイッチでポリシーを変更します。
  2. より高い帯域幅からより低い帯域幅への変更: 最初に既存のフローのすべてのファースト ホップ ルータでポリシーを変更し、次にすべてのスパイン スイッチで、次に残りのスイッチでポリシーを変更します。
- IPFM フロー ポリサーを無効にすると、統計は利用できません。
- 障害時に、IPFM フローの優先順位付け機能は、可能な場合、優先順位のフローを回復しようとします。設計上、IPFM フローの優先順位付けは、優先順位のフローに対応するために既に確立されているフローを停止しません。

- Cisco Nexus リリース 10.1(1) 以降、IPFM を使用した IPFM フローの優先順位付けは、Cisco Nexus 9300-FX3 プラットフォーム スイッチでサポートされています。
- Cisco NX-OS リリース 10.1 (2) 以降、IPFM は N9K-X9624D-R2 および N9K-C9508-FM-R2 プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.2(1q)F 以降、IPFM は N9K-C9332D-GX2B プラットフォーム スイッチでサポートされます。
- Cisco Nexus 9500 -R ライン カードの場合、IPFM パッシブ モードで構成されている場合、入力廃棄が増加しますが、これは予期されるものであり、影響はないと判断されています。
- Cisco NX-OS リリース 10.3(1)F 以降、IPFM 機能と VXLAN は、同じボックスで 2 つの異なる VRF で共存できます。
- Cisco NX-OS リリース 10.3(1)F 以降、次の IPFM 機能が Cisco Nexus 9808 プラットフォーム スイッチでサポートされています。
  - スパインおよびシングル ボックスのサポート（L3 フロント パネル ポートのみ、L2 ポート/SVI サポートなし）。
  - ホスト管理のためのフロー ポリシー/ホスト ポリシー。
  - フロー プロビジョニングの Pim-Active モードと Pim-Passive モード。
  - NDFC の有効化のために公開されたフロー/エンド ポイントの Oper MO 公開。
- Cisco NX-OS リリース 10.4(1)F 以降、この機能は、Cisco Nexus X98900CD-A ラインカードを搭載した Cisco Nexus 9808 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、この機能は、Cisco Nexus X98900CD-A ラインカードおよび X9836DM-A を搭載した Cisco Nexus 9804 スイッチでサポートされます。
- Cisco NX-OS リリース 10.3(2)F 以降、マルチキャスト サービス リフレクション（マルチキャスト NAT）は、Cisco Nexus 9300、9408、および 9800 プラットフォーム スイッチ、および -R ライン カードを搭載した Cisco Nexus 9504 および 9508 スイッチにおいて、IPFM モード pim-active および IPFM モード pim-passive の全ホストおよびファブリック ポートのサブインターフェイスに拡張されました。
- 親ポートとそれに対応するサブインターフェイスは、同じ IPFM pim-active または IPFM pim-passive モードの VRF の一部であることが期待されます。

  例：親ポートが PIM アクティブ モードの IPFM VRF の一部である場合、そのサブインターフェイスも同じ PIM アクティブ モードの VRF（異なる VRF コンテキストである可能性があります）にある必要があります。
- Cisco NX-OS リリース 10.3(2)F 以降、サブインターフェイス タイプは IPFM モード pim-active および IPFM モード pim-passive でサポートされるようになりました。

- レイヤ 3 ポートチャネルおよびポートチャネル サブインターフェイスは、 IPFMではサポートされていません。IPFMで使用できるのは、ルーティングされた物理レイヤ 3 インターフェイスのみです。
- Cisco NX-OS リリース 10.3(2)F 以降、IPFM モードの pim-active と IPFM モードの pim-passive を同じスイッチ上で共存させることができます。
- Cisco NX-OS リリース 10.4(1)F 以降、ISIS は IPFM でサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、IPFM は Cisco Nexus 9348GC-FX3 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(2)F 以降、IPFM は Cisco Nexus C93108TC-FX3 スイッチでサポートされます。
- Cisco NX-OS リリース 10.4(2)F 以降では、ホスト IP ではなくインターフェイス IP に基づいてエンドポイント MO がパブリッシュされます。SVI インターフェイスの受信者と frowMQ のreporterIP の場合、SVI 受信者はホスト IP ではなく インターフェイス IP を持つことになるからです。
- Cisco NX-OS リリース 10.4(2)F 以降では、 IPFM を使用して、既存の L3 ポート フローデータに加えて L2 ポート情報にアクセスできるようになり、フロー パスの可視性が向上しました。この機能は、次の TOR および EOR スイッチでサポートされています。
  - Cisco Nexus 9300-FX/FX2/FX3/H1 プラットフォーム スイッチ
  - Nexus 9300-GX/GX2 プラットフォーム スイッチ
  - Nexus X97160YC- EX、9700-FX/GX ライン カード
  - Nexus 9600-R/R2 ライン カード
- Cisco NX-OS リリース 10.5(2)F 以降、IPFM の詳細な優先順位ベースのフロー機能は、IPFM フローに 16 レベルのプライオリティを提供し、リンク帯域幅の制約が存在する場合に、プライオリティの低いフローよりも重要なフローを優先させることを可能にします。この機能では、必要に応じてフローの優先順位を制御、カスタマイズし、割り当てることができます。優先順位フロー機能は、新しいコマンドによって制御されます。ただし、優先順位フローは PIM パッシブ モードではサポートされません。

ホスト ポリシーの注意事項と制限事項

次の注意事項と制限事項はホスト ポリシーに適用されます。

- デフォルトのホスト ポリシーは自動的に設定され、デフォルトで許可されます。
- デフォルトでは、すべての外部受信者（PIM）および送信者ホスト ポリシーが外部リンクに適用されます。
- デフォルト ポリシーを更新する前に、カスタム IPFM ホスト ポリシーを削除します。

- すべての受信側ポリシーは、特定の (S、G) のインターフェイスごとです。ポリシーが特定の（S、G）のインターフェイスに適用されると、そのサブネット内のすべてのレポーターに適用されます。
- ホストポリシーはソフトウェアに実装され、ACLやルートマップなどの物理インターフェイスには適用されません。
- インターフェイスの動作アップおよびダウンイベントは、ホストポリシーがインターフェイスに適用されているかどうかを判断しません。
- IP アドレスが割り当てられた有効なインターフェイスには、サブネット IP アドレスに基づいて関連付けられたホスト ポリシーがあります。
- インターフェイスが稼働状態にある場合にのみ、インターフェイスの送信側と受信側のホスト ポリシーが調べられます。
- PIM およびローカル レシーバ ホスト ポリシーの場合、ソースまたはグループを定義する必要があり、0.0.0.0 (any) にすることはできません。受信者がすべてのグループにサブスクライブできるようにするには、次の例を使用します。

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

（注） ローカル レシーバー ホスト ポリシーのホスト IP アドレスにワイルドカード（0.0.0.0）を入力すると、ソース IP アドレスもワイルド カードになりますが、有効なグループが必要です。

- 同じホスト IP アドレスと同じマルチキャスト グループ プレフィックスを使用して送信側ホスト ポリシーを構成しているが、アクションが異なる場合、最新の設定は拒否されます。

```
nbm host-policy
sender
10 host 101.1.1.3 group 229.1.1.1/32 deny
20 host 101.1.1.3 group 229.1.1.1/32 permit ←This policy is rejected.
```

- 同じソース IP アドレスと同じマルチキャスト グループ プレフィックスを使用して外部受信者 (PIM) ホストポリシーを構成しますが、アクションが異なる場合、最新の設定は拒否されます。

```
nbm host-policy
pim
30 source 111.1.1.3 group 239.1.1.1/32 deny
40 source 111.1.1.3 group 239.1.1.1/32 permit ←This policy is rejected.
```

- 同じソース IP アドレスとマルチキャスト グループ プレフィックスを使用してローカル レシーバー ホスト ポリシーを設定し、異なるホスト IP アドレスと異なるアクションを使用して設定する場合、シーケンス番号が最も小さい（10）ポリシーが優先されます。最も小さいシーケンス番号（10）のポリシーを削除すると、次に小さいシーケンス番号（20）のポリシーがアクティブになります。

```
nbm host-policy
receiver
10 host 100.1.1.1 source 145.1.1.1 group 234.1.1.1/32 deny ←This policy takes
precedence.
20 host 100.1.1.2 source 145.1.1.1 group 234.1.1.1/32 permit
```

ユニキャスト PTP の注意事項と制約事項

ユニキャスト PTP には、次の注意事項および制約事項が適用されます。

- 固有の PTP ユニキャスト ソース アドレスを使用して、すべてのユニキャスト PTP インターフェイスを設定します。
- グローバル PTP ソースとユニキャスト インターフェイス PTP ソースは同じであってはなりません。
- ユニキャストとマルチキャストは、同じインターフェイスではサポートされていません。
- デフォルトの CoPP プロファイルを変更し、PTP の認定情報レート (CIR) を 280 kbps から 1024 kbps に増やすことをお勧めします。
- NX-OS スイッチ宛ての gRPC トラフィックは、デフォルト クラスの CoPP にヒットします。gRPC ドロップの可能性を制限するには、管理クラスの gRPC 構成ポートを使用してカスタム CoPP ポリシーを構成することをお勧めします。
- ユニキャスト PTP は、次のプラットフォームでのみサポートされています。
  - Cisco Nexus 9236C、9272Q、および 92160YC-X スイッチ
  - Cisco Nexus 93108TC-FX, 93180YC-FX、93216TC-FX2、93240YC-FX2、93360YC-FX2、9336C-FX2、9348GC-FXP、および 9364C プラットフォーム スイッチ
  - -R ライン カードを搭載した Cisco Nexus 9504 および 9508 スイッチ

Cisco NDFC の注意事項と制約事項

一般に、次の注意事項と制限事項が NDFC に適用されます。

- 冗長パスを確保することにより、コントローラへの接続が常にあることを確認してください。
- NDFC からプッシュされたポリシーを変更する場合、CLI コマンドを使用しないでください。NDFC を使用して変更を加えます。
- **[NDFC 管理（NDFC Administration）]** > **[NDFC サーバ（NDFC Server）]** > **[サーバ プロパティ（Server Properties）]** を使用して、メディア関連のサーバ プロパティの IP ファブリックを変更した場合は、NDFC を再起動する必要があります。インストール手順については、『Cisco Nexus Dashboard Fabric Controller のインストールおよびアップグレード ガイド』を参照してください。

- NDFC は、スイッチのテレメトリ機能を利用してメディア データの IP ファブリックをストリーミングし、ElasticSearch を使用して永続化します。デフォルトでは、NDFC は履歴データを最大 7 日間保存します。データ保持期間は、NDFC サーバ プロパティ **pmn.elasticsearch.history.days** を使用して調整できます。
- スイッチが NDFC にインポートされると、DCNM は、そのスイッチに設定されているすべてのホスト ポリシー、フロー ポリシー、WAN リンク、ASM 範囲、および予約済みユニキャスト帯域幅を削除します。また、ホスト ポリシーを許可にリセットし、フロー ポリシーを 0 Kbps にリセットし、予約済みユニキャスト帯域幅を 0% にリセットします。同じファブリック内の他のスイッチに、NDFC によって展開されたポリシーと構成がすでに存在する場合。NDFC は、同じポリシーと構成のセット (WAN リンク構成を除く) を新しくインポートされたスイッチに展開し、ファブリック内のすべてのスイッチのポリシーと構成が同期するようにします。
- NDFC は、スイッチの SNMP リロード トラップをリスンします。NDFC は、スイッチがリロードされたことを検出すると、そのスイッチに構成されているすべてのホスト ポリシー、フロー ポリシー、および WAN リンクを削除します。また、ホスト ポリシーを許可にリセットし、フロー ポリシーを 0 Kbps にリセットし、予約済みユニキャスト帯域幅を 0% にリセットし、そのスイッチに展開されたポリシーと設定を再展開します。
- スイッチのインポートおよびリロード中にスイッチの既存の構成をそのまま維持することを選択した場合は、NDFC サーバ プロパティ **pmn.deploy-on-import-reload.enabled** を **'false'** に構成し、NDFC を再起動して、変更を有効にすることができます。

次の注意事項と制限事項は、フロー設定に適用されます。

- API 呼び出しが失敗した場合、NDFC はブロードキャスト コントローラまたはユーザーに通知します。その場合、ブロードキャスト コントローラまたはユーザーは再試行する必要があります。
- 静的レシーバ API は、SVI ではサポートされていません。
- VM スナップショットはサポートされません。以前の NDFC スナップショットにロールバックすることはできません。

次の注意事項と制限事項は、フロー ポリシーに適用されます。

- ファブリックでフローがアクティブになる前に、デフォルトのポリシーを変更します。
- フローをポリシングせずに一定量のバーストに対応するために、フロー ビット レートより 5% 多いことを考慮します。たとえば、3G フローを 3.15 Gbps としてプロビジョニングします。
- フローポリシーは変更できますが、それらのポリシーを使用するフローは変更中に影響を受けます。

次の注意事項と制限事項は、ホスト ポリシーに適用されます。

- レシーバ ホスト ポリシーがレイヤ 2 ポートおよび SVI を介して接続されたホストに適用される場合、そのポリシーは、その VLAN 上のすべてのホストによって送信されるすべての加入に適用され、単一のレシーバには適用できません。
- デフォルトのホスト ポリシーは、カスタム ホスト ポリシーが定義されていない場合にのみ変更できます。デフォルト ポリシーを変更するには、すべてのカスタム ポリシーを展開解除してから削除する必要があります。
- NDFC は、ホスト ポリシーのマルチキャスト範囲をサポートします。デフォルトでは、NDFC ではネットマスクまたはプレフィックスを指定できませんが、ホスト ポリシーのシーケンス番号は自動的に生成されます。マルチキャスト範囲を指定し、ホストポリシーのシーケンス番号を手動で入力する場合は、NDFC サーバ プロパティ **pmn.hostpolicy.multicast-ranges.enabled** を **'true'** に設定して NDFC を再起動できます。

次の注意事項と制限事項は、ネットワークと NDFC 接続に適用されます。

- NDFC HA ペアは同じ VLAN 上にある必要があります。
- NDFC とスイッチ間の接続は、アウトオブバンド管理ポートまたはインバンド管理を使用して行うことができます。

NDFC Media Controller のライセンス要件

製品	ライセンス要件
Cisco NDFC	Cisco NDFC メディア コントローラには、Advanced Server NDFC ライ ル手順については、『Cisco Nexus Dashboard Fabric Controller のイン ガイド』を参照してください。

Cisco NX-OS 9.x リリースへのアップグレード

Cisco NX-OS 9.x リリースからのアップグレード

メディア展開用の IP ファブリックで Cisco NX-OS 9.x リリースからそれ以降の 9.x リリースにアップグレードするには、次の手順に従います。

手順

ステップ 1 **install all** コマンドを使用して、スイッチ ソフトウェアを新しい 9.x リリースにアップグレードします。

ステップ 2 IPFM の TCAM カービングを設定し、スイッチをリロードします。

ステップ 3 NDFC をアップグレードします。

Cisco NX-OS 7.x リリースからのアップグレード

メディア展開用の IP ファブリックで Cisco NX-OS 7.x リリースから 9.x リリースにアップグレードするには、次の手順に従います。

（注） -R ラインカードを備えた Cisco Nexus 9504 および 9508 スイッチの場合、Cisco NX-OS リリース 7.0(3)F3(4) から 9.x リリースにアップグレードする必要があります。

手順

ステップ 1 スイッチのエンドポイント側ポートをシャットダウンします。
ステップ 2 IPFM を無効にします（**no feature nbm** コマンドを使用）。
ステップ 3 Cisco NX-OS リリース 9.2(3) 以降のリリースにアップグレードする場合は、ファブリックのスパイン スイッチで **ip pim pre-build-spt force** コマンドを無効にします。
ステップ 4 PIM パッシブ モードを無効にします (**no ip pim passive** コマンドを使用)。
ステップ 5 スイッチ ソフトウェアを 9.x リリースにアップグレードします。
ステップ 6 IPFM の TCAM カービングを設定し、スイッチをリロードします。
ステップ 7 NDFC をアップグレードします。
ステップ 8 該当する場合は、PIM と MSDP を設定します。
ステップ 9 IPFM を有効にします（**feature nbm** コマンドを使用）。
ステップ 10 CLI または NDFC を使用して IPFM ポリシーを構成します。
ステップ 11 Cisco NX-OS リリース 9.2(3) 以降のリリースにアップグレードし、NDFC を使用していない場合は、IGMP スタティック OIF を無効にして、フローを確立するための IPFM フロー定義を作成します。
ステップ 12 エンドポイントに面するすべてのポートを有効にします。

NDFC 向け SNMP サーバーの設定

スイッチを NDFC インベントリに追加すると、NDFC は、スイッチが SNMP トラップの送信先を認識できるように、次の構成でスイッチを自動的に構成します。**snmp-server host***dcnm-host-IP* **traps version 2c public udp-port 2162**。

コントローラ展開を計画している場合は、次の手順に従って、スイッチから NDFC への接続を確立します。

手順

ステップ 1 NDFC がスイッチから SNMP トラップを確実に受信するには、NDFC サーバ プロパティ **trap.registaddress=***dcnm-ip* under**Web UI Administrator->Server Properties** を構成して、スイッチが SNMP トラップを送信する IP アドレス（またはネイティブ HA の VIP アドレス）を指定します。

ステップ 2 インバンド環境の場合、NDFC でパッケージ化された **`pmn_telemetry_snmp`** CLI テンプレートを使用して、スイッチでより多くの SNMP 設定 (ソース インターフェイスなど) を構成できます。詳細については、「スイッチのグローバル構成」を参照してください。

ステップ 3 構成を保存し、NDFC を再起動します。

IPFM の構成

メディア向け IP ファブリックを構成する手順（IPFM）は、メディア ソリューションの IP ファブリックに使用した展開方法を構成する手順によって異なります。

- スパイン リーフ トポロジ
- シングル モジュラ スイッチ

スパイン リーフ トポロジの IPFM の構成

スパイン リーフ展開でスイッチの IPFM を構成するには、次の手順に従います。このモードでは、スパイン スイッチとリーフ スイッチで PIM アクティブ モードを有効にできます。この機能は、ファブリック内のマルチキャスト フローセットアップ インテリジェンスを提供します。複数のスパインと可変フロー サイズをサポートします。

スパイン リーフ トポロジは、ファブリック内のフローをプロビジョニングするために、IPFM と Protocol Independent Multicast（PIM）および Multicast Source Discovery Protocol（MSDP）を利用します。ファブリックは、PIM スパース モードおよび MSDP で設定する必要があります。

始める前に

PIM 機能を有効にします (**feature pim** コマンドを使用)。

OSPF ユニキャスト ルーティング プロトコルを使用している場合は、OSPF 機能を有効にします（**feature ospf** コマンドを使用）。

手順の概要

1. **configure terminal**
2. [**no**] **feature nbm**
3. （任意） [**no**] **nbm host-policy**

4. （任意） {**sender** | **receiver** | **pim**}
5. （任意） **default** {**permit** | **deny**}
6. （任意） 次のいずれかのコマンドを入力します。
   - 送信側ホスト ポリシーの場合：*sequence-number* **host** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
   - ローカル受信者ホスト ポリシーの場合：*sequence-number* **host** *ip-address* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
   - 外部受信者 (PIM) ホスト ポリシーの場合：*sequence-number* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
7. （任意） [**no**] **nbm reserve unicast fabric bandwidth** *value*
8. [**no**] **nbm flow asm range** [*group-range-prefixes*]
9. [**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**}
10. [**no**] **nbm flow dscp** *value*
11. （任意） [**no**] **nbm flow policer**
12. [**no**] **nbm flow-policy**
13. [**no**] **policy** *policy-name*
14. （任意） [**no**] **policer**
15. [**no**] **bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**}
16. [**no**] **dscp** *value*
17. [**no**] **ip group-range** *ip-address* **to** *ip-address*
18. （任意） [**no**] **priority critical**
19. （任意） [**no**] **priority level** <*1-15*>

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	[**no**] **feature nbm** 例： `switch(config)# feature nbm`	IPFM 機能と PIM アクティブ モードを有効にします。これにより、IPFM ファブリックは、外部コントローラからの支援なしでマルチキャスト フローを形成できます。 **feature nbm** コマンドを入力すると、次のコマンドも自動的に有効になります。 • **nbm mode pim-active** • **ip multicast multipath nbm**

	コマンドまたはアクション	目的

		• **ip pim prune-on-expiry**
		• **cdp enable**
		
		このコマンドの **no** 形式を使用すると、次のコマンドが無効になります。**feature nbm**、**nbm mode pim-active**、**ip multicast multipath nbm**、および **ip pim prune-on-expiry**.
		
		（注）
		-R ライン カードを使用して Cisco Nexus 9504 および 9508 スイッチの IPFM を無効にする場合は、これらの TCAM カービング コマンドを次の順序で設定し、スイッチをリロードする必要があります。推奨される TCAM 値は 2048 です。
		`hardware access-list tcam region ing-nbm 0`
		`hardware access-list tcam region redirect_v6 TCAM-size`
		
		（注）
		IPFM VRF を設定する場合は、アクティブ フロー プロビジョニングのための IPFM VRF の構成 （63 ページ）を参照してください。

ステップ 3	（任意） [**no**] **nbm host-policy**
	例：
	`switch(config)# nbm host-policy`
	`switch(config-nbm-host-pol)#`
		スイッチの IPFM ホスト ポリシーを設定します。

ステップ 4	（任意） {**sender** | **receiver** | **pim**}
	例：
	`switch(config-nbm-host-pol)# sender`
	`switch(config-nbm-host-pol-sender)#`
		送信者、ローカル受信者、または外部受信者 (PIM) の IPFM ホスト ポリシーを構成します。
		
		（注）
		デフォルトの IPFM ホスト ポリシーを更新する前に、最初にカスタム ホスト ポリシーを削除する必要があります。

ステップ 5	（任意） **default** {**permit** | **deny**} **例**： `switch(config-nbm-host-pol-sender)# default permit`	IPFM ホスト ポリシーのデフォルト アクションを指定します。デフォルトでは、3 種類のホスト ポリシーがすべて許可されます。
ステップ 6	（任意） 次のいずれかのコマンドを入力します。 • 送信側ホスト ポリシーの場合：*sequence-number* **host** *ip-address* **group** *ip-prefix* {**deny** | **permit**}	送信側または受信側のフローを許可するか拒否するかを指定します。

	コマンドまたはアクション	目的

	• ローカル受信者ホスト ポリシーの場合：*sequence-number* **host** *ip-address* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
	• 外部受信者 (PIM) ホスト ポリシーの場合：*sequence-number* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
	例：
	`switch(config-nbm-host-pol-sender)# 10 host 101.1.1.3 group 229.1.1.1/32 deny`
	例：
	`switch(config-nbm-host-pol-rcvr)# 40 host 100.1.1.1 source 145.1.1.1 group 234.1.1.1/32 deny`
	例：
	`switch(config-nbm-host-pol-pim)# 50 source 101.1.1.1 group 235.1.1.1/32 deny`
		送信側およびローカル受信側のホスト ポリシーのホスト IP アドレスには、ワイルドカード (0.0.0.0) を入力できます。以前のリリースでは、ホスト ポリシーをスイッチのインターフェイスに関連付けるために、ホストの IP アドレスが必要でした。ワイルドカードを使用すると、単一の設定を使用して、特定のグループまたはマスクでマルチキャスト トラフィックを送受信しているすべてのホストを検出できます。ホスト IP アドレスがローカル受信者ホスト ポリシーのワイルドカードである場合、ソース IP アドレスもワイルドカードです。この手順の最後にあるワイルドカード設定の例を参照してください。

ステップ 7	（任意） [**no**] **nbm reserve unicast fabric bandwidth** *value* **例**： `switch(config)# nbm reserve unicast fabric bandwidth 2`	ユニキャスト フロー用にファブリック ポートの帯域幅の割合を予約します。IPFM フロー管理は、この帯域幅をフロー セットアップに使用せず、ユニキャスト トラフィック用にすべてのファブリック インターフェイスで予約します。範囲は 0 ～ 100% で、デフォルト値は 0 です。
ステップ 8	[**no**] **nbm flow asm range** [*group-range-prefixes*] **例**： `switch(config)# nbm flow asm range 224.0.0.0/8 225.0.0.0/8 226.0.0.0/8 227.0.0.0/8`	*,G 結合の IPFM ASM グループ範囲をプログラムします。このグループ範囲内の IGMP 加入は、V2 加入または（*、G）加入であると予想されます。最大 20 のグループ範囲を設定できます。デフォルトでは、グループ範囲は構成されていません。 （注） このコマンドは、マルチスパイン展開でのみ必要です。
ステップ 9	[**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} **例**： `switch(config)# nbm flow bandwidth 3000 mbps`	Kbps、Mbps、または Gbps でグローバル IPFM フロー帯域幅を設定します。サポートされる最小フロー帯域幅は 200 Kbps です。

範囲	デフォルト値
1 ～ 25,000,000 Kbps	0 Kbps
1 ～ 25,000 Mbps	0 Mbps
1 ～ 25 Gbps	0 Gbps

	コマンドまたはアクション	目的
ステップ 10	[**no**] **nbm flow dscp** *value* 例： `switch(config)# nbm flow dscp 10`	グローバル IPFM フロー DSCP 値を設定します。範囲は 0 ～ 63 です。いずれかのフローが IPFM フロー グループ範囲と一致しない場合、デフォルトのフロー DSCP が帯域幅管理とフロー設定に使用されます。
ステップ 11	（任意） [**no**] **nbm flow policer** 例： `switch(config)# no nbm flow policer`	すべての IPFM フロー ポリシーのポリサーを有効または無効にします。ポリサーはデフォルトで有効になっています。

ステップ 12	[**no**] **nbm flow-policy**
	例：
	`switch(config)# nbm flow-policy`
	`switch(config-nbm-flow-pol)#`
		フローごとのフロー帯域幅を設定します。

ステップ 13	[**no**] **policy** *policy-name*
	例：
	`switch(config-nbm-flow-pol)# policy nbmflow10`
	`switch(config-nbm-flow-pol-attr)#`
		IPFM フロー ポリシーを構成します。ポリシー名には最大63文字の英数字を指定できます。

ステップ 14	（任意） [**no**] **policer** 例： `switch(config-nbm-flow-pol-attr)# no policer`	指定された IPFM フロー ポリシーのポリサーを有効または無効にします。 デフォルトでは、各送信元フローは送信元リーフでポリサーを使用します（最初のホップ ルータ）マルチキャスト送信元の数がポリサーの数を超えた場合、フローは送信元リーフで承認されません。動作をオーバーライドするには、フロー ポリシーでポリサーを無効にできます。ポリサーが無効になっている場合のフロー ポリシーに一致するフローは、ポリサー リソースが消費されません。 （注） 誤動作のエンドポイントにより許可されている以上の送信が発生した場合、ネットワークが保護されない状態を招く可能性があるため、注意深くこのコマンドを使用します。集約ポリサーなど別の方法を使用して、IPFM でプログラミングされているポリサーがないフローをレート制限します。集約ポリサーの設定に関する詳細は、「共有ポリサーの設定」を参照してください。
ステップ 15	[**no**] **bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} 例：	このポリシーに一致するマルチキャスト グループに、Kbps、Mbps、または Gbps でフロー帯域幅を設

	コマンドまたはアクション	目的
	`switch(config-nbm-flow-pol-attr)# bandwidth 10 mbps`	定します。サポートされる最小フロー帯域幅は200 Kbps です。 範囲 / デフォルト値 1 ～ 25,000,000 Kbps / 0 Kbps 1 ～ 25,000 Mbps / 0 Mbps 1 ～ 25 Gbps / 0 Gbps
ステップ 16	[**no**] **dscp** *value* 例： `switch(config-nbm-flow-pol-attr)# dscp 10`	指定されたグループ範囲に一致するフローの最初のホップの冗長性に、差別化サービス コード ポイント (DSCP) 値を設定します。

ステップ 17	[**no**] **ip group-range** *ip-address* **to** *ip-address*
	例：
	`switch(config-nbm-flow-pol-attr)# ip group-range 224.19.10.1 to 224.19.255.1`
	`switch(config-nbm-flow-pol-attr)# ip group-range 224.20.10.1 to 224.20.255.1`
		このポリシーに関連付けられているマルチキャスト グループの IP アドレス範囲を指定します。

ステップ 18	（任意） [**no**] **priority critical**
	例：
	`switch(config-nbm-flow-pol-attr-prop)# priority critical`
	`switch(config-nbm-flow-pol-attr-prop)#`
		設定されているマルチキャスト グループのクリティカル フローの優先順位付けを有効にします。**Critical** が最高の優先順位です。

ステップ 19	（任意） [**no**] **priority level** *<1-15>* 例： `switch(config-nbm-flow-pol-attr-prop)# priority level 1`	構成中のマルチキャスト グループの詳細なフロー優先順位を、レベル 1 ～ 15 で有効にします。デフォルト値は **low** で、これはゼロ（0）です。最も低いプライオリティでもあります。

例

次の例では、ワイルドカード ホスト ポリシーのサンプル設定を示します。

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

switch(config)# show nbm host-policy applied sender all
Default Sender Policy: Allow
Applied WildCard host policies
Seq Num    Source     Group       Group Mask  Action
```

```
1100       0.0.0.0    224.1.1.1   32          Allow
Total Policies Found = 1

switch(config)# show nbm host-policy applied receiver local all
Default Local Receiver Policy: Allow
Interface  Seq Num  Source   Group      Group Mask  Action  Deny counter  WILDCARD

           1100     0.0.0.0  231.1.1.1  32          Allow   0
Total Policies Found = 1
```

次のタスク

PIM の設定

MSDP の設定

ファブリックおよびホスト インターフェイスの設定

IPFM VRF の構成 （62 ページ）

IPFM フローの確立

スパインおよびリーフ スイッチの PIM の設定

スパイン リーフ トポロジでスパインおよびリーフ スイッチの PIM を設定するには、次の手順に従います。設定は、すべてのノードで同じである必要があります。

始める前に

スパイン リーフ トポロジの IPFM を設定します。

手順の概要

1. **configure terminal**
2. **ip pim rp-address** *rp-address* **group-list** *ip-prefix*
3. **ip pim ssm range none**
4. **ip pim spt-threshold infinity group-list** *route-map-name*
5. **route-map** *policy-name* **permit** *sequence-number*
6. **match ip multicast group** *policy-name* **permit** *sequence-number*
7. **interface** *interface-type slot/port*
8. **mtu** *mtu-size*
9. **ip address** *ip-prefix*
10. **ip ospf passive-interface**
11. **ip router ospf** *instance-tag* **area** *area-id*
12. **ip pim sparse-mode**
13. **ip igmp version** *number*
14. **ip igmp immediate-leave**
15. RP インターフェイスを設定します。

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**ip pim rp-address** *rp-address* **group-list** *ip-prefix* 例： `switch(config)# ip pim rp-address 1.2.1.1 group-list 224.0.0.0/4`	マルチキャスト グループ範囲に、PIM スタティック RP アドレスを設定します。スパインは RP として設定する必要があります。マルチ スパイン展開では、すべてのスパインを、ループバック インターフェイスで設定された同じ IP アドレスを持つ RP として設定する必要があります。
ステップ 3	**ip pim ssm range none** 例： `switch(config)# ip pim ssm range none`	送信側トラフィックをスパイン層に強制し、フロー設定の遅延を減らします。 （注） SSM はファブリックで引き続きサポートされており、このコマンドは SSM を無効にしません。
ステップ 4	**ip pim spt-threshold infinity group-list** *route-map-name* 例： `switch(config)# ip pim spt-threshold infinity group-list mcast-all`	指定されたルート マップで定義されているグループ プレフィックスに対して、IPv4 PIM（*, G）状態のみを作成します。

ステップ 5	**route-map** *policy-name* **permit** *sequence-number*
	例：
	`switch(config)# route-map mcast-all permit 10`
	`switch(config-route-map)#`
		ルートマップ コンフィギュレーション モードを開始します。

ステップ 6	**match ip multicast group** *policy-name* **permit** *sequence-number* 例： `switch(config-route-map)# match ip multicast group 224.0.0.0/4`	指定されたグループに一致します。ルート マップ グループ アドレスが IPFM フロー ASM 範囲グループ アドレスと一致していることを確認してください。

ステップ 7	**interface** *interface-type slot/port*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 8	**mtu** *mtu-size* 例： `switch(config-if)# mtu 9216`	ジャンボ トラフィックをサポートする MTU サイズを設定します。すべてのホストおよびファブリック インターフェイスで設定する必要があります。
ステップ 9	**ip address** *ip-prefix* 例： `switch(config-if)# ip address 10.3.10.1/24`	このインターフェイスの IP アドレスを設定します。
ステップ 10	**ip ospf passive-interface** 例： `switch(config-if)# ip ospf passive-interface`	インターフェイス上でルーティングが更新されないようにします。このコマンドによって、ルータまたは VRF コマンド モードの設定が上書きされます。OSPF は、ホスト側のインターフェイスでのみパッシブに実行されます。この構成は、エンドポイント インターフェイスでのみ必要であり、ファブリック インターフェイスでは必要ありません。
ステップ 11	**ip router ospf** *instance-tag* **area** *area-id* 例： `switch(config-if)# ip router ospf p1 area 0.0.0.0`	インターフェイスで OSPF を有効にします。
ステップ 12	**ip pim sparse-mode** 例： `switch(config-if)# ip pim sparse-mode`	インターフェイスで PIM スパース モードをイネーブルにします。
ステップ 13	**ip igmp version** *number* 例： `switch(config-if)# ip igmp version 3`	エンドポイント インターフェイスでのみ IGMPv3 パケットのサポートを有効にします。
ステップ 14	**ip igmp immediate-leave** 例： `switch(config-if)# ip igmp immediate-leave`	エンドポイント インターフェイスだけに IGMP 即時脱退を設定します。

ステップ 15	RP インターフェイスを設定します。
	例：
	`switch(config)# interface loopback0`
	`  ip address 1.2.1.1/32`
	`  ip router ospf p1 area 0.0.0.0`
	`  ip pim sparse-mode`
		RP インターフェイスの IP アドレスが各スパイン スイッチで同じであることを確認してください。
		（注）
		この設定は、スパイン スイッチでのみ入力します。

スパイン スイッチで MSDP の設定

スパイン リーフ トポロジでスパイン スイッチの MSDP を設定するには、次の手順に従います。

（注） MSDP は、ASM 範囲を使用するマルチスパイン展開でのみ必要です。シングル スパイン展開では、MSDP は必要ありません。

始める前に

MSDP 機能を有効にします（**feature msdp** コマンドを使用）。

手順の概要

1. **configure terminal**
2. スパイン スイッチ間で MSDP セッションを確立するようにループバック インターフェイスを設定します。
3. **ip msdp originator-id** *interface*
4. **ip msdp peer** *peer-ip-address* **connect-source** *interface*
5. **ip msdp sa-policy** *peer-ip-address policy-name* **out**
6. **route-map** *policy-name* **permit** *sequence-number*
7. **match ip multicast group** *policy-name* **permit** *sequence-number*

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	スパイン スイッチ間で MSDP セッションを確立するようにループバック インターフェイスを設定します。
	例：
	`interface loopback1`
	`  ip address 2.2.3.3/32`
	`  ip router ospf p1 area 0.0.0.0`
	`  ip pim sparse-mode`
		スパイン スイッチ間に MSDP セッションを確立します。

ステップ 3	**ip msdp originator-id** *interface* 例： `switch(config)# ip msdp originator-id loopback1`	Source-Active（SA）メッセージエントリの RP フィールドで使用される IP アドレスを設定します。
ステップ 4	**ip msdp peer** *peer-ip-address* **connect-source** *interface* 例：	MSDP ピアを設定してピア IP アドレスを指定します。

	コマンドまたはアクション	目的
	`switch(config)# ip msdp peer 2.2.1.1 connect-source loopback1`	
ステップ 5	**ip msdp sa-policy** *peer-ip-address policy-name* **out** 例： `switch(config)# ip msdp sa-policy 2.2.1.1 msdp-mcast-all out`	発信 SA メッセージのルートマップ ポリシーをイネーブルにします。デフォルトでは、発信される SA メッセージには登録済みの全送信元が含まれます。

ステップ 6	**route-map** *policy-name* **permit** *sequence-number*
	例：
	`switch(config)# route-map msdp-mcast-all permit 10`
	`switch(config-route-map)#`
		ルートマップ コンフィギュレーション モードを開始します。

ステップ 7	**match ip multicast group** *policy-name* **permit** *sequence-number* 例： `switch(config-route-map)# match ip multicast group 224.0.0.0/8`	指定されたグループに一致します。ルート マップ グループ アドレスが IPFM フロー ASM 範囲グループ アドレスと一致していることを確認してください。

優先順位ベースのフロー

IPFM 優先順位ベースのフロー機能は、特定の重要なフローまたは高優先順位のフローに優先順位を付け、優先順位の低いフローに影響が及ぶようにして、これらのリソースに制約がある状況で必要な帯域幅またはポリサーを確保するオプションを提供します。

このアクションは、固有のコマンドによって制御されます。優先順位ベースのフロー機能の有効化を参照してください。したがって、高優先順位のフロー、レポート、または Join が機能をサポートしているシステムに到着し、システムが OIF または IIF の帯域幅またはポリサー リソースで飽和状態になると、低優先順位のフローに影響が及びます。低優先順位のフローは、帯域幅に応じて影響を受けます。高優先順位のフローに対応し、通過を許可するために必要な帯域幅を解放するために、低優先順位のフローが影響を受ける順序は、その帯域幅に基づいて昇順になっており、優先順位 レベル 0 から始まり、順に優先順位 レベル 1 ～ 15 となります。詳細については、 高優先順位フローが低優先順位フローに及ぼす影響を参照してください。

IPFM は、フローの先頭または開始時に、クリティカルつまり高優先順位フローの優先順位を保証します。これは、IGMP プロセスが高優先順位として分類されたフローに参加することを要求すると、IPFM が優先順位の低いフローの一部をプロアクティブに中断して、優先順位の高いフローの通過を許可することを意味します。

プライオリティベースのフロー機能の有効化

詳細なプライオリティベースのフロー機能は、デフォルトでは無効になっています。この機能を有効にするには、**nbm flow impact-low-priority** コマンドを使用します。

この機能を無効にするには、このコマンドの **no** 形式を使用します。

優先順位ベースのフローの設定に関するガイドラインと制約事項

ここでは、詳細な優先順位ベースのフロー設定に関するガイドラインと制限事項について説明します。

リリースごとの機能サポート

リリース	機能の説明
9.3(x)	リンクフラップ、トポロジ変更通知（TCN）、またはプレフィックスの変更などのネットワークイベント中に、MRIB は影響を受けたフローの再 RPF を実行します。その際、クリティカルな優先順位のフローを優先させて代替 RPF を見つけ、その後で優先順位の低いフローにアクセスします。
10.5（2）F	優先順位ベースのフロー機能は有効または無効にできます。この機能は、マルチレベル優先順位、つまり、優先順位ゼロ（0）と優先順位レベル 1 ～ 15 をサポートします。

ISSD と ISSU

- 機能の優先順位ベースのフローは、無停止の（ND）ISSU をサポートしていません。
- 10.5(2)F より前のリリースに対して ISSD を実行する前には、構成されたすべてのマルチレベル優先順位を削除し、優先順位ベースのフロー機能を無効にしてください。

サポートされない機能

優先順位ベースのフローは、PIM パッシブ モードではサポートされません。

優先順位の低いフローに対して優先順位の高いフローが及ぼす影響

フローには常に優先順位が付けられます。ただし、フローの優先順位付け方法は、フローの優先順位機能が有効か無効かということや、さまざまなレベルの優先順位が定義されているかどうかによって異なります。このセクションでは、クリティカルなフローが着信したときに、優先順位の低いフローと優先順位レベル 1 ～ 15 がどのように影響を受けるかについて説明します。

入力または出力、または両方のインターフェイスで帯域幅が小さい場合、またはポリサーがない場合、優先順位の低いフローは影響を受けます。

（注） SVI フローには、次のガイドラインと制約事項があります。

- 優先順位の低いフローが存在しない場合、SVI 固有のスロット、ユニット、スライス、または UMNAT フローが影響を受けます。
- SVI に低優先順位フローが存在しない場合、すべてのスロット、ユニット、またはスライスの最初の低優先順位フローが影響を受けます。

例

ここでは、クリティカルな優先順位に対応する必要がある、複数の優先順位を持つフローの例について説明します。この例では、一連のクリティカルなフローに対応するために、設定された優先順位がどのように影響を受けるかを示します。

次のシナリオでは、優先順位 0 および優先順位 1 のフローで帯域幅が使い果たされてしまうため、より高い優先順位のフローに対応する必要があります。

最初に受信した優先順位の高いフローは 225.3.3.1 です。

プライオリティ 0	帯域幅	優先順位 1	帯域幅	優先順位 2	帯域幅	優先順位クリティカル	帯域幅
225.1.1.1	10	225.2.2.1	40	225.3.3.1	160	225.64.64.1	160
225.1.1.2	20	225.2.2.2	50	225.3.3.2	20	225.64.64.2	110
225.1.1.3	30	225.2.2.3	100	225.3.3.3	10	-	-

影響を受ける優先順位の低いフローは、225.1.1.1、225.1.1.2、225.1.1.3、および 225.2.2.3 です。

次に、優先順位の高いフロー 225.64.64.2 に対応する必要があります。この表は、優先順位フローと使用可能な帯域幅を示しています。

プライオリティ 0	帯域幅	優先順位 1	帯域幅	優先順位 2	帯域幅	優先順位クリティカル	帯域幅
-	-	225.2.2.1	40	225.3.3.1	160	225.64.64.1	160
-	-	225.2.2.2	50	225.3.3.2	20	225.64.64.2	110
-	-	-	-	225.3.3.3	10	-	-

優先順位レベルと使用可能な帯域幅に基づいて、このシナリオで影響を受けるフローは 225.2.2.1、225.2.2.2、および 225.3.3.2 です。

プライオリティベース フロー制御の構成例

これは、マルチレベル プライオリティ フローの例です。

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

これは、プライオリティ レベルの構成例です。

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

ファブリックおよびホスト インターフェイスの設定

このセクションの CLI コマンドを使用してファブリックとホスト インターフェイスを構成するか、NDFC を使用してこれらの構成を自動プロビジョニングできます。

（注） エンドポイントへのレイヤ 3 ルーテッド ポートを使用することをお勧めします。

ファブリック インターフェイスを設定する

各リーフ スイッチでファブリック インターフェイスを設定する必要があります。このインターフェイスは、リーフ スイッチからスパイン スイッチに移動します。

（注） 、メディアの IP ファブリックと外部システムの間でメディア フローを交換できるようにする場合は、WAN リンクでは必ず

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot*/*port*
3. **ip address** *ip-prefix*/*length*
4. **ip router ospf** *instance-tag* **area** *area-id*
5. **ip pim sparse-mode**
6. **no shutdown**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**interface ethernet** *slot*/*port*
	例：
	`switch(config)# interface ethernet 1/49`
	`switch(config-if)#`
		ファブリック インターフェイスとエントリ インターフェイス設定モードを指定します。

ステップ 3	**ip address** *ip-prefix*/*length* 例： `switch(config-if)# ip address 1.1.1.0/31`	このインターフェイスにIPアドレスおよびサブネット マスクを割り当てます。
ステップ 4	**ip router ospf** *instance-tag* **area** *area-id* 例： `switch(config-if)# ip router ospf 100 area 0.0.0.0`	OSPFv2 インスタンスおよびエリアにインターフェイスを追加します。
ステップ 5	**ip pim sparse-mode** 例： `switch(config-if)# ip pim sparse-mode`	現在のインターフェイスで PIM スパース モードをイネーブルにします。
ステップ 6	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをイネーブルにします。

レイヤ 3 ホスト インターフェイスの設定

各リーフ スイッチでレイヤ3ルーテッドホストインターフェイスを設定する必要があります。このインターフェイスは、リーフ スイッチからエンドポイントに移動します。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	**interface ethernet** *slot*/*port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		ホスト インターフェイスとエントリ インターフェイス設定モードを指定します。

ステップ 3	**ip igmp version 3** 例： `switch(config-if)# ip igmp version 3`	IGMP バージョンを 3 に設定します。
ステップ 4	**ip address** *ip-prefix*/*length* 例： `switch(config-if)# ip address 100.1.1.1/24`	このインターフェイスに IP アドレスおよびサブネット マスクを割り当てます。
ステップ 5	**ip router ospf** *instance-tag* **area** *area-id* 例： `switch(config-if)# ip router ospf 100 area 0.0.0.0`	OSPFv2 インスタンスおよびエリアにインターフェイスを追加します。
ステップ 6	**ip pim sparse-mode** 例： `switch(config-if)# ip pim sparse-mode`	現在のインターフェイスで PIM スパース モードをイネーブルにします。
ステップ 7	**ip ospf passive-interface** 例： `switch(config-if)# ip ospf passive-interface`	インターフェイス上でルーティングが更新されないようにします。このコマンドによって、ルータまたは VRF コマンド モードの設定が上書きされます。OSPF は、ホスト側のインターフェイスでのみパッシブに実行されます。この構成は、エンドポイント インターフェイスでのみ必要であり、ファブリック インターフェイスでは必要ありません。
ステップ 8	**ip igmp immediate-leave** 例： `switch(config-if)# ip igmp immediate-leave`	スイッチが、グループに関する Leave メッセージの受信後、ただちにマルチキャスト ルーティング テーブルからグループ エントリを削除できるようにします。

	コマンドまたはアクション	目的
ステップ 9	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをイネーブルにします。

SVI ホスト インターフェイスでレイヤ 2 を選択する

各リーフ スイッチで SVI ホスト インターフェイスを備えたレイヤ 2 を設定する必要があります。このインターフェイスは、リーフ スイッチからエンドポイントに移動します。

手順の概要

1. **configure terminal**
2. **feature interface-vlan**
3. **vlan** *vlan-id*
4. **exit**
5. **vlan configuration** *vlan-id*
6. **ip igmp snooping**
7. **ip igmp snooping fast-leave**
8. **exit**
9. **interface vlan** *vlan-id*
10. （任意） **ip igmp version 3**
11. **ip router ospf** *instance-tag* **area** *area-id*
12. **ip address** *ip-address*
13. **ip pim sparse-mode**
14. **ip pim passive**
15. **ip igmp suppress v3-gsq**
16. **no shutdown**
17. **exit**
18. **interface ethernet** *port/slot*
19. **switchport**
20. **switchport mode** {**access** | **trunk**}
21. switchport {access | trunk allowed} **vlan** *vlan-id*
22. **no shutdown**
23. **exit**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	グローバル設定モードを開始します。

	コマンドまたはアクション	目的
	`switch# configure terminal` `switch(config)#`	
ステップ 2	**feature interface-vlan** 例： `switch(config)# feature interface-vlan`	VLAN インターフェイスの作成を有効にします。

ステップ 3	**vlan** *vlan-id*
	例：
	`switch(config)# vlan 5`
	`switch(config-vlan)#`
		VLAN を作成します。範囲は 2 ～ 3967 です。VLAN 1 はデフォルト VLAN であり、作成や削除はできません。VLAN の詳細については、『Cisco Nexus 9000 シリーズ NX-OS レイヤ 2 スイッチング設定ガイド』を参照してください。

ステップ 4	**exit**
	例：
	`switch(config-vlan)# exit`
	`switch(config)#`
		VLAN モードを終了します。

ステップ 5	**vlan configuration** *vlan-id*
	例：
	`switch(config)# vlan configuration 5`
	`switch(config-vlan-config)#`
		実際にこれらを作成しないで VLAN を設定できるようにします。

ステップ 6	**ip igmp snooping** 例： `switch(config-vlan-config)# ip igmp snooping`	特定の VLAN のデバイスで IGMP スヌーピングを有効にします。IGMP スヌーピングの詳細については、『Cisco Nexus 9000 シリーズ NX-OS マルチキャスト ルーティング設定ガイド』を参照してください。
ステップ 7	**ip igmp snooping fast-leave** 例： `switch(config-vlan-config)# ip igmp snooping fast-leave`	IGMPv2 プロトコルのホスト レポート抑制メカニズムのために、明示的に追跡できない IGMPv2 ホストをサポートします。高速脱退が有効な場合、IGMP ソフトウェアは、各 VLAN ポートに接続されたホストが 1 つだけであると見なします。デフォルトは、すべての VLAN でディセーブルです。

ステップ 8	**exit**
	例：
	`switch(config-vlan-config)# exit`
	`switch(config)#`
		VLAN コンフィギュレーション モードを終了します。

ステップ 9	**interface vlan** *vlan-id*
	例：
	`switch(config)# interface vlan 5`
	`switch(config-if)#`
		VLAN インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。範囲は 2 ～ 3967 です。

	コマンドまたはアクション	目的
ステップ 10	（任意） **ip igmp version 3** 例： `switch(config-if)# ip igmp version 3`	IGMP バージョンを 3 に設定します。IGMP バージョン 3 を使用している場合は、このコマンドを入力します。
ステップ 11	**ip router ospf** *instance-tag* **area** *area-id* 例： `switch(config-if)# ip router ospf 201 area 0.0.0.15`	OSPFv2 インスタンスおよびエリアにインターフェイスを追加します。
ステップ 12	**ip address** *ip-address* 例： `switch(config-if)# ip address 192.0.2.1/8`	このインターフェイスの IP アドレスを設定します。
ステップ 13	**ip pim sparse-mode** 例： `switch(config-if)# ip pim sparse-mode`	現在のインターフェイスで PIM スパース モードをイネーブルにします。PIM スヌーピングの詳細については、『Cisco Nexus 9000 シリーズ NX-OS マルチキャスト ルーティング設定ガイド』を参照してください。
ステップ 14	**ip pim passive** 例： `switch(config-if)# ip pim passive`	デバイスがインターフェイス上で PIM メッセージを送信したり、このインターフェイスを介して他のデバイスからの PIM メッセージを受け入れたりしないようにします。代わりに、デバイスはネットワーク上の唯一の PIM デバイスであると見なし、すべての Bidir PIM グループ範囲の指定ルーターおよび指定フォワーダーとして機能します。
ステップ 15	**ip igmp suppress v3-gsq** 例： `switch(config-if)# ip igmp suppress v3-gsq`	ルータが IGMPv3 Leave レポートを受信したときにクエリを生成しないようにします。
ステップ 16	**no shutdown** 例： `switch(config-if)# no shutdown`	ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。 （注） このコマンドは、前のマルチキャスト コマンドを入力した後にのみ適用してください。

ステップ 17	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		VLAN コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 18	**interface ethernet** *port/slot* 例： `switch(config-if)# interface ethernet 2/1`	イーサネット インターフェイスを設定します。
ステップ 19	**switchport** 例： `switch(config-if)# switchport`	インターフェイスをレイヤ2インターフェイスとして設定します。
ステップ 20	**switchport mode** {**access** | **trunk**} 例： `switch(config-if)# switchport mode trunk`	次のいずれかのオプションを構成します。 **access**：インターフェイスを、非トランキング、タグなし、シングル VLAN レイヤ 2 インターフェイスとして設定します。アクセス ポートは、1 つの VLAN のトラフィックだけを伝送できます。アクセス ポートは、デフォルトで、VLAN 1 のトラフィックを送受信します。 **trunk**：インターフェイスをレイヤ 2 トランク ポートとして設定します。トランク ポートは、同じ物理リンクで 1 つ以上の VLAN 内のトラフィックを伝送できます。(VLAN は、トランク許可 VLAN リストに基づいています。)デフォルトでは、トランク インターフェイスはすべての VLANのトラフィックを伝送できます。
ステップ 21	switchport {access | trunk allowed} **vlan** *vlan-id* 例： `switch(config-if)# switchport trunk allowed vlan 5`	次のいずれかのオプションを構成します。 **access**：このアクセス ポートでトラフィックを伝送する VLAN を指定します。このコマンドを入力しない場合、アクセス ポートは VLAN 1 だけでトラフィックを伝送します。 **trunk allowed**：トランク インターフェイスの許可された VLAN を指定します。デフォルトでは、トランク インターフェイス上のすべての VLAN（1 ～ 3967 および 4048 ～ 4094）が許可されます。VLAN 3968 ～ 4047 は、内部で使用するデフォルトで予約されている VLAN です。
ステップ 22	**no shutdown** 例： `switch(config-if)# no shutdown`	ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。
ステップ 23	**exit** 例：	インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
	`switch(config-if)# exit` `switch(config)#`	

単一モジュラ スイッチのための IPFM 構成

IP ファブリックを設定したら、スイッチで IPFM 機能を有効にする必要があります。IPFM 機能により、ファブリックに着信する帯域幅と発信される帯域幅とがまったく同じになることが保証されます。

単一のモジュラー スイッチの IPFM を構成するには、次の手順に従います。

始める前に

PIM 機能を有効にします (**feature pim** コマンドを使用)。

OSPF ユニキャスト ルーティング プロトコルを使用している場合は、OSPF 機能を有効にします（**feature ospf** コマンドを使用）。

手順の概要

1. **configure terminal**
2. [**no**] **feature nbm**
3. [**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**}
4. （任意） [**no**] **nbm flow policer**
5. [**no**] **nbm flow-policy**
6. [**no**] **policy** *policy-name*
7. （任意） [**no**] **policer**
8. [**no**] **bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**}
9. [**no**] **ip group** *ip-address*
10. （任意） [**no**] **priority critical**
11. [**no**] **ip group-range** *ip-address* **to** *ip-address*
12. （任意） [**no**] **priority critical**
13. （任意） [**no**] **priority level** <*1-15*>

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	[no] **feature nbm**
	例：
	`switch(config)# feature nbm`
		IPFM 機能を有効にします。この機能を無効にするには、このコマンドの **no** 形式を使用します。
		（注）
		-R ライン カードを搭載した Cisco Nexus 9504 および 9508 スイッチの IPFM を無効にするには、これらの TCAM カービング コマンドを次の順序で設定し、スイッチをリロードする必要があります。推奨される TCAM 値は 2048 です。
		`hardware access-list tcam region ing-nbm 0`
		`hardware access-list tcam region redirect_v6 TCAM-size`
		（注）
		IPFM VRF を設定する場合は、アクティブ フロー プロビジョニングのための IPFM VRF の構成 （63 ページ）を参照してください。

ステップ 3	[no] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} 例： `switch(config)# nbm flow bandwidth 150 mbps`	Kbps、Mbps、または Gbps でグローバル IPFM フロー帯域幅を設定します。サポートされる最小フロー帯域幅は 200 Kbps です。 範囲：1 ～ 25,000,000 Kbps / デフォルト値：0 Kbps 範囲：1 ～ 25,000 Mbps / デフォルト値：0 Mbps 範囲：1 ～ 25 Gbps / デフォルト値：0 Gbps
ステップ 4	（任意） [no] **nbm flow policer** 例： `switch(config)# no nbm flow policer`	すべての IPFM フロー ポリシーのポリサーを有効または無効にします。ポリサーはデフォルトで有効になっています。

ステップ 5	[no] **nbm flow-policy**
	例：
	`switch(config)# nbm flow-policy`
	`switch(config-nbm-flow-pol)#`
		フローごとのフロー帯域幅を設定します。

ステップ 6	[no] **policy** *policy-name*
	例：
	`switch(config-nbm-flow-pol)# policy 1.5gbps`
	`switch(config-nbm-flow-pol-attr)#`
		IPFM フロー ポリシーを構成します。ポリシー名には最大63文字の英数字を指定できます。

ステップ 7	（任意） [no] **policer** 例：	指定された IPFM フロー ポリシーのポリサーを有効または無効にします。

	コマンドまたはアクション	目的
	`switch(config-nbm-flow-pol-attr)# no policer`	デフォルトでは、各送信元フローは送信元リーフでポリサーを使用します（最初のホップ ルータ）マルチキャスト送信元の数がポリサーの数を超えた場合、フローは送信元リーフで承認されません。動作をオーバーライドするには、フロー ポリシーでポリサーを無効にできます。ポリサーが無効になっている場合のフロー ポリシーに一致するフローは、ポリサー リソースが消費されません。 （注） 誤動作のエンドポイントにより許可されている以上の送信が発生した場合、ネットワークが保護されない状態を招く可能性があるため、注意深くこのコマンドを使用します。集約ポリサーなど別の方法を使用して、IPFM でプログラミングされているポリサーがないフローをレート制限します。集約ポリサーの詳細については、Cisco.com の『*Cisco Nexus 9000* シリーズ*NX-OS Quality of Service* 構成ガイド』の「ポリシングの構成」の章の「共有ポリサーの構成」のセクションを参照してください。
ステップ 8	[**no**] **bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} 例： `switch(config-nbm-flow-pol-attr)# bandwidth 1500 mbps`	このポリシーに一致するマルチキャスト グループに、Kbps、Mbps、または Gbps でフロー帯域幅を設定します。サポートされる最小フロー帯域幅は 200 Kbps です。 範囲：1 ～ 25,000,000 Kbps / デフォルト値：0 Kbps 範囲：1 ～ 25,000 Mbps / デフォルト値：0 Mbps 範囲：1 ～ 25 Gbps / デフォルト値：0 Gbps

ステップ 9	[**no**] **ip group** *ip-address*
	例：
	`switch(config-nbm-flow-pol-attr)# ip group 228.0.0.15`
	`switch(config-nbm-flow-pol-attr)# ip group 228.0.255.15`
		/32 マルチキャスト グループの IP アドレスを指定します。

ステップ 10	（任意） [**no**] **priority critical**
	例：
	`switch(config-nbm-flow-pol-attr-prop)# priority critical`
	`switch(config-nbm-flow-pol-attr-prop)#`
		設定されているマルチキャスト グループのクリティカル フローの優先順位付けを有効にします。

	コマンドまたはアクション	目的

ステップ 11	[**no**] **ip group-range** *ip-address* **to** *ip-address*
	例：
	`switch(config-nbm-flow-pol-attr)# ip group-range 239.255.255.121 to 239.255.255.130`
	`switch(config-nbm-flow-pol-attr)# ip group-range 239.255.255.131 to 239.255.255.140`
	`switch(config-nbm-flow-pol-attr)# ip group-range 239.255.255.141 to 239.255.255.150`
	`switch(config-nbm-flow-pol-attr)# ip group-range 239.255.255.151 to 239.255.255.160`
		このポリシーに関連付けられたマルチキャスト グループの IP アドレス範囲を指定します。

ステップ 12	（任意） [**no**] **priority critical**
	例：
	`switch(config-nbm-flow-pol-attr-prop)# priority critical`
	`switch(config-nbm-flow-pol-attr-prop)#`
		設定されているマルチキャストグループのクリティカルフローの優先順位付けを有効にします。**Critical** が最高の優先順位です。

ステップ 13	（任意） [**no**] **priority level** *<1-15>* 例： `switch(config-nbm-flow-pol-attr-prop)# priority level 1`	構成中のマルチキャスト グループの詳細なフロー優先順位を、レベル 1 ～ 15 で有効にします。デフォルト値は **low**で、これはゼロ（0）です。最も低いプライオリティでもあります。

例

次の例は、設定サンプルを示しています。

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

次のタスク

IPFM VRF の構成 （62 ページ）
IPFM フローの確立

IPFM VRF の構成

nbm feature コマンドを使用して IPFM を構成すると、システムはデフォルトの IPFM 仮想ルーティングおよび転送インスタンス (VRF) を自動的に作成します。カスタム IPFM VRF を構成することもできます。

IPFM VRF はファブリック レベルでマルチテナンシーをサポートし、複数の顧客がメディア インフラストラクチャに同じ IP ファブリックを同時に利用できるようにします。IPFM VRF はデフォルトの VRF から独立しており、既存のすべてのコマンドをサポートします。各 VRF には、独自のポリシー セットがあります。

アクティブまたはスタティック フロープロビジョニングを有効にするかどうかに応じて、PIM アクティブ モードまたは PIM パッシブ モードのいずれかにカスタム VRF を設定できます。これにより、IPFM ファブリックは、外部コントローラからの支援の有無にかかわらず、マルチキャスト フローを形成できます。

（注） すべての VRF を同じモードで設定する必要があります。

サポートされる IPFM VRF の数については、Cisco Nexus 9000 シリーズ NX-OS 確認済みスケーラビリティ ガイド、リリース 9.3(x) を参照してください。

アクティブ フロー プロビジョニングのための IPFM VRF の構成

アクティブ フロー プロビジョニング用に IPFM VRF を設定できます。これにより、IPFM ファブリックは、外部コントローラからの支援なしでマルチキャスト フローを形成できます。

始める前に

IPFM を構成します。

IPFM VRF を関連付ける前に、**vrf context** *vrf-name* コマンドを使用して VRF ルーティング コンテキストを作成し、ユニキャスト ルーティングと PIM 構成を完了します。

手順の概要

1. **configure terminal**
2. **no** [**nbm vrf** *vrf-name*]
3. **nbm mode pim-active**
4. （任意） [**no**] **nbm host-policy**
5. （任意） {**sender** | **receiver** | **pim**}
6. （任意） **default** {**permit** | **deny**}
7. （任意） 次のいずれかのコマンドを入力します。
   - 送信側ホスト ポリシーの場合：*sequence-number* **host** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
   - ローカル受信者ホスト ポリシーの場合：*sequence-number* **host** *ip-address* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
   - 外部受信者 (PIM) ホスト ポリシーの場合：*sequence-number* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
8. （任意） [**no**] **nbm reserve unicast fabric bandwidth** *value*
9. [**no**] **nbm flow asm range** [*group-range-prefixes*]
10. [**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**}

11. [**no**] **nbm flow dscp** *value*
12. （任意） [**no**] **nbm flow reserve-bandwidth receiver-only**
13. （任意） [**no**] **nbm flow policer**
14. [**no**] **nbm flow-policy**
15. [**no**] **policy** *policy-name*
16. （任意） [**no**] **policer**
17. [**no**] **bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**}
18. [**no**] **dscp** *value*
19. [**no**] **ip group-range** *ip-address* **to** *ip-address*
20. （任意） [**no**] **priority critical**
21. （任意） [**no**] **priority level** *<1-15>*

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**no** [**nbm vrf** *vrf-name*] 例： `switch(config)# nbm vrf nbm`	IPFM VRF を作成します。
ステップ 3	**nbm mode pim-active** 例： `switch(config)# nbm mode pim-active`	IPFM ファブリックが外部コントローラからの支援なしでマルチキャスト フローを形成できるようにします。 （注） カスタム IPFM VRF の PIM アクティブ モードを無効にすることはできません。IPFM VRF を PIM アクティブ モードから PIM パッシブ モードに変更することはできますが、VRF でカスタム設定を最初に削除した場合に限られます。もしくは、次の意味のエラーが表示されます。「IPFMは、カスタム設定が存在している間PIMパッシブ モードに設定することはできません。すべてのカスタムIPFM構成を削除し、再試行してください」。
ステップ 4	（任意） [**no**] **nbm host-policy** 例：	スイッチの IPFM ホスト ポリシーを設定します。

	コマンドまたはアクション	目的
	`switch(config)# nbm host-policy` `switch(config-nbm-host-pol)#`	

ステップ 5	（任意） {**sender** | **receiver** | **pim**}
	例：
	`switch(config-nbm-host-pol)# sender`
	`switch(config-nbm-host-pol-sender)#`
		送信者、ローカル受信者、または外部受信者(PIM)の IPFM ホスト ポリシーを構成します。
		（注）
		デフォルトの IPFM ホスト ポリシーを更新する前に、最初にカスタムホストポリシーを削除する必要があります。

ステップ 6	（任意） **default** {**permit** | **deny**} 例： `switch(config-nbm-host-pol-sender)# default permit`	IPFM ホスト ポリシーのデフォルト アクションを指定します。デフォルトでは、3種類のホストポリシーがすべて許可されます。

ステップ 7	（任意） 次のいずれかのコマンドを入力します。
	• 送信側ホスト ポリシーの場合：*sequence-number* **host** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
	• ローカル受信者ホスト ポリシーの場合：*sequence-number* **host** *ip-address* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
	• 外部受信者 (PIM) ホスト ポリシーの場合：*sequence-number* **source** *ip-address* **group** *ip-prefix* {**deny** | **permit**}
	例：
	`switch(config-nbm-host-pol-sender)# 10 host 101.1.1.3 group 229.1.1.1/32 deny`
	例：
	`switch(config-nbm-host-pol-rcvr)# 40 host 100.1.1.1 source 145.1.1.1 group 234.1.1.1/32 deny`
	例：
	`switch(config-nbm-host-pol-pim)# 50 source 101.1.1.1 group 235.1.1.1/32 deny`
		送信側または受信側のフローを許可するか拒否するかを指定します。
		送信側およびローカル受信側のホスト ポリシーのホスト IP アドレスには、ワイルドカード (0.0.0.0) を入力できます。以前のリリースでは、ホスト ポリシーをスイッチのインターフェイスに関連付けるために、ホストの IP アドレスが必要でした。ワイルドカードを使用すると、単一の設定を使用して、特定のグループまたはマスクでマルチキャスト トラフィックを送受信しているすべてのホストを検出できます。ホスト IP アドレスがローカル受信者ホスト ポリシーのワイルドカードである場合、ソース IP アドレスもワイルドカードです。この手順の最後にあるワイルドカード設定の例を参照してください。

ステップ 8	（任意） [**no**] **nbm reserve unicast fabric bandwidth** *value* 例： `switch(config)# nbm reserve unicast fabric bandwidth 2`	ユニキャスト フロー用にファブリック ポートの帯域幅の割合を予約します。IPFM フロー管理は、この帯域幅をフロー セットアップに使用せず、ユニキャスト トラフィック用にすべてのファブリック インターフェイスで予約します。範囲は 0 ～ 100% で、デフォルト値は 0 です。
ステップ 9	[**no**] **nbm flow asm range** [*group-range-prefixes*] 例：	*,G 結合の IPFM ASM グループ範囲をプログラムします。このグループ範囲内の IGMP 加入は、V2 加入または（*、G）加入であると予想されます。最

	コマンドまたはアクション	目的
	`switch(config)# nbm flow asm range 224.0.0.0/8 225.0.0.0/8 226.0.0.0/8 227.0.0.0/8`	大 20 のグループ範囲を設定できます。デフォルトでは、グループ範囲は構成されていません。 （注） このコマンドは、マルチスパイン展開でのみ必要です。
ステップ 10	[**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} 例： `switch(config)# nbm flow bandwidth 3000 mbps`	Kbps、Mbps、または Gbps でグローバル IPFM フロー帯域幅を設定します。サポートされる最小フロー帯域幅は 200 Kbps です。 範囲：1 ～ 25,000,000 Kbps / 1 ～ 25,000 Mbps / 1 ～ 25 Gbps デフォルト値：0 Kbps / 0 Mbps / 0 Gbps
ステップ 11	[**no**] **nbm flow dscp** *value* 例： `switch(config)# nbm flow dscp 10`	グローバル IPFM フロー DSCP 値を設定します。範囲は 0 ～ 63 です。いずれかのフローが IPFM フローグループ範囲と一致しない場合、デフォルトのフロー DSCP が帯域幅管理とフロー設定に使用されます。
ステップ 12	（任意）[**no**] **nbm flow reserve-bandwidth receiver-only** 例： `switch(config)# nbm flow reserve-bandwidth receiver-only`	RP に有効な受信者がないことを判断することにより、帯域幅使用率の最適化を有効にし、不要な RPF 帯域幅を解放します。（RP が FHR に向けて帯域幅を事前予約するのを防ぎます。） **no nbm flow reserve-bandwidth receiver-only** コマンドで帯域幅利用の最適化を無効にします。この機能はデフォルトで無効に設定されています。
ステップ 13	（任意）[**no**] **nbm flow policer** 例： `switch(config)# no nbm flow policer`	すべての IPFM フロー ポリシーのポリサーを有効または無効にします。ポリサーはデフォルトで有効になっています。

ステップ 14	[**no**] **nbm flow-policy**
	例：
	`switch(config)# nbm flow-policy`
	`switch(config-nbm-flow-pol)#`
		フローごとのフロー帯域幅を設定します。

ステップ 15	[**no**] **policy** *policy-name* 例：	IPFM フロー ポリシーを構成します。ポリシー名には最大63文字の英数字を指定できます。

	コマンドまたはアクション	目的
	`switch(config-nbm-flow-pol)# policy nbmflow10` `switch(config-nbm-flow-pol-attr)#`	
ステップ 16	（任意） [**no**] **policer** 例： `switch(config-nbm-flow-pol-attr)# no policer`	指定された IPFM フロー ポリシーのポリサーを有効または無効にします。 デフォルトでは、各送信元フローは送信元リーフでポリサーを使用します（最初のホップ ルータ）マルチキャスト送信元の数がポリサーの数を超えた場合、フローは送信元リーフで承認されません。動作をオーバーライドするには、フロー ポリシーでポリサーを無効にできます。ポリサーが無効になっている場合のフロー ポリシーに一致するフローは、ポリサー リソースが消費されません。 （注） 誤動作のエンドポイントにより許可されている以上の送信が発生した場合、ネットワークが保護されない状態を招く可能性があるため、注意深くこのコマンドを使用します。集約ポリサーなど別の方法を使用して、IPFM でプログラミングされているポリサーがないフローをレート制限します。集約ポリサーの詳細については、Cisco.com の『*Cisco Nexus 9000* シリーズ*NX-OS Quality of Service* 構成ガイド』の「ポリシングの構成」の章の「共有ポリサーの構成」のセクションを参照してください。
ステップ 17	[**no**] **bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} 例： `switch(config-nbm-flow-pol-attr)# bandwidth 10 mbps`	このポリシーに一致するマルチキャスト グループに、Kbps、Mbps、または Gbps でフロー帯域幅を設定します。サポートされる最小フロー帯域幅は 200 Kbps です。 **範囲** / **デフォルト値** 1 ～ 25,000,000 Kbps / 0 Kbps 1 ～ 25,000 Mbps / 0 Mbps 1 ～ 25 Gbps / 0 Gbps
ステップ 18	[**no**] **dscp** *value* 例： `switch(config-nbm-flow-pol-attr)# dscp 10`	指定されたグループ範囲に一致するフローの最初のホップの冗長性に、差別化サービス コード ポイント (DSCP) 値を設定します。
ステップ 19	[**no**] **ip group-range** *ip-address* **to** *ip-address* 例：	このポリシーに関連付けられているマルチキャスト グループの IP アドレス範囲を指定します。

	コマンドまたはアクション	目的
	`switch(config-nbm-flow-pol-attr)# ip group-range 224.19.10.1 to 224.19.255.1` `switch(config-nbm-flow-pol-attr)# ip group-range 224.20.10.1 to 224.20.255.1`	

ステップ 20	（任意）[**no**] **priority critical**
	例：
	`switch(config-nbm-flow-pol-attr-prop)# priority critical`
	`switch(config-nbm-flow-pol-attr-prop)#`
		設定されているマルチキャスト グループのクリティカル フローの優先順位付けを有効にします。**Critical** が最高の優先順位です。

ステップ 21	（任意）[**no**] **priority level** *<1-15>* 例： `switch(config-nbm-flow-pol-attr-prop)# priority level 1`	構成中のマルチキャスト グループの詳細なフロー優先順位を、レベル 1 ～ 15 で有効にします。デフォルト値は **low**で、これはゼロ（0）です。最も低いプライオリティでもあります。

次のタスク

IPFM フローの確立

静的フロー プロビジョニングのための IPFM VRF の構成

スタティック フロー プロビジョニング用に IPFM VRF を設定できます。これにより、IPFM ファブリックは、外部コントローラからの支援を受けてマルチキャスト フローを形成できます。

このモードでは、スイッチはフロー ポリシーやホスト ポリシーなどの IPFM 設定を受け入れることができません。スイッチはフロー ステッチの決定に参加せず、コントローラからの API 呼び出しに厳密に従います。さらに、スタティック フローはリロード時に保存されません。

フロープロビジョニングでエラーが発生した場合、スイッチはエラーを修正せず、設定を自動的に再試行しません。

始める前に

IPFM を構成します。

IPFM VRF を関連付ける前に、**vrf context** *vrf-name* コマンドを使用して VRF ルーティング コンテキストを作成し、ユニキャスト ルーティングと PIM 構成を完了します。

IPFM VRF を PIM アクティブ モードから PIM パッシブ モードに変更することはできますが、VRF でカスタム設定を最初に削除した場合に限られます。もしくは、次の意味のエラーが表示されます。「IPFM は、カスタム設定が存在している間 PIM パッシブ モードに設定することはできません。すべてのカスタム IPFM 構成を削除し、再試行してください」。

手順の概要

1. **configure terminal**
2. **no** [**nbm vrf** *vrf-name*]

3. **nbm mode pim-passive**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	**no** [**nbm vrf** *vrf-name*] 例： `switch(config)# nbm vrf nbm`	IPFM VRF を作成します。
ステップ 3	**nbm mode pim-passive** 例： `switch(config)# nbm mode pim-passive`	IPFM ファブリックが外部コントローラからの支援によりマルチキャスト フローを形成できるようにします。

次のタスク

API の詳細については、『Cisco Nexus NX-API リファレンス』を参照してください「

IPFM サブインターフェイス タイプの構成

Cisco NX-OS リリース 10.3(2)F 以降では、サブインターフェイスの帯域幅も管理できる IPFM を備えたサブインターフェイスがサポートされています。これは、PIM アクティブ/PIM パッシブ IPFM モードの両方のサブインターフェイス ホスト/ファブリック ポートに適用されます。

親ポートとそのサブインターフェイスの合計帯域幅キャパシティ % は 100% を超えてはなりません。デフォルトでは、親ポートには 100% の帯域幅キャパシティが割り当てられます。サブインターフェイスに容量を設定するには、親インターフェイスにキャパシティ % を最初に構成する必要があります。

帯域幅キャパシティの予約をプロビジョニングするために、対応する構成モデル オブジェクト (MO) が提供されます。

帯域幅キャパシティの予約に加えて、既存の IPFM インターフェイス設定もサブインターフェイスでサポートされます。

（注） **nbm bandwidth capacity** コマンドは、PIM アクティブ モードの IPFM VRF にのみ適用されます。PIM パッシブ VRF では、ブロードキャスト コントローラが帯域幅管理を行います。

- ポートごとのユニキャスト帯域幅の予約設定
- `nbm external-link`

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します

ステップ 2	**interface** *interface-type slot/port*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**[no] nbm bandwidth capacity** *percentage* 例： `switch(config-subif)# nbm bandwidth capacity 1`	IPFMサブインターフェイスの帯域幅を構成します。パーセンテージの範囲は 0 ～ 100 です。0 は、このリンクのIPFM帯域幅の予約がないことを示します。 IPFM 帯域幅を構成解除するには、 **no nbm bandwidth capacity** を使用します。 を実行する前に、ユーザ名がフィギュレーション ファイルに指定されていることを確認してください。
ステップ 4	**[no] nbm bandwidth unicast** *percentage* 例： `switch(config-subif)# nbm bandwidth unicast 10`	ユニキャストの帯域幅を構成します。パーセンテージの範囲は 0 ～ 100 です。0 は、このリンクのユニキャスト帯域幅の予約がないことを示します。 ユニキャスト帯域幅を構成解除するには、 **no nbm bandwidth unicast** を使用します。 コマンドを使用します。

フローの確立 (オプション)

IPFM フロー定義を作成するか、IGMP 静的 OIF を構成することにより、フローを確立できます。IPFM フロー定義を構成することをお勧めします。

IPFM フロー定義の作成

IPFM フロー定義を作成することにより、IPFM フローを確立できます。

IPFM は CLI と API を公開して、受信者にフローをプロビジョニングします。これは、IGMP を使用しない場合です。次の図に示すように、ネットワーク帯域幅を事前に予約するために、受信者リーフに至るまでフローをプログラムするか、出力インターフェイスを指定して、リーフ スイッチにトラフィックを受信者に送信するように指示できます。

図 *1* : 送信元からリーフへのトラフィック

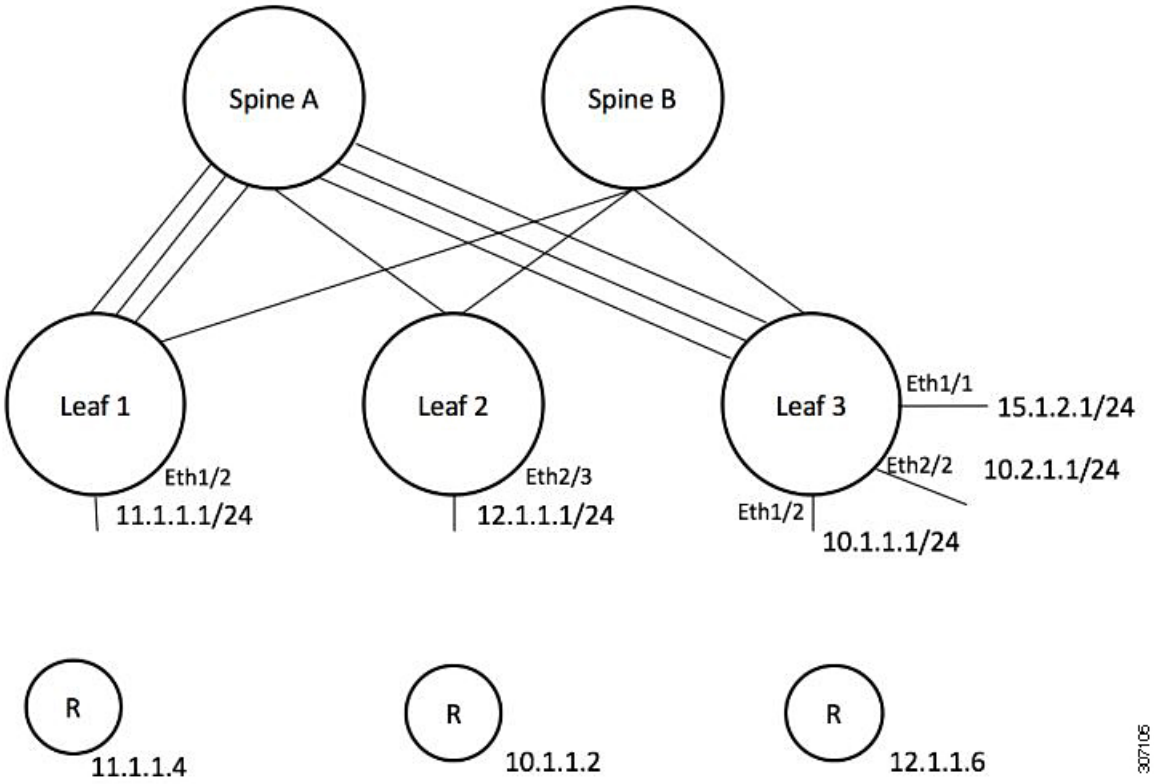
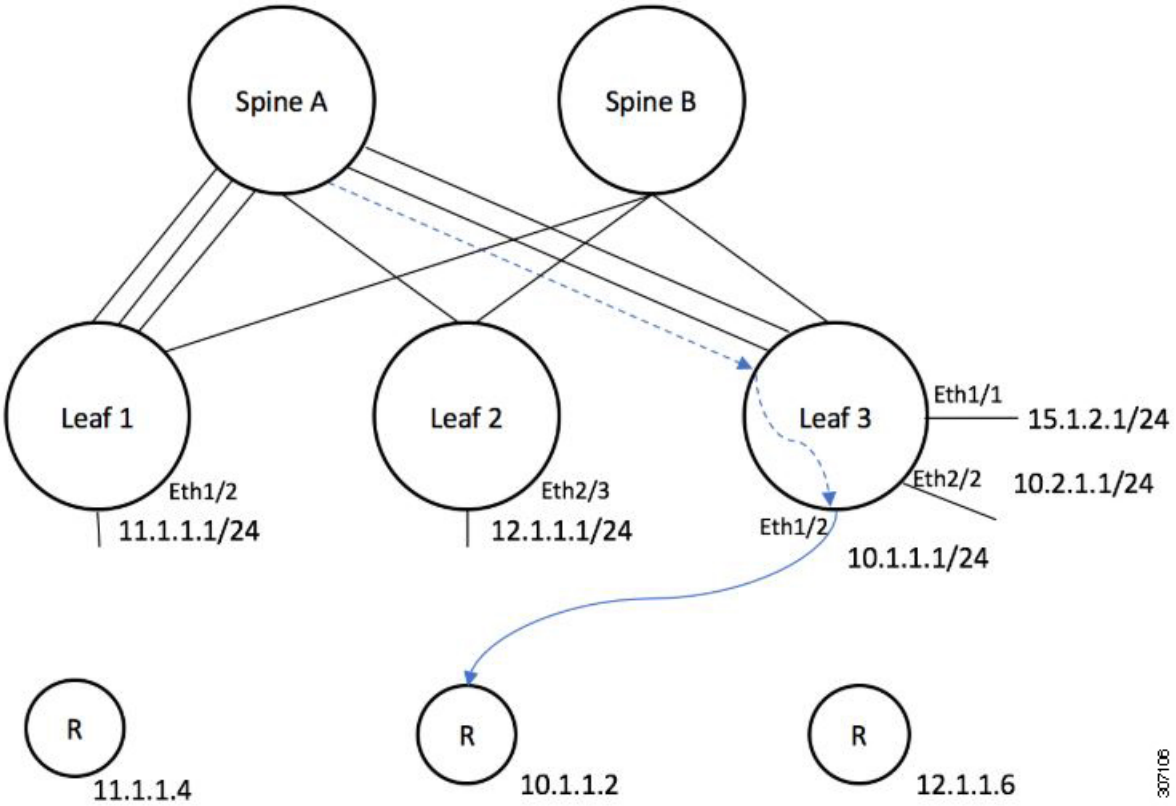


図 *2:* リーフから受信者へのトラフィック



始める前に

IPFM を有効にします。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します

ステップ 2	[**no**] *group* nbm flow-definition[*source]*
	例：
	`switch(config)# nbm flow-definition 235.1.1.13 100.1.1.40`
	`switch(config-nbm-flow-def)#`
	例：
	`switch(config)# nbm flow-definition 235.1.1.10 0.0.0.0`
	`switch(config-nbm-flow-def)#`
		IPFM フロー定義を構成します。

ステップ 3	（任意） [**no**] **stage-flow** 例： `switch(config-nbm-flow-def)# stage-flow`	送信元からスイッチに至るまでフローをもたらします。
ステップ 4	（任意） [**no**] **egress-interface** *interface* 例： `switch(config-nbm-flow-def)# egress-interface ethernet 1/3`	指定されたインターフェイスからフローを転送します。
ステップ 5	（任意） [**no**] **egress-host** *reporter-ip-address* 例： `switch(config-nbm-flow-def)# egress-host 10.10.10.1`	指定された受信者にフローを転送します。

例

次の例は、設定サンプルを示しています。

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

```
  egress-host 145.1.1.29
nbm flow-definition 225.0.0.11 100.1.1.40
  stage-flow
  egress-interface ethernet 1/4
  egress-host 100.1.1.21
nbm flow-definition 235.1.1.13 100.1.1.40
  stage-flow
  egress-interface vlan 12
  egress-host 101.1.1.11
  egress-host 101.1.1.12
  egress-host 101.1.1.13
  egress-host 101.1.1.14
```

IGMP スタティック OIF の設定

スタティック IGMP OIF を設定することでフローを確立できますが、静的 IGMP OIF を構成するのではなく、IPFM フロー定義を作成することをお勧めします。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します

ステップ 2	**interface** *interface-type slot/port*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **ip igmp static-oif** *group* [**source** *source*] 例： `switch(config-if)# ip igmp static-oif 230.0.0.0`	指定されたマルチキャスト グループのフローを確立します。 （注） このコマンドは、**route-map** オプションをサポートしません。

ポートごとのユニキャスト帯域幅の予約設定

ユニキャスト帯域幅 (BW) は、現在、ファブリック レベルでのみ管理されています。ポートごとにユニキャスト用に帯域幅を細かく予約する規定はありません。マルチサイト シナリオの場合、ポートごとのユニキャスト帯域幅を管理できる設定ノブが必要です。展開された新しい設定ノブは、ポートごとにユニキャスト帯域幅を予約します。ユニキャスト帯域幅予約をプロビジョニングするために、対応する構成モデル オブジェクト (MO) が提供されます。

ポートごとのユニキャスト BW パーセンテージ（%）予約を設定すると、スイッチは、入力方向と出力方向の両方でユニキャスト用に確保する帯域幅を確認します。十分な帯域幅が利用可能で、一方向または両方向のいずれかが設定されたパーセンテージを満たしている場合、スイッチはユニキャスト使用のために帯域幅をすぐに予約します。設定された割合がいずれかの方向で利用できない場合、スイッチはユニキャストの目的で部分的な予約を行います。その後、マルチキャスト フローがティアダウンすると、スイッチは解放された帯域幅をユニキャスト目的に再利用し、設定された割合に達するまで継続します。

ユニキャスト BW のポート単位の % 予約設定は、vrf ファブリック単位のユニキャスト BW 予約よりも常に優先されます。ポートごとの設定が削除され、リンクに Cisco Discovery Protocol（CDP）ネイバーが確立されている場合、スイッチは vrf ファブリックごとのユニキャスト BW パーセンテージを使用します。リンクでポートごとの値を 0 に設定すると、そのリンクでユニキャストが予約されないことを示します。これは、リンクに CDP ネイバーが確立されていて、vrf ごとのファブリック ユニキャスト BW % が設定されている場合に可能です。スイッチが VRF ごとのファブリック ユニキャスト BW % を使用して予約するには、リンクのポートごとの % BW 予約を削除します。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します

ステップ 2	**interface** *interface-type slot/port*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 3	**[no] nbm unicast bandwidth percentage**
	例：
	`switch(config-if)# nbm bandwidth unicast ?`
	`<0-100> Percentage value`
	`switch(config-if)# no nbm bandwidth unicast`
		0 は、このリンクでのユニキャストの予約がないことを示します。
		ユニキャスト BW の構成を解除するには、**no nbm bandwidth unicast** を使用します。

マルチサイトの設定

メディアの IP ファブリックは、送信側が 1 つのサイトにあり、受信側が別のサイトにある複数のサイト間で信頼できる通信チャネルを提供します。一部の外部(またはホスト側)インターフェイスを外部リンクとして構成し、それらのリンクに外部デバイスを接続して、マルチサイトソリューションを作成できます。一部のインターフェイスを外部リンクとして設定することにより、ソリューションはそれらのインターフェイスで帯域幅管理を実行できます。PIM アクティブモードで実行されているスイッチは、すべてのスイッチで実行されている分散帯域幅管理アルゴリズムを使用してファブリック帯域幅を管理します。

始める前に

スパイン リーフ トポロジまたは単一のモジュラ スイッチの IPFM を構成します。

サイト全体で ASM フローをサポートするには、サイト間の RP 間でフル メッシュ MSDP を有効にする必要があります。構成情報については、MSDP の設定を参照してください。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	[**no**] **feature nbm** 例：	IPFM 機能を有効にします。この機能を無効にするには、このコマンドの **no** 形式を使用します。

	コマンドまたはアクション	目的
	`switch(config)# feature nbm`	
ステップ 3	**ip pim sparse mode** 例： `switch(config)# ip pim sparse mode`	IPFM 外部リンクで PIM を設定します。

ステップ 4	**interface** *interface-type slot/port*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを指定します。インターフェイス コンフィギュレーション モードを開始します。

ステップ 5	**nbm external-link** 例： `switch(config-if)# nbm external-link`	マルチサイト ソリューションで複数のファブリックを接続するために、IPFM インターフェイスを外部リンクとして設定します。

マルチキャストおよびユニキャスト フローの有効化 (オプション)

メディアの IP ファブリックは、ユニキャスト フローだけでなくマルチキャストにも使用できます。マルチキャスト トラフィックをプライオリティ キュー (7) に割り当て、ユニキャスト トラフィックをデフォルト キュー (0) に割り当てることができます。この設定により、ユニキャスト トラフィックがマルチキャスト トラフィックを輻輳させないことが保証されます。

（注） スパイン スイッチの場合、トラフィック分類はアクセス コントロール リスト (ACL) と差別化サービス コードポイント（DSCP）の値に基づいています。送信側リーフ スイッチの場合、分類とマーキングは NDFC からのフロー プログラミング（S、G）に基づいています。

始める前に

次のコマンドを使用して、すべてのスイッチ（-R ライン カードを備えた Cisco Nexus 9504 および 9508 スイッチを除く）で TCAM カービングを設定し、設定を保存して、スイッチをリロードします。

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

（注） 上記の TCAM サイズを推奨しますが、ネットワーク要件に合わせて値を調整できます。ACL TCAM リージョンの詳細については、『Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイド』を参照してください。

手順の概要

1. **configure terminal**
2. **ip access-list** *acl-name*
3. *sequence-number* **permit** *protocol source destination*
4. **exit**
5. **ip access-list** *acl-name*
6. *sequence-number* **permit** *protocol source destination*
7. **exit**
8. **class-map type qos match-all** *unicast-class-name*
9. **match access-group name** *acl-name*
10. **exit**
11. **class-map type qos match-any** *multicast-class-name*
12. **match access-group name** *acl-name*
13. **exit**
14. **policy-map type qos** *policy-map-name*
15. **class** *unicast-class-map-name*
16. **set qos-group 0**
17. **exit**
18. **class** *multicast-class-map-name*
19. **set qos-group 7**
20. **exit**
21. **exit**
22. **interface ethernet** *slot/port*
23. **service-policy type qos input** *policy-map-name*
24. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ip access-list** *acl-name*
	例：
	`switch(config)# ip access-list pmn-ucast`
	`switch(config-acl)#`
		IP ACL を作成し、IP ACL 設定モードを開始します。

	コマンドまたはアクション	目的

ステップ 3	*sequence-number* **permit** *protocol source destination*
	例：
	`switch(config-acl)# 10 permit ip any 0.0.0.0/1`
	`switch(config-acl)# 20 permit ip any 128.0.0.0/2`
	`switch(config-acl)# 30 permit ip any 192.0.0.0/3`
		すべてのユニキャスト IP アドレス（クラス A、B、および C）に一致するルールを IP ACL に作成します。

ステップ 4	**exit**
	例：
	`switch(config-acl)# exit`
	`switch(config)#`
		IP ACL 設定モードを終了します。

ステップ 5	**ip access-list** *acl-name*
	例：
	`switch(config)# ip access-list pmn-mcast`
	`switch(config-acl)#`
		IP ACL を作成し、IP ACL 設定モードを開始します。

ステップ 6	*sequence-number* **permit** *protocol source destination* 例： `switch(config-acl)# 2 permit ip any 224.0.0.0/4`	すべてのマルチキャスト フローに一致するルールを作成します。

ステップ 7	**exit**
	例：
	`switch(config-acl)# exit`
	`switch(config)#`
		IP ACL 設定モードを終了します。

ステップ 8	**class-map type qos match-all** *unicast-class-name*
	例：
	`switch(config)# class-map type qos match-all pmn-ucast`
	`switch(config-cmap-qos)#`
		ユニキャスト トラフィックのクラス マップを作成し、class-map configuration モードを開始します。

ステップ 9	**match access-group name** *acl-name* 例： `switch(config-cmap-qos)# match access-group name pmn-ucast`	ユニキャスト トラフィックの ACL に基づいてパケットを照合することによって、トラフィック クラスを設定します。

ステップ 10	**exit**
	例：
	`switch(config-cmap-qos)# exit`
	`switch(config)#`
		クラスマップ コンフィギュレーション モードを終了します。

ステップ 11	**class-map type qos match-any** *multicast-class-name* 例：	マルチキャスト トラフィックのクラス マップを作成し、class-map 設定モードを開始します。

	コマンドまたはアクション	目的
	`switch(config)# class-map type qos match-any pmn-mcast` `switch(config-cmap-qos)#`	
ステップ 12	**match access-group name** *acl-name* 例： `switch(config-cmap-qos)# match access-group name pmn-mcast`	マルチキャスト トラフィックの ACL に基づいてパケットを照合することによって、トラフィック クラスを設定します。

ステップ 13	**exit**
	例：
	`switch(config-cmap-qos)# exit`
	`switch(config)#`
		クラスマップ コンフィギュレーション モードを終了します。

ステップ 14	**policy-map type qos** *policy-map-name*
	例：
	`switch(config)# policy-map type qos pmn-qos`
	`switch(config-pmap-qos)#`
		ポリシーマップを作成し、ポリシーマップ コンフィギュレーション モードを開始します。

ステップ 15	**class** *unicast-class-map-name*
	例：
	`switch(config-pmap-qos)# class pmn-ucast`
	`switch(config-pmap-c-qos)#`
		ユニキャスト トラフィックのクラスを作成し、policy-map class configuration モードを開始します。

ステップ 16	**set qos-group 0** 例： `switch(config-pmap-c-qos)# set qos-group 0`	QoS グループ値を設定し、IPFM ユニキャストクラスマップへのトラフィックの分類に一致します。

ステップ 17	**exit**
	例：
	`switch(config-pmap-c-qos)# exit`
	`switch(config-pmap-qos)#`
		ポリシーマップ クラス コンフィギュレーション モードを終了します。

ステップ 18	**class** *multicast-class-map-name*
	例：
	`switch(config-pmap-qos)# class pmn-mcast`
	`switch(config-pmap-c-qos)#`
		マルチキャスト トラフィックのクラスを作成し、policy-map class 設定モードを開始します。

ステップ 19	**set qos-group 7** 例： `switch(config-pmap-c-qos)# set qos-group 7`	QoS グループ値を設定し、IPFM マルチキャスト クラスマップへのトラフィックの分類に一致します。

ステップ 20	**exit**
	例：
	`switch(config-pmap-c-qos)# exit`
	`switch(config-pmap-qos)#`
		ポリシーマップ クラス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的

ステップ 21	**exit**
	例：
	`switch(config-pmap-qos)# exit`
	`switch(config)#`
		ポリシーマップ コンフィギュレーション モードを終了します。

ステップ 22	**interface ethernet** *slot/port*
	例：
	`switch(config)# interface ethernet 1/49`
	`switch(config-if)#`
		インターフェイスを作成して、インターフェイス コンフィギュレーション モードを開始します。このコマンドは、ファブリック インターフェイスにのみ使用する必要があります。

ステップ 23	**service-policy type qos input** *policy-map-name* 例： `switch(config-if)# service-policy type qos input pmn-qos`	policy-map 名をインターフェイスの入力パケットに追加します。
ステップ 24	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

例

設定例：

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

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

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

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

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

IPFM 構成の確認

IPFM 構成情報を表示するには、次のいずれかの操作を行います。

コマンド	説明
show ip mroute *group-address*	指定したグループの IP マルチキャスト ルーティング テーブルを表示します。
show nbm defaults [**vrf** {**all** | *vrf-name*}]	IPFM のデフォルト フロー ポリシー、ホスト ポリシー、およびユニキャスト ファブリック帯域幅を表示します。
show nbm flow-policy [*policy-name*] [**vrf** {**all** | *vrf-name*}]	設定されているすべてのカスタム フローポリシーまたは特定のカスタム フローポリシーのマルチキャスト範囲、帯域幅、DSCP、およびQoSを表示します。
show nbm flows [[**group-based** [**group** *group-ip*] | **source** *source-ip* [**group** *group-ip*] | **group** *group-ip* [**source** *source-ip*] | **flow-policy** *pol-name* | **interface** *if-name*] [**all** | **active** | **inactive** | no-**receiver**] [**detail**] [**vrf** {*vrf-name* | **all**}]	すべてのデフォルトおよびカスタム フローポリシーについて、スイッチ上のアクティブなフローを表示します。オプションのキーワードを追加して、出力を絞り込むことができます。
show nbm flows static [[**group** *group-ip*] | **source** *source-ip*] **priority** | **stitched** | **unstitched** [**all** | **critical** | **level** | **low**]] | [**vrf** {**all** | *vrf-name*}]]	IPFM フロー定義の静的フローを表示します。オプションのキーワードを追加して、出力を絞り込むことができます。
show nbm flows static [**vrf** {**all** | *vrf-name*}]	IPFM フロー定義の静的フローを表示します。
show nbm flows static group *group-address*	指定されたグループの IPFM フロー定義のスタティック フローを表示します。
show nbm flows statistics [**group-based** [**group** *group-ip*] | **source** *source-ip* [**group** *group-ip*] | **group** *group-ip* [**source** *source-ip*] | **flow-policy** *pol-name* | **interface** *if-name*] [**vrf** {**all** | *vrf-name*}]	IPFM フロー統計情報を表示します。 このコマンドは、送信側が接続されているファースト ホップ ルータ、またはフローがファブリックに入るスイッチで有効です。

show nbm flows summary [**vrf** {**all** | *vrf-name*}]	IPFM フローの要約を表示します。
show nbm host-policy {**all** {**receiver external** | **receiver local** | **sender**} | **applied** {**receiver external** | **receiver local** {**all** | **interface** *type slot/port* | **wildcard**} | **sender** {**all** | **interface** *type slot/port* | **wildcard**}}} [**vrf** {**all** | *vrf-name*}]	すべての IPFM ホスト ポリシーまたは外部受信者 (PIM)、ローカル受信者、または送信者に適用される IPFM ホスト ポリシーを表示します。
show nbm interface bandwidth	IPFM インターフェイスの帯域幅を表示します。
show running-config nbm	IPFM の実行構成情報を表示します。

（注） **vrf** *vrf-name* オプションを使用して VRF を指定しない場合、これらのコマンドは、現在のルーティング コンテキストの出力を表示します。ルーティング コンテキストは、**vrf context** *vrf-name* コマンドを使用して設定できます。

コマンド出力の例については、**show**Show コマンドのサンプル出力 （189 ページ） を参照してください。

IPFM フロー統計のクリア

IPFM フロー統計をクリアするには、次のタスクのいずれかを実行します。

clear nbm flow statistics
`switch# clear nbm flows statistics`
`Clearing all NBM flow statistics for all VRFs ...`
`Done.`
	すべての VRF の IPFM フロー統計をクリアします。

clear nbm flow statistics [**source** *source-ip* [**group** *group-ip*] | **group** *group-ip* [**source** *source-ip*]] [**vrf** {**all** | *vrf-name*}]
`switch# clear nbm flows statistics vrf red`
`Clearing all NBM flow statistics for VRF 'red'...`
`Done.`
 	
`switch# clear nbm flows statistics vrf all`
`Clearing all NBM flow statistics for all VRFs ...`
`Done.`
	現在のルーティング コンテキストに関連付けられている VRF の IPFM フロー統計をクリアします。
	（注）
	-R ライン カードを搭載した Cisco Nexus 9504 および 9508 スイッチのみが **source**、**group**、および **vrf** オプションをサポートします。

ユニキャスト PTP ピアの設定

マスターとスレーブの両方のユニキャスト PTP ピアを設定する必要があります。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **ptp transport ipv4 ucast** {**master** | **slave**}
4. {**master** | **slave**} **ipv4** *ip-address*
5. **ptp ucast-source** *ip-address*
6. （任意） **show ptp brief**
7. （任意） **show ptp counters interface ethernet** *slot/port* **ipv4** *ip-address*
8. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	**interface ethernet** *slot/port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		ユニキャストPTPを有効にするインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**ptp transport ipv4 ucast** {**master**	**slave**} 例： `switch(config-if)# ptp transport ipv4 ucast master`	マスターまたはスレーブのユニキャストPTPピアを設定します。
ステップ 4	{**master**	**slave**} **ipv4** *ip-address* 例： `switch(config-if)# slave ipv4 81.0.0.2`	マスターまたはスレーブ ユニキャスト ピアの IP アドレスを指定します。
ステップ 5	**ptp ucast-source** *ip-address* 例： `switch(config-if)# ptp ucast-source 81.0.0.1`	PTP ユニキャスト送信元の IP アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 6	（任意） **show ptp brief** 例： `switch(config-if)# show ptp brief`	PTP のステータスを表示します。
ステップ 7	（任意） **show ptp counters interface ethernet** *slot/port* **ipv4** *ip-address* 例： `switch(config-if)# show ptp counters interface ethernet 1/1 ipv4 81.0.0.2`	ユニキャスト PTP カウンタを表示します。
ステップ 8	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

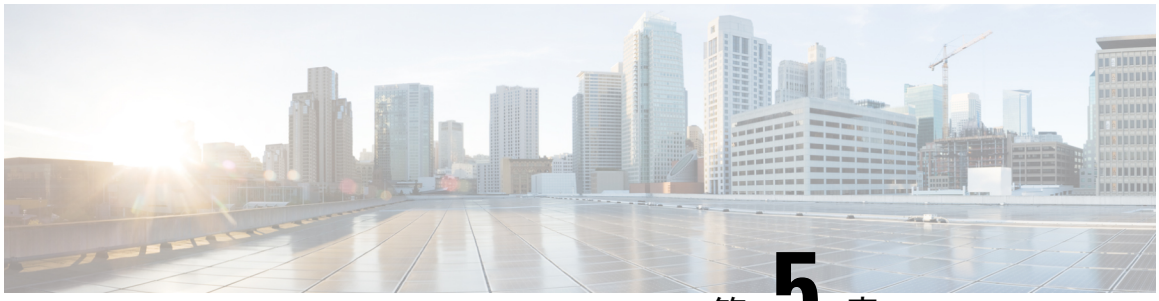
例

次の例は、マスターとスレーブのユニキャスト PTP ピアを設定する方法を示しています。

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

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

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

vPC のサポート

Cisco NX-OS リリース 10.3(1)F 以降、vPC は機能 IPFM でサポートされます。



第 5 章

メディア フロー分析の設定

この章には、メディア ソリューション向けのシスコの IP ファブリックのメディア フロー分析に関する情報が含まれています。

RTP フロー モニタリング

リアルタイム トランスポート プロトコル（RTP）は、IP ネットワークを介して音声とビデオをお届けするネットワーク プロトコルです。ストリーミング メディアのエンド ツー エンドのリアルタイム転送用に設計されています。このプロトコルは、IP ネットワークでの UDP 送信中に一般的なジッタ補正とパケット損失の検出のための機能を提供します。

RTP フロー モニタリングは、スイッチ上の RTP フローをキャッシュし、RTP フレームの損失を示す RTP シーケンス番号のギャップを検出します。この情報は、損失が発生している場所を特定するのに役立ち、ハードウェア リソースをより適切に計画できるようになります。

RTP フロー モニタリングの注意事項と制限事項

次の注意事項と制限事項は RTP フロー モニタリングに適用されます。

- Cisco Nexus 9300-FX、9300-FX2 および 9300-FX3 プラットフォーム スイッチは RTP フロー モニタリングをサポートします。

  さらに、Cisco NX-OS 9.3(6) 以降、Cisco Nexus 9300-GX プラットフォーム スイッチは RTP フロー モニタリングをサポートします。

- RTP フロー モニタリングが最初の ACL で構成され、別の ACL に変更された場合は、コマンドの `no flow rtp` 形式で RTP 構成を削除してから、必要な ACL で再構成する必要があります。

- RTP フロー モニタリング用に UDF を構成した後、スイッチを再起動する必要があります。
- RTP フロー モニタリング UDF は 1 つだけ設定できます。
- RTP フロー モニタリング UDF は、最初の UDF である必要があります。
- 従来の NetFlow モニターと RTP フロー モニタリングは、スイッチ上で共存できません。
- Cisco Nexus 9300-GX2、H2R、H1、および 9408 シリーズ スイッチでは、マルチキャスト RTP フロー モニタリングの最適化は次のシナリオでサポートされません。
  - PIM が有効になっているポートチャネルが設定されている場合
  - SVI が設定されている場合

RTP フロー モニタリングの設定

Cisco Nexus 9300-FX、9300-FX2、および 9300-FX3 プラットフォーム スイッチの RTP フロー モニタリングを構成できます。

さらに、Cisco NX-OS 9.3(6) 以降、Cisco Nexus 9300-GX プラットフォーム スイッチの RTP フロー モニタリングを設定できます。

始める前に

udf netflow_rtp netflow-rtp コマンドを使用して RTP フロー モニタリングの UDF を有効にし、実行コンフィギュレーションをスタートアップにコピーして、スイッチを再起動します。RTP フロー モニタリング UDF が最初の UDF であることを確認してください。

手順の概要

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

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	[**no**] **feature netflow** 例： `switch(config)# feature netflow`	スイッチ上で RTP フロー モニタリングをグローバルに有効にします。

ステップ 3	（任意） **ip access-list** *acl*
	例：
	`ip access-list ipv4-test-acl`
	`  10 permit ip any 224.0.1.39/32`
	`  20 permit ip any 224.0.1.40/32`
		特定のトラフィックをフィルタリングするように ACL ポリシーを設定します。

ステップ 4	[**no**] {**ip** | **ipv6**} **flow rtp** [*acl*]
	例：
	`switch(config)# ip flow rtp`
		IPv4 または IPv6 フローの RTP フロー モニタリングを有効にします。
		• このコマンドは、システム全体のアクセス コントロール リスト (ACL) を作成して、16384 ～ 32767 の UDP ポート範囲をフィルタリングします。この範囲は、RTP トラフィックの RFC 標準 UDP ポート範囲です。
		（注）
		この **ignore routable** コマンドは、マルチキャスト トラフィックをフィルタリングします。
		`switch(config)# show ip access-list`
		`IP access list nfm-rtp-ipv4-acl`
		`  ignore routable`
		`  10 permit udp any any range 16384 32767`
		（注）
		コマンドで ACL を指定すると、指定した ACL に一致するトラフィックだけが RTP フローとして報告されます。
		`switch(config)# ip flow rtp ipv4-test-acl`

RTP フローとエラーの表示

RTP フローとエラーを表示するには、次のいずれかのタスクを実行します。

show flow rtp details	すべての IPv4 および IPv6 RTP フローを表示します。
show flow rtp details {**ipv4** | **ipv6**}	IPv4 または IPv6 RTP フローを表示します。

show flow rtp errors active	現在損失が発生しているすべての RTP フローの詳細を表示します (過去 10 秒以内の少なくとも 1 つの更新間隔でパケット損失が検出された場合)。アクティブな損失ウィンドウの損失統計も表示されます。損失ウィンドウはまだアクティブであると見なされるため、損失の終了時刻は「N/A」と表示されます。
show flow rtp errors history	過去 1000 件の過去の損失ウィンドウの詳細を (新しい順に) 表示し、それぞれのフローの詳細を表示します。

次の例は、**show flow rtp details** コマンドのサンプル出力を示しています。

```
RTP Flow timeout is 1440 minutes
IPV4 Entries
SIP      DIP      BD ID S-Port D-Port Intf/Vlan Name  Packet Count BytesPerSec  FlowStart
50.1.1.2 20.1.1.2 4151  16385  17999  Ethernet1/49/1  269207033    594468000    00:21:16
 PST Apr 07 2019
20.1.1.2 50.1.1.2 4100  16385  18999  port-channel500 2844253      199000       00:21:59
 PST Apr 07 2019

IPv6 Entries
SIP         DIP    BD ID S-Port D-Port Intf/Vlan Name   Packet Count BytesPerSec FlowStart
20::2        50::2  4100  30000  31999  port-channel500  2820074      199000      00:22:04
 PST Apr 07 2019
50::2        20::2  4151  30000  31999  Ethernet1/49/1   3058232      199000      00:21:16
 PST Apr 07 2019
```

次の例は、**show flow rtp errors active** コマンドのサンプル出力を示しています。

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

（注） RTP フローが「アクティブ エラー」状態になると、次の syslog メッセージが表示されます。

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

次の例は、**show flow rtp errors history** コマンドのサンプル出力を示しています。

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

（注） RTP フローが「アクティブ エラー」状態でなくなると、次の syslog メッセージが表示されます。

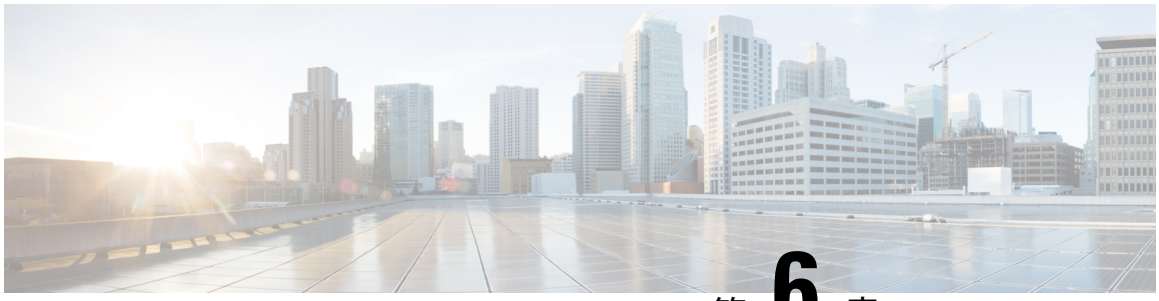
```
%NFM-1-RTP_FLOW_ERROR_STOP: Flow SIP: 30.30.1.2 DIP: 20.20.1.2 Interface: Ethernet1/98
loss no longer detected
```

RTP フローのクリアリング

RTP フローをクリアするには、次のタスクのいずれかを実行します。

clear flow rtp detail	すべての RTP フローと損失履歴をクリアします。
clear flow rtp detail {**ipv4** | **ipv6**}	IPv4 または IPv6 RTP フローと損失履歴をクリアします。

[**no**] **flow rtp timeout** *value* 例： `switch(config)# flow rtp timeout 100`	**show rtp details**, **show flow rtp errors active** および **show flow rtp errors history** テーブルから非アクティブな RTP フローをクリアします。 デフォルト値は 1440 分（24 時間）で、範囲は 0 ～ 1440 分です。値 0 は、RTP フローがクリアされないようにします。 （注） このコマンドは、アクティブな RTP フローをクリアしません。



第 6 章

IPFM を使用したマルチキャスト サービス リフレクションの設定

この章では、Cisco の IPFM を使用したマルチキャスト サービス リフレクションに Cisco Nexus 9000 シリーズ スイッチを設定する方法について説明します。

IPFM を使用したマルチキャスト サービス リフレクション

IPFM を使用したマルチキャスト サービス リフレクション機能は、外部で受信したマルチキャスト宛先アドレスを組織の内部アドレッシング ポリシーに準拠したアドレスに変換できます。これは、入力マルチキャスト ストリーム (S1、G1) から出力 (S2、G2) インターフェイスへのマルチキャスト ネットワーク アドレス変換 (NAT) です。この機能は、一般にマルチキャスト サービス リフレクション機能 (SR 機能) と呼ばれます。送信元 IP アドレスのみを変換する IP マルチキャスト ネットワーク アドレス変換（NAT）とは異なり、マルチキャスト サービス リフレクションは送信元と宛先アドレスの両方を返還します。

S1、G1 として着信するフローは S2、G2 に変換され、宛先 MAC アドレスは G2 のマルチキャスト MAC アドレスに書き換えられます。

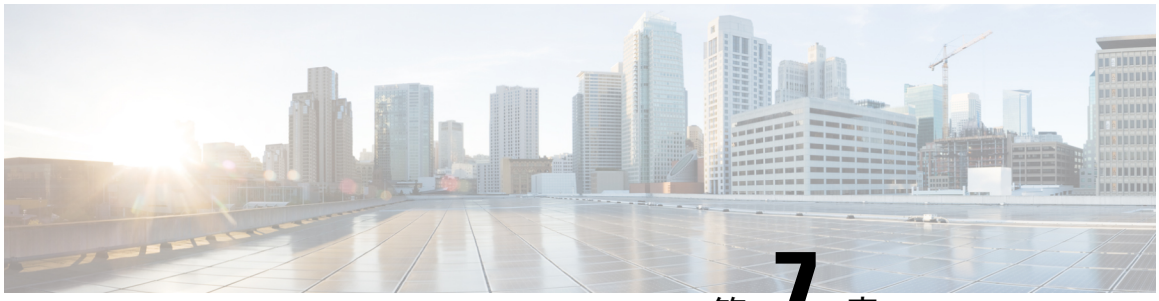
S1、G1 フローは S2、G2 に変換され、宛先 MAC アドレスは書き換えられず、グループ G1 に対応したままになります。

マルチキャスト サービス リフレクション機能に関する詳細とコマンドについては、『Cisco Nexus 9000 シリーズ NX-OS マルチキャスト ルーティング設定ガイド』を参照してください。

（注） 必要な帯域幅が利用できないなど、トラフィック フローをサポートできないと IPFM が判断した場合、トラフィック フローは停止し、IPFM が要求された変換をサポートできないことを示すアラートが発行されます。

（注） IPFM を使用したマルチキャスト サービス リフレクションは、Cisco Nexus 9316D-GX、Cisco Nexus 9364C-GX、Cisco Nexus 93600CD-GX、および Cisco Nexus 93180YC-FX3S スイッチ (Cisco Nexus NX-OS 9.3(5) 以降のリリース) でサポートされています。

（注） Cisco Nexus リリース 10.1(1) 以降、IPFM を使用したマルチキャスト サービス リフレクションは、Cisco Nexus 9300-FX3、Cisco Nexus C9316D-GX、Cisco Nexus C93600CD-GX、および Cisco Nexus C9364C-GX プラットフォーム スイッチでサポートされます。



第 7 章

非ブロッキング マルチキャスト サービス リフレクション

NAT 注意事項と制限事項

IPFM サービス リフレクション機能には、次の注意事項と制限事項があります。

- Cisco NX-OS リリース 10.2(3)F 以降では、ユニキャストからマルチキャスト NAT、マルチキャストからユニキャスト NAT、マルチキャストからマルチキャスト NAT、および出力 NAT がデフォルト以外の VRF でサポートされています。
- NAT 構成が存在する場合、構成のロールバックはサポートされません（失敗します）。
- 場合によっては、サービスインターフェイスの再構成が拒否され、それを変更するには、特定のシーケンスが必要になる場合があります。また、再構成後、NAT ルールが自動的に回復しない場合があり、追加のアクションが必要です。
- Cisco NX-OS リリース 10.3(2)F 以降、「feature nbm」が有効になっている場合にのみ、サブインターフェイスで NAT がサポートされるようになりました。
- Cisco NX-OS リリース 10.3(2)F 以降、出力サービス リフレクション（出力マルチキャスト NAT、およびマルチキャストからユニキャスト NAT）は、出力インターフェイスの IP アドレスとして NAT 後の送信元 IP をサポートします。この機能拡張は、通常のマルチキャストおよび IPFM でサポートされます。

マルチキャストからマルチキャスト入力 NAT

入力 NAT では、着信（S、G）を別の送信元、グループ、またはその両方に変換できます。ドメイン内のすべての受信者は、変換後のフローに参加できます。この機能は、マルチキャストトラフィックが次の場合に役立ちます。

- アドレスが重複している可能性がある別のドメインからネットワークに入る
- ネットワーク内のアプリケーションによって認識されないアドレスが付属しています

事前変換されたルートでの動的 IGMP 参加または PIM 参加は、入力 NAT ではサポートされていません。

マルチキャストからマルチキャストへの入力 NAT は、PIM アクティブ モードでのみ機能します。PIM パッシブ モードはサポートされていません。

マルチキャストからマルチキャスト出力 NAT

出力 NAT では、既存のフロー（S、G）を、発信インターフェイスごとに異なる送信元またはグループ アドレスに変換できます。この機能は、特定のソースまたはグループ アドレスのみを受け入れる可能性のある外部エンティティへのマルチキャスト配信に役立ちます。また、フローが外部エンティティに公開されるときに、内部アドレス空間を非表示にするパスとして機能することもできます。

変換後のルートでの動的 IGMP 参加または PIM 参加は、出力 NAT ではサポートされていません。

変換前と変換後のフローの帯域幅に不一致がある場合、障害 MO が生成されます。

PIM パッシブ モードでは、フローの帯域幅管理は外部コントローラによって実行され、変換前と変換後の両方のフローがプロビジョニングされます。フローの作成は、API を介して利用できます。

ENAT PIM パッシブの例

サービス インターフェイス loopback1 の設定

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

```
}
}
}
]
}
}
```

NAT モードを出力に設定する

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

マッピング インターフェイスの設定

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

SR ルールの設定:

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

NAT 前のフロー

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

NAT 後のフロー

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

マルチキャストからユニキャスト NAT

マルチキャストからユニキャストへの NAT は、コンテンツをパブリック クラウドにホストするために使用されます。クラウドがマルチキャストをサポートしていない可能性があるため、

変換が必要です。変換後、ユニキャスト パケットはユニキャスト転送ロジックに従ってルーティングされます。

異なるサイトに接続する場合も同様の使用例が見られます。コアがエンド ツー エンドのマルチキャストをサポートしていない場合、コンテンツはさまざまなサイトにユニキャストとして配信されます。境界ボックスは、マルチキャストをユニキャストに変換し、消費のためにさまざまなサイトに配信します。

MU NAT の場合、IPFM は、事前に変換されたマルチキャスト フローの帯域幅管理を引き続き実行します。変換されたユニキャスト フローの場合、変換されたユニキャスト トラフィックが中断することなく送信されるように、発信インターフェイスはユニキャスト帯域幅を予約する必要があります。IPFM は、NAT 関係を示すためにフロー操作 MO も発行します。ユニキャスト変換ごとに内部で 3 つの再循環が発生するため、再循環ポート帯域幅の 3 分の 1 だけが想定されていることを確認する必要があります。再循環に使用されるサービス リフレクト マップ インターフェイスで輻輳が発生した場合、IPFM は障害 MO を公開しません。

PIM パッシブ モードでは、コントローラは帯域幅管理を実行し、Rest API を呼び出して事前変換されたフローをプロビジョニングします。IPFM は、NAT 関係を示すために、フロー操作 MO を公開します。

MU NAT PIM パッシブの例

以下は、MUNAT Rest API 呼び出しとペイロード情報です。

Re-circ インターフェイスの設定

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

サービス リフレクト ルール

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

```
"udpsrcPort": "0"
}
}
}
```

IPFM フロー

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

ユニキャストからマルチキャスト NAT へ

ユニキャストからマルチキャストへの NAT は、入力変換モードで機能します。マルチキャスト変換されたパケットは、出力変換してマルチキャストに戻すことができます。ユニキャストパケットの接続先アドレスは、NAT 送信元ループバック インターフェイス セカンダリ IP アドレスと一致する必要があります。

ユニキャストからマルチキャストへの NAT は、1:1 の変換のみをサポートします。1 対多の変換が必要な場合は、1:1 のユニキャストからマルチキャストへの NAT を設定してから、1 対多のマルチキャストからマルチキャストへの NAT 変換を設定する必要があります。

ユニキャストからマルチキャストへの NAT では、事前変換されたユニキャスト トラフィックが到着するポートでユニキャスト帯域幅予約を設定する必要があります。これにより、そのポートのマルチキャスト トラフィックがすべてのポート帯域幅を消費しないようにすることができます。IPFM は、変換後のマルチキャスト グループのフロー ポリシーから派生した帯域幅を使用して、すべてのスライスにポリサーをインストールして、ユニキャスト フローをポリシングします。マルチキャスト変換ごとに 1 つの再循環があるため、再循環ポートの帯域幅は着信ポートの帯域幅と同じである必要があります。

IPFM は、NAT 関係を示すためにフロー操作 MO を公開します。再循環に使用されるサービス リフレクト マップ インターフェイスに輻輳がある場合、IPFM は障害 MO を公開しません。

（注） 後続のマルチキャストからマルチキャストへの変換フローにフローの優先度を割り当てることはできません。このフローの優先順位は、ユニキャストからマルチキャストへの変換フロー（親フロー）に設定する必要があります。

ユニキャストからマルチキャストへの NAT PIM アクティブの例

次に、PIM アクティブ モードでのユニキャストからマルチキャストへの NAT の例を示します。

UMNAT フロー

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

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

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

連鎖 MMNAT フロー

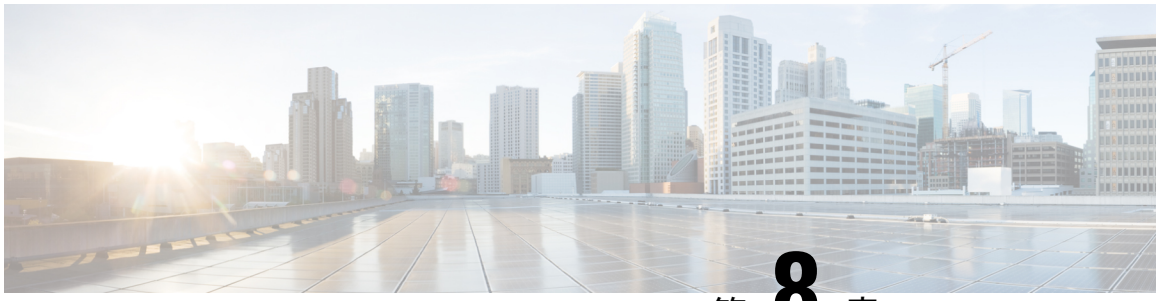
```
ip service-reflect destination 234.34.203.11 to 234.34.253.11 mask-len 32 source
10.34.201.1 to 10.34.202.111 mask-len 32 to-udp-src-port 25010 to-udp-dest-port 25310
static-oif Ethernet1/56
ip service-reflect destination 234.34.203.11 to 234.34.253.11 mask-len 32 source
10.34.201.1 to 10.34.202.111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

other supporting config needed for above flow stitching are:

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

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

(10.30.17.11/32, 10.34.202.11/32)
  Translation:
    SR: (10.34.201.1/32, 234.34.203.11/32) udp src: 0, udp dst : 0
      Outgoing interface list: (count: 3)
        Ethernet1/56, uptime: 02:13:44, igmp
        Ethernet1/55, uptime: 02:13:44, igmp
        Ethernet1/60, uptime: 02:13:51, static
      Chained translations:
       SR: (10.34.202.111, 234.34.253.11) udp src: 25010 udp dst: 25310 OIF: Ethernet1/56

       SR: (10.34.202.111, 234.34.253.11) udp src: 25010 udp dst: 25510 OIF: Ethernet1/55

switch#

switch# show forwarding distribution multicast route group 234.34.203.11 source 10.34.201.1


  (10.34.201.1/32, 234.34.203.11/32), RPF Interface: Ethernet1/6.100, flags: EPrePstUM
    Upstream Nbr: 10.34.201.1, Stats State: NA
    Received Packets: 16964898 Bytes: 23784786996
```

```
    Number of Outgoing Interfaces: 6
    Outgoing Interface List Index: 1609
      Ethernet1/55
      Ethernet1/56
      Ethernet1/60
      Null0
        Type: NAT_EGR_RW
        Source IF: Ethernet1/6.100
        RW Group IP: 234.34.203.11
        RW Source IP: 10.34.201.1
        RW source L4 port: 0
        RW dest L4 port: 0
        Original Group IP: 10.34.202.11
        Original Source IP: 10.30.17.11

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

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

switch#

switch# show forwarding multicast route group 234.34.203.11 source 10.34.201.1

slot  1
=======


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

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

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



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

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

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

Mcast-Group      Src-IP           Uptime   Src-Intf     Nbr-Device         LID Profile
Status  Num Rx  Bw Mbps   CFG Bw Slot Unit Slice DSCP QOS Policed FHR Priority
Policy-name
   Rcvr-Num Rcvr-slot Unit    Num-Rcvrs    Rcvr-ifidx  IOD Rcvr-Intf  Nbr-Device

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

          1         1    0            3    0x1a006e00   64 Eth1/56    not-available

          2         1    0            3    0x1a006c00   63 Eth1/55    not-available

          3         1    0            3    0x1a007600   68 Eth1/60
LEAF34-PMN-SOLN-SOUTHLAKE
switch#


switch# show nbm flows statis group 234.34.203.11 source 10.34.201.1

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

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

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


NBM Oper MO:

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

```
}

{
  "nbmNbmFlow": {
    "attributes": {
      "bucket": "1",
      "bwKbps": "15000",
      "dn": "sys/nbm/show/flows/dom-default/s-[10.34.201.1]-g-[234.34.203.11]",
      "dscp": "0",
      "egressIfCount": "3",
      "flowPol": "umnat",
      "group": "234.34.203.11",
      "ingressIf": "335544354",
      "ingressIfName": "loopback34",
      "isFhr": "YES",
      "modTs": "2021-11-30T11:35:23.384+00:00",
      "policed": "YES",
      "priority": "LOW",
      "qid": "7",
      "source": "10.34.201.1",
      "tStamp": "1638300923224"
    },
    "children": [
      {
        "nbmOifList": {
          "attributes": {
            "dn":
"sys/nbm/show/flows/dom-default/s-[10.34.201.1]-g-[234.34.203.11]/oif-436237824",
            "modTs": "2021-11-30T11:35:35.387+00:00",
            "oif": "436237824",
            "oifName": "Ethernet1/60",
            "oifTstamp": "1638300935386",
            "origin": "PROTOCOL",
            "reporterIP": "10.34.60.1"
          }
        }
      },
      {
        "nbmOifList": {
          "attributes": {
            "dn":
"sys/nbm/show/flows/dom-default/s-[10.34.201.1]-g-[234.34.203.11]/oif-436235264",
            "modTs": "2021-11-30T11:35:42.436+00:00",
            "oif": "436235264",
            "oifName": "Ethernet1/55",
            "oifTstamp": "1638300942436",
            "origin": "PROTOCOL",
            "reporterIP": "10.34.55.11"
          }
        }
      },
      {
        "nbmOifList": {
          "attributes": {
            "dn":
"sys/nbm/show/flows/dom-default/s-[10.34.201.1]-g-[234.34.203.11]/oif-436235776",
            "modTs": "2021-11-30T11:35:42.437+00:00",
            "oif": "436235776",
            "oifName": "Ethernet1/56",
            "oifTstamp": "1638300942437",
            "origin": "PROTOCOL",
            "reporterIP": "10.34.56.11"
          }
        }
```

```
      },
      {
        "nbmUmIngNat": {
          "attributes": {
            "dn":
"sys/nbm/show/flows/dom-default/s-[10.34.201.1]-g-[234.34.203.11]/umng-pres-[10.30.17.11]-pred-[10.34.202.11]-postsp-[0]-postdp-[0]",

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



第 8 章

メディア コントローラ

このセクションでは、Cisco NDFC Web クライアント UI の **[メディア コントローラ（Media Controller）]** タブについて説明します。

（注） Cisco NDFC リリース 11.1(1) 以降、ネットワーク管理者ロールを持つユーザだけが、ホストまたはフロー ポリシー、およびグローバル コンフィギュレーション設定を設定できます。

（注）

- Cisco NDFC リリース 11.1(1) 以降、ネットワーク管理者ロールを持つユーザだけが、ホストまたはフロー ポリシー、およびグローバル コンフィギュレーション設定を設定できます。
- IPFM は、通信を停止する前に、スイッチの既知の最後の監視状態を維持します。スイッチが 2 分以内に報告しない場合、**同期がとれていない**とマークされます。**メディア コントローラ / フロー / フロー ステータス**など、それぞれのモニタリング ページで **[テレメトリ スイッチの同期ステータス（Media Controller / Flow / Flow Status）]** リンクをクリックして、同期ステータスと最後の同期タイムスタンプを確認します。

POAP を使用して基本設定からデバイスを起動するには、テンプレートを定義し、Cisco NDFC の **[Web クライアント（Web Client）] > [設定（Configure）] > [展開（Deploy）] > [POAP 定義（POAP Definitions）]** から POAP 定義を公開する必要があります。詳細については、「*POAP Launchpad*」セクションを参照してください。

（注） メディア コントローラ展開用のリーフおよびスパイン用の特定の POAP テンプレートは、Cisco NDFC ソフトウェアにパッケージ化されています。

メディア コントローラ モードで Cisco NDFC サーバを設定し、「POAP ランチパッド」に記載されている手順を実行した場合、メディア コントローラ テンプレートを表示できます。Cisco NDFC Web クライアントでは、必要なテンプレートを選択し、必要に応じて編集して、POAP 定義を公開できます。

メディア コントローラ API の詳細については、Cisco DevNet の『Cisco NDFC メディア コントローラ API リファレンス』を参照してください。

NDFC メディア コントローラの展開は、監視目的のみに使用でき、ポリシー マネージャとしては使用できません。詳細については、『メディア コントローラの *NDFC* 読み取り専用モード』を参照してください。

NX-OS ストリーミング テレメトリと NDFC

ストリーミング テレメトリを使用して、スイッチの IPFM プロセスは NDFC にその状態を通知します。これを使用して、検出されたホストと IP ファブリック全体のフローを表示できる NDFC を使用します。NDFC にパッケージ化されている POAP および `pmn_telemetry_snmp` CLI テンプレートは、スイッチで必要なテレメトリ構成を生成します。生成された設定の例は、次のサンプルに示すとおりです。

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

```
subscription 201
  dst-grp 200
  snsr-grp 200 sample-interval 60000
  snsr-grp 201 sample-interval 30000
  snsr-grp 205 sample-interval 30000
subscription 202
  dst-grp 200
  snsr-grp 202 sample-interval 30000
subscription 203
  dst-grp 200
  snsr-grp 203 sample-interval 30000
subscription 204
  dst-grp 200
  snsr-grp 204 sample-interval 30000
subscription 300
  dst-grp 200
  snsr-grp 300 sample-interval 30000
  snsr-grp 301 sample-interval 30000
subscription 500
  dst-grp 200
  snsr-grp 500 sample-interval 30000
subscription 400
  dst-grp 200
  snsr-grp 400 sample-interval 0
```

メディア コントローラの範囲

[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [スイッチ グループ（Switch Groups）] ウィンドウで作成したスイッチ グループが、**[範囲（SCOPE）]** ドロップダウン リストの下に表示されます。

[範囲（SCOPE）] ドロップダウン リストは、**[イベント（Events）]** ウィンドウを除く、**[メディア コントローラ（Media Controller）]** の下のすべてのウィンドウに適用されます。

たとえば、**トポロジ** ウィンドウで検索する場合、**[範囲（SCOPE）]** ドロップダウン リストで選択されているスイッチ グループだけが検索対象となります。

同様に、ホスト、フロー、RTP フロー モニタ、グローバル設定の各画面の操作は、**[範囲（SCOPE）]**ドロップダウン リストで選択したスイッチグループ配下の装置に対してのみ有効です。

スイッチ グループは互いに分離されています。たとえば、2つの異なるスイッチ グループに同じ名前と IP アドレスを持つホスト エイリアスを作成できます。詳細については、「スイッチ グループの管理」を参照してください。

（注） **[範囲（SCOPE）]** ドロップダウン リストから **[データ センター（Data Center）]** を選択すると、データ センターがサポートされていないことを示すポップアップ ウィンドウが表示されます。

- 一般的なマルチキャスト モニタリング （108 ページ）
- トポロジ, on page 110
- ホスト, on page 112
- フロー, on page 129

一般的なマルチキャスト モニタリング

Cisco NDFC リリース 11.4(1) 以降、監視目的で汎用マルチキャスト機能を使用できます。この機能は、Cisco NX-OS リリース 9.3(5) 以降のスイッチに適用できます。

汎用マルチキャストは、メディア コントローラ展開モードで使用できます。NDFC のインストール後、メディア用 IP ファブリック（IPFM）モードまたは汎用マルチキャスト モードのどちらで NDFC を実行するかを決定します。汎用マルチキャスト モードを有効にするには、**pmn.generic-multicast.enabled** サーバ プロパティを使用します。

汎用マルチキャスト モードの有効化

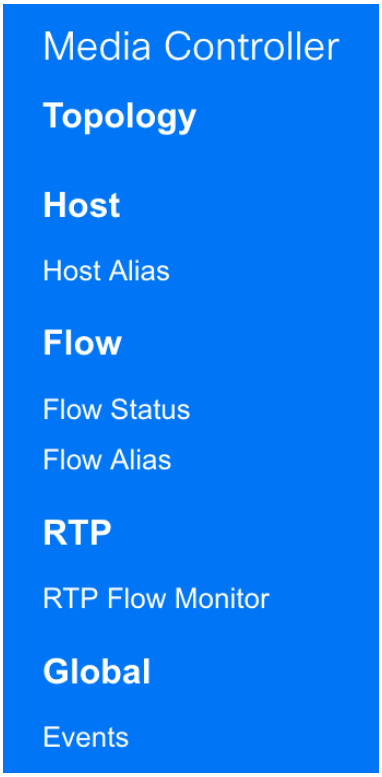
1. **[管理 (Administration)] > [DCNM サーバ (DCNM Server)] > [サーバ ステータス (Server Status)]** を選択します。
2. **pmn.generic-multicast.enabled** サーバ プロパティを **true** に設定します。デフォルトでは、**false** に設定されています。
3. **[変更を適用（Apply Changes）]** をクリックしてサーバ設定を保存します。
4. すべての NDFC サービスを再起動するように求めるポップアップ ダイアログ ボックスが表示されます。**[OK]**をクリックします。
5. スタンドアロン NDFC インストールの場合、プロパティを有効にするために **appmgr restart dcnm** コマンドを使用して NDFC を再起動します。

   NDFC HA モードの場合、**pmn.generic-multicast.enabled** サーバープロパティを **true** に設定し、**[管理（Administration）]/[DCNM サーバ（DCNM Server）]/[ネイティブ HA（Native HA）]** ウィンドウで **[フェールオーバ（Failover）]** をクリックします。新しい NDFC アクティブは、汎用マルチキャスト モードで起動します。

（注）
- **pmn.generic-multicast.enabled** サーバ プロパティを **false** に設定し、NDFC を再起動して、IPFM モードで NDFC を有効にすることができます。
- IPFM は、**[サーバ プロパティ（Server Properties）]** ウィンドウの設定を使用して、読み取り専用モードまたは読み取り/書き込みモードをサポートします。IPFM と汎用マルチキャストは相互に排他的な機能であるため、NDFC を汎用マルチキャスト モードに設定した後は、このプロパティは適用されません。

汎用マルチキャスト メニュー

汎用マルチキャスト モードの Cisco NDFC には、モニタリング用の IPFM 機能のサブセットが含まれています。



NX-OS ストリーミング テレメトリと NDFC（汎用マルチキャスト）

ストリーミングテレメトリを使用して、スイッチはNDFCにその状態を通知します。これは、どの NDFC が IP ファブリック全体で検出されたホストとフローを表示できるかを使用して行います。NDFC にパッケージ化されている **pmn_generic_multicasttelemetry_snmp** CLI テンプレートは、スイッチで必要なテレメトリ設定を生成します。生成された設定の例は、次のサンプルに示すとおりです。

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

```
subscription 300
   dst-grp 600
   snsr-grp 300 sample-interval 30000
   snsr-grp 301 sample-interval 60000
subscription 500
   dst-grp 600
   snsr-grp 500 sample-interval 30000
```

トポロジ

[Web UI] > [メディア コントローラ（Media Controller）] > [トポロジ（Topology）] ページで、メディア コントローラ トポロジを表示できます。このトポロジは、メディア コントローラとして NDFC によって実行される操作に固有です。

スイッチをクリックすると、スライド アウト ウィンドウの **[フロー（Flow）]** セクションに NAT ラベル情報、つまり、入力、出力、または入力と出力が表示されます。

Note このセクションは、NDFC の IPFM と汎用マルチキャスト モードの両方に適用されます。

汎用マルチキャストは、2 階層スパインまたはリーフ トポロジに制限されません。フロー分類とパス トラッキングは、すべての関連スイッチが Cisco NX-OS リリース 9.3(5) を搭載した Cisco Nexus 9000 シリーズ スイッチでない限り、特定のトポロジに制限されません。汎用マルチキャストは、デフォルト VRF でサポートされます。

Note この機能は、インストール プロセス中にメディア コントローラを有効にした場合にのみ使用できます。メディア コントローラを有効にするには、NDFC の OVA/ISO インストール中に **IP ファブリック メディア コントローラ**のインストール オプションを選択します。以前のリリースで使用されていた **appmgr set-mode media-controller** コマンドは、NDFC 10.4(2) では使用できません。

Note

- インベントリからデバイスを削除すると、そのスイッチのポリシー展開ステータスが削除されます。ただし、スイッチのポリシー構成もクリアします。
- あるポートから別のポートにケーブルを移動した後、古いリンクは **[トポロジ（Topology）]** ウィンドウに保持され、リンクがダウンしていることを示す赤色で表示されます。ポートの移動は、**[トポロジ（Topology）]** ウィンドウでは更新されません。更新されたポートが NDFC に表示されるようにスイッチを再検出します。

高速検索

検索文字列を入力して、関連するデバイスを強調表示します。

スイッチまたはホスト名、スイッチまたはホストの IP アドレス、スイッチの MAC、および**スイッチのシリアル番号**を検索できます。

Generic Multicast モードでは、このウィンドウでレシーバインターフェイス名または IP アドレスを検索することもできます。

マルチキャスト グループ

フィールドを右クリック (または Return キーを押します) します。マルチキャスト アドレスのリストを表示します。トポロジを表示する必要があるマルチキャスト IP アドレスを選択できます。

このマルチキャスト IP アドレスの下のデバイス、およびスパインおよびリーフへのリンクが強調表示されます。移動する点線は、メディア コントローラ トポロジ内のトラフィックのフローを示しています。

トポロジのフローエイリアス名に基づいて検索またはフィルタリングできます。マルチキャストグループを検索する場合、IP アドレスまたはフローエイリアス名を使用して検索できます。

パネルを表示 > 帯域幅

[帯域幅（Bandwidth）] チェックボックスをオンにすると、スパインとリーフによって消費される帯域幅がカラー インジケータとして表示されます。

- 緑：40% 未満
- 黄色：40% ～ 80%
- 赤：80% 以上

表示形式は送信-受信です。

一般的なメディア コントローラ ファブリックでは、ISL リンクはリーフとスパインの間に設定され、ISL リンクは Cisco NDFC がフローをステッチするために必要な帯域幅を計算するのに役立ちます。設定に問題がある場合、Cisco NDFC 帯域幅マネージャが間違ったリンクを判断する可能性があります。

Cisco NDFC 帯域幅計算アルゴリズムは、送信側と受信側の間で共通のノードを見つけようとします。

ホスト側リンクでの帯域幅追跡

送信側と受信側は、IPFM ファブリックのリーフ スイッチに接続できます。送信側はマルチキャスト フローを開始し、受信側はマルチキャスト フローにサブスクライブします。マルチキャストが使用されるため、フローにサブスクライブする受信者が複数存在する可能性があります。送信側は、カメラ、マイク、再生デバイスなどのデバイスです。レシーバは、ビデオモニタ、スピーカー、マルチビューアなどのデバイスです。

Note ホスト ポート帯域幅の追跡は、**[Web UI] > [管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** ページの **pmn.host.port.policing.enabled** フィールドで有効または無効にできます。デフォルトでは、ホスト ポートの帯域幅追跡は無効になっています。

ホスト側のリンクで帯域幅を追跡できます。この機能を使用すると、NDFCでは、受信者がより多くのフローを要求したり、送信者がホストに面しているリンクで使用可能な帯域幅よりも多くのフローを送信したりすることはできません。

ホスト

ホスト メニューには次のサブメニューが含まれます。

検出されたホスト

この画面には、テレメトリによって入力されたすべてのホストを表示できます。スイッチが検出されると、ファブリック内のすべてのスイッチがテレメトリを使用して定期的にNDFCサーバーにデータをプッシュします。Cisco NDFC サーバーは、アクティブなフローごとに受信したイベントとフローの統計情報を表示します。

次の表で、このページに表示されるフィールドを説明します。テーブルヘッダーをクリックすると、エントリがそのパラメータのアルファベット順にソートされます。

Table 4: 検出されたホスト テーブルのフィールドと説明

フィールド	説明
VRF	VRF インスタンスを指定します。
ホスト名	ホストIPアドレスの設定済みホストエイリアスを指定します。 ホストエイリアスが設定されていない場合は、ホスト IP が表示されます。

フィールド	説明
職務	ホスト デバイスのロールを指定します。ホストのロールは次のいずれかになります。 • 送信者 • 外部送信者 • ダイナミック レシーバ • 外部レシーバ • スタティック レシーバ
マルチキャスト グループ	ホストが参加するフローのマルチキャスト アドレスを指定します。
ソース言語	検出されたホストが参加するフローの送信元を指定します。
スイッチ	スイッチの名前を示します。
インターフェイス	送信側または受信側スイッチでホストが接続されているインターフェイスを指定します。
MAC アドレス	物理ホストのMACアドレスを指定します（スイッチにそのホストのARPエントリがある場合）。
NDFC 検出時間	スイッチがホストを検出した日時を指定します。
障害の理由（Fault Reason）	検出されたホストが参加しているフローの失敗理由を指定します。

Cisco NDFC リリース 11.3(1) 以降、同じホストの複数のエントリは、展開可能な行としてグループ化されます。矢印アイコンをクリックして、特定の行を展開するか、複数の行を1つの行に折りたたんでください。

ホスト エイリアス

Note このセクションは、NDFC の IPFM と汎用マルチキャスト モードの両方に適用されます。

Cisco NDFC では、メディア コントローラの送信者ホストと受信者ホストのホスト エイリアスを作成できます。アクティブなマルチキャスト トラフィックの送受信デバイスは、ホストと呼ばれます。Cisco NDFC リリース 11.0(1) 以降、ホスト エイリアス名を送信者と受信者のホスト

に追加すると、ホストを名前で識別しやすくなります。また、多くのホストエイリアスをCisco NDFC メディア コントローラにインポートすることもできます。

次の表で、このページに表示されるフィールドを説明します。

Table 5: ホスト エイリアス テーブルのフィールドと説明

フィールド	説明
ホスト エイリアス	ホストを識別するように設定されているホスト名を指定します。
IP アドレス	エイリアス名で参照するスイッチに接続するホストの IP アドレスを指定します。
最終更新日時	ホスト エイリアスが最後に更新された日時を指定します。

この項の内容は、次のとおりです。

ホスト エイリアスの追加

以下のタスクを実行して、新しいホスト エイリアスを Cisco NDFC で検出したファブリックのデバイスに追加します。

Procedure

ステップ 1 **[メディア コントローラ（Media Controller）] > [ホスト（Host）] > [ホスト エイリアス（Host Alias）]** を選択し、**[追加]** をクリックします。

ステップ 2 [ホスト エイリアスの追加/編集（Add/Edit Host Alias）] ウィンドウで、以下を入力します。

- **[ホスト名（Host Name）]**：識別用の完全修飾ホスト名を入力します。
- **[IP アドレス（IP Address）]**：フローの一部であるホストの IP アドレスを入力します。

Note
また、ホストが直接接続された送信側または受信側リーフにデータを送信する前に、ホスト エイリアスを作成することもできます。

ステップ 3 **[保存（Save）]** をクリックして、変更内容を保存します。

ホスト エイリアスを破棄するには、**[キャンセル（Cancel）]** をクリックします。

新しいホスト エイリアスが **[ホスト エイリアス（Host Alias）]** ウィンドウのテーブルに表示されます。

ホスト エイリアスの編集

ホスト エイリアスを編集するには、次のタスクを実行します。

Procedure

ステップ 1 **[メディア コントローラ（Media Controller）] > [ホスト（Host）] > [ホスト エイリアス（Host Alias）]** を選択し、変更する必要があるホスト エイリアスの横にあるチェック ボックスをオンにします。

ステップ 2 **[ホスト エイリアスの追加/編集（Add/Edit Host Alias）]** ウィンドウで、以下を入力します。

- **[ホスト名（Host Name）]**：識別用の完全修飾ホスト名を入力します。
- **[IP アドレス（IP Address）]**：フローの一部であるホストの IP アドレスを入力します。

ステップ 3 **[保存（Save）]** をクリックして、変更内容を保存します。

ホスト エイリアスを破棄するには、**[キャンセル（Cancel）]** をクリックします。

編集したホスト エイリアスが **[ホスト エイリアス（Host Alias）]** ウィンドウのテーブルに表示されます。

ホスト エイリアスの削除

ホスト エイリアスを削除するには、次のタスクを実行します。

Procedure

ステップ 1 **[メディア コントローラ（Media Controller）] > [ホスト（Host）] > [ホスト エイリアス（Host Alias）]** を選択し、削除するホスト エイリアスの隣にあるチェックボックスをオンにします。

同じインスタンスで、削除する複数のホスト エイリアス エントリを選択できます。

ステップ 2 [削除（Delete）] をクリックします。

ステップ 3 確認ウィンドウで、**[OK]** をクリックしてホスト エイリアスを削除します。

ホスト エイリアスを保持するには、**[キャンセル（Cancel）]** をクリックします。

ホスト エイリアスのインポート

次のタスクを実行して、ファブリックのデバイスにホスト エイリアスをインポートします。

Procedure

ステップ 1 **[メディア コントローラ（Media Controller）] > [ホスト（Host）] > [ホスト エイリアス（Host Alias）]** を選択し、**[インポート]** アイコンをクリックします。

ステップ 2 ディレクトリを参照し CSV ファイルを選択します。これには、ホスト IP アドレスと対応する固有ホスト名情報を含みます。

ステップ 3 [開く（Open）] をクリックします。

ホスト エイリアスはホスト エイリアス テーブルにインポートされ表示されます。

ホスト エイリアスのエクスポート

以下のタスクを実行して、ファブリックのデバイス向けにホストエイリアスをエクスポートします。

Procedure

ステップ 1 **[メディア コントローラ（Media Controller）] > [ホスト（Host）] > [ホスト エイリアス（Host Alias）]** を選択し、**[エクスポート（Export）]** アイコンをクリックします。

通知ウィンドウが表示されます。

ステップ 2 NDFC からホスト エイリアス設定を保存するローカル システム ディレクトリの場所を選択し、**[OK]** をクリックします。

ホスト エイリアス コンフィギュレーション ファイルがローカル ディレクトリにエクスポートされます。ファイルがエクスポートされた日時がファイル名に付加されます。エクスポートされるファイルの形式は `.csv` です。

ホスト ポリシー

ホスト デバイスにポリシーを追加できます。 [メディア コントローラ（Media Controller）] > [ホスト（Host）] > [ホスト ポリシー（Host Policies）] に移動して、ホスト ポリシーを設定します。

（注） スイッチは、デフォルトのホストポリシーを使用して展開する必要があります。デフォルトのホスト ポリシーを編集して、許可または拒否することができます。展開ドロップダウン リストから、**[選択したポリシーの展開（Deploy Selected Policies）]** を選択してスイッチにデフォルトのポリシーを展開します。また、デフォルト ポリシーを選択しなくても、**[すべてのデフォルト ポリシーを展開（Deploy All Default Policies）]** を選択することで、すべてのデフォルト ポリシーをすべての管理対象スイッチに展開できます。

デフォルトでは、ポリシーのシーケンス番号はによって自動生成され、NDFC およびマルチキャストマスク/プレフィックスは/32 として取得されます。**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** の下のプロパティ **pmn.hostpolicy.multicast-ranges.enabled** は、シーケンス番号とマルチキャストマスク/プレフィックスを提供できるように、ユーザに対して「**true**」に設定する必要があります。サーバプロパティが **True** に設定されている場合、シーケンス番号とマルチキャストマスク/プレフィックスを入力するフィールドは、**[メディア コントローラ（Media Controller）] > [ホスト（Host）] > [ホスト ポリシー（Host Policies）] > [追加（Add）]** および **[メディア コントローラ（Media Controller）] > [ホスト（Host）] > [ホスト ポリシー（Host Policies）] > [編集（Edit）]** ページで使用できます。

スイッチにカスタム ホスト ポリシーを展開する前に、デフォルトのホスト ポリシーをスイッチに正しく展開する必要があります。そうしなかった場合、カスタムポリシーの展開に失敗します。カスタムポリシーを追加、編集、インポート、または展開する前に、すべてのスイッチにすべてのデフォルト ポリシーが正常に展開されていることを確認します。

（注） ユーザがネットワーク オペレータ ロールでNDFCにログインすると、ポリシーを追加、削除、変更、インポート、エクスポート、または展開するためのすべてのボタンまたはオプションが無効になります。このユーザはポリシー、展開ステータスまたは履歴を確認することのみ、可能です。

次の表で、このページに表示されるフィールドを説明します。

表 *6 :* ホスト ポリシーの操作

フィールド	説明
追加（Add）	新しいホスト ポリシーを追加できます。
編集	選択したホスト ポリシー パラメータを表示または編集できます。

フィールド	説明
削除	ユーザ定義ホスト ポリシーを削除できます。 （注） • NDFCからそれらを削除する前に、すべてのスイッチからポリシーを展開解除します。 • デフォルト ポリシーを展開解除できますが、デフォルト ポリシーは削除できません。カスタム ポリシーのみを削除および展開解除できます。 • デフォルト ポリシーを展開解除するとき、すべてのデフォルト ポリシーはデフォルトの権限をもつようにリセットされます（許可）。
すべて削除	ポリシーチェックボックスを選択せずに、すべてのカスタム ポリシーを削除できます。 （注） • NDFCからそれらを削除する前に、すべてのスイッチからポリシーを展開解除します。 • デフォルト ポリシーを展開解除できますが、デフォルト ポリシーは削除できません。カスタム ポリシーのみを削除および展開解除できます。
インポート	CSV ファイルから NDFC にホスト ポリシーをインポートできます。 （注） インポート後、CSV ファイルからインポートされたすべてのポリシーは、すべての管理対象スイッチに自動的に適用されます。
エクスポート	NDFC から CSV ファイルにホスト ポリシーをエクスポートできます。

フィールド	説明
デプロイ	

フィールド	説明

	[展開（Deployment）] ドロップダウン リストから、適切な値を選択します。
	• [展開（Deploy）]
	  • 選択したポリシー：このオプションを選択して、選択したポリシーをスイッチに展開します。
	  • すべてのデフォルト ポリシー：このオプションを選択して、すべてのデフォルト ポリシーをスイッチに展開します。
	  • すべてのカスタム ポリシー：このオプションを選択して、すべてのユーザ定義ポリシーを展開します。
	• 展開解除
	  • 選択したポリシー：このオプションを選択して、選択したポリシーを展開解除します。
	  • すべてのデフォルト ポリシー：このオプションを選択して、デフォルト ポリシーを展開解除します。
	  • すべてのカスタム ポリシー：このオプションを選択して、すべてのユーザ定義ポリシーを展開解除します。
	• すべての失敗したポリシーを再試行する：このオプションを選択して、すべての失敗したポリシーを展開します。
	以前にスイッチで失敗したすべての展開は、それらのスイッチにのみ再度展開されます。以前スイッチの展開解除が失敗した場合、同じスイッチからのみ再度展開解除ができます。
	• 展開履歴：ドロップダウン リストからポリシーを1つ選択します。このオプションを選択して、選択したポリシーの展開履歴を表示します。
	[展開履歴（Deployment History）] には、次のフィールドが表示されます。
	  • ポリシー名：選択したポリシー名を表示します。
	  • スイッチ名：ポリシーが展開されたスイッチ名を指定します。

フィールド	説明
	• 展開ステータス：展開のステータスを表示します。導入が成功したか失敗したかが表示されます。 • アクション：ホストポリシーのスイッチで実行されるアクションを指定します。[作成（Create）] は、ポリシーがスイッチに展開されていることを意味します。[削除（Delete）] は、ポリシーがスイッチから展開解除されたことを意味します。 • 展開日時：ホストポリシーが最後に更新された日時を指定します。日時の表示形式は *Day MMM DD YYYY HH:MM:SS* タイムゾーン（*Timezone*） です。 • 失敗理由：ポリシーが正常に展開されなかった理由。

表 *7:* ホスト ポリシー テーブルのフィールドと説明

フィールド	説明
ポリシー名	ユーザの定義に従って、ホストのポリシー名を指定します。
ホスト名	ホスト ID を指定します。
受信者 IP	受信側デバイスの IP アドレスを指定します。
送信者IP（Sender IP）	転送するデバイスの IP アドレスを指定します。
マルチキャストIP	ホストのマルチキャスト IP アドレスを指定します。
送信者IP（Sender IP）	送信者の IP アドレスを指定します。
[ホストロール（Host Role）]	ホストデバイスロールを指定します。ホストデバイスロールは、次のいずれかです。 • 送信者 • 受信者 - 外部（Receiver-External） • 受信者 - ローカル（Receiver-Local）
オペレーション	ホスト ポリシーの動作かどうかを指定します。ポリシーには次の操作があります。 • 許可 • 拒否

フィールド	説明
Sequence #	マルチキャスト範囲が選択されている場合のカスタム ポリシーのシーケンス番号を指定します。
展開アクション（Deployment Action）	ホスト ポリシーのスイッチで実行されるアクションを指定します。 • **作成**：ポリシーがスイッチで展開されます。 • **削除**：ポリシーがスイッチから展開解除されます。
展開ステータス	展開が成功したか、失敗したか、またはポリシーが展開されていないかを指定します。
最終更新日	ホスト ポリシーが最後に更新された日時を指定します。 日時の表示形式は *Day MMM DD YYYY HH:MM:SS* タイムゾーン（*Timezone*） です。

この項の内容は、次のとおりです。

ホスト ポリシーの追加

デフォルトでは、ポリシーのシーケンス番号は NDFC により自動生成され、マルチキャスト マスク/プレフィックスはデフォルトで /32 です。**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバ プロパティ（Server Properties）]** の下のプロパティ **pmn.hostpolicy.multicast-ranges.enabled** は、シーケンス番号とマルチキャスト マスク/プレフィックスを提供できるように、ユーザに対して「**true**」に設定する必要があります。サーバ プロパティが **True** に設定されている場合、シーケンス番号とマルチキャスト マスク/プレフィックスを入力するフィールドは、**[メディア コントローラ（Media Controller）] > [ホスト（Host）] > [ホスト ポリシー（Host Policies）] > [追加（Add）]** および **[メディア コントローラ（Media Controller）] > [ホスト（Host）] > [ホスト ポリシー（Host Policies）] > [編集（Edit）]** ウィンドウで使用できます。

スイッチにカスタム ホスト ポリシーを展開する前に、デフォルトのホスト ポリシーをスイッチに正しく展開する必要があります。そうしなかった場合、カスタム ポリシーの展開に失敗します。カスタム ポリシーを追加する前に、すべてのスイッチにすべてのデフォルト ポリシーが正しく展開されていることを確認します。

Cisco NDFC Web UI からホスト ポリシーを追加するには、次の手順を実行します。

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [ホスト（Host）] > [ホスト ポリシー（Host Policies）]** を選択します。

[ホスト ポリシー（Host Policies）] ウィンドウが表示されます。

ステップ 2 [追加（Add）] アイコンをクリックします。

ステップ 3 [ホスト ポリシーの追加 (Add Host Policy)] ウィンドウで、次のフィールドにパラメータを指定します。

- **ポリシー名**：ホスト ポリシーの一意のポリシー名を指定します。
- **ホスト ロール**：ホストをマルチキャスト送信者または受信者として指定します。次のいずれかを選択します。
  - 送信者
  - 受信者 - ローカル（Receiver-Local）
  - 受信者 - 外部（Receiver-External）
- **ホスト名**：ポリシーが適用されるホストを指定します。宛先ホストが検出された場合は、ドロップダウン リストからホスト名を選択できます。

  （注）
  受信者または送信者のホスト ポリシーを作成するために、リモート受信者として検出されたホストを選択しないでください。ただし、リモート送信者として検出されたホストは、送信者ホスト ポリシーの作成に使用できます。
- **送信者 IP**：ホストの送信側の IP アドレスを指定します。このフィールドに *（アスタリスク）記号または 0.0.0.0 を指定すると、この IP アドレスにワイルドカードを指定できます。
- **受信者 IP**：受信者ホストの IP アドレスを指定します。このフィールドは表示され、[ホスト ロール（Host Role）] が **[Receiver-Local]** に設定されている場合にのみ適用されます。このフィールドに *（アスタリスク）記号または 0.0.0.0 を指定すると、この IP アドレスにワイルドカードを指定できます。

  （注）
  受信者ホスト ポリシーの**受信者 IP**がワイルドカード（***** または 0.0.0.0）の場合、送信者 IP もワイルドカード（* または 0.0.0.0）である必要があります。
- **マルチキャスト**：ホスト ポリシーのマルチキャスト IP アドレスを指定します。このフィールドに（アスタリスク）記号を指定すると、この IP アドレスにワイルドカードを指定できます。これは 224.0.0.0/4 に変換されます。**[送信者IP（Sender IP）]** フィールドと **[受信者IP（Receiver IP）]** フィールドにワイルドカード IP アドレスを指定する場合、マルチキャスト グループは常に必要です。つまり、* または 0.0.0.0としてマルチキャストを指定することはできません。
- **許可/拒否**：ポリシーでトラフィック フローを**許可**または**拒否**する必要がある場合は、ラジオ ボタンをクリックして選択します。

ステップ 4 **[保存して展開（Save＆Deploy）]** をクリックして、ポリシーを設定および展開します。

[キャンセル（Cancel）] をクリックして新しいポリシーを破棄します。

ホスト ポリシーの編集

スイッチにカスタム ホスト ポリシーを展開する前に、デフォルトのホスト ポリシーをスイッチに正しく展開する必要があります。そうしなかった場合、カスタムポリシーの展開に失敗します。カスタム ポリシーを編集する前に、すべてのスイッチにすべてのデフォルト ポリシーが正常に展開されていることを確認します。

Cisco NDFC Web UI からホスト ポリシーを編集するにｈ、次の手順を実行します。

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [ホスト（Host）] > [ホスト ポリシー（Host Policies）]** を選択します。

[ホスト ポリシー（Host Policies）] ウィンドウが表示されます。

ステップ 2 編集する必要があるホスト ポリシー名の隣にあるチェックボックスをオンにします。

ステップ 3 ホスト ポリシーの **[編集（Edit）]** アイコンをクリックします。

ステップ 4 [ホスト ポリシーの編集（Edit Host Policy ）] ウィンドウで、ポリシーがトラフィックを**許可**するか**拒否**するかを編集して指定します。

（注）
ホスト ポリシーへの変更はすぐに適用されます。ポリシーがすでにデバイスに適用されている場合、変更が既存のフローに影響する可能性があります。

ステップ 5 **[保存して展開（Save＆Deploy）]** をクリックして、ポリシーを設定および展開します。

[キャンセル（Cancel）] をクリックして、変更を破棄します。

ホストポリシーの削除

Cisco NDFC Web UI からホスト ポリシーを削除するには、以下の手順を実行します。

（注） ユーザ定義のホスト ポリシーのみを削除できます。

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [ホスト（Host）] > [ホスト ポリシー（Host Policies）]** を選択します。

[ホスト ポリシー（Host Policies）] ウィンドウが表示されます。

ステップ 2 削除する必要があるホスト ポリシー名の隣にあるチェックボックスをオンにします。

削除するホスト ポリシーを複数選択できます。

ステップ 3 ホスト ポリシーの **[削除（Delete）]** アイコンをクリックします。

[すべて削除（Delete All）] をクリックして、単一インスタンスのすべてのポリシーを削除します。

ステップ 4 削除通知で、**[OK]** をクリックしてホスト ポリシーを削除します。**[キャンセル（Cancel）]**をクリックして [ホスト ポリシー（Host Policies）] ページに戻ります。

（注）
NDFC からホスト ポリシーを削除しても、ポリシーが展開されているスイッチからポリシーは展開解除されません。NDFC から削除する前に、スイッチのポリシーを展開解除することを強くお勧めします。

ページの下部に、ホスト ポリシーの削除に成功したことを示すメッセージが表示されます。

ホスト ポリシーのインポート

スイッチにカスタム ホスト ポリシーを展開する前に、デフォルトのホスト ポリシーをスイッチに正しく展開する必要があります。そうしなかった場合、カスタム ポリシーの展開に失敗します。カスタム ポリシーを追加する前に、すべてのスイッチにすべてのデフォルト ポリシーが正しく展開されていることを確認します。

Cisco NDFC Web UI からホスト ポリシーをインポートを追加するには、以下の手順を実行します。

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [ホスト（Host）] > [ホスト ポリシー（Host Policies）]** を選択します。

[ホスト ポリシー（Host Policies）] ウィンドウが表示されます。

ステップ 2 ホスト ポリシーの **[インポート（Import）]** アイコンをクリックします。

ステップ 3 ディレクトリを参照し、ホスト ポリシー設定情報を含む `.csv` ファイルを選択します。

`.csv` ファイル内のフォーマットが正しくない場合、ポリシーはインポートされません。

ステップ 4 [開く（Open）] をクリックします。

インポートされたポリシーは、ファブリック内のすべてのスイッチに自動的に展開されます。

ホストのエクスポート ポリシー

Cisco NDFC Web UI からホスト ポリシーをエクスポートを追加するには、以下の手順を実行します。

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [ホスト（Host）] > [ホスト ポリシー（Host Policies）]** を選択します。

[ホスト ポリシー（Host Policies）] ウィンドウが表示されます。

ステップ 2 ホスト ポリシーの **[エクスポート（Export）]** アイコンをクリックします。

通知ウィンドウが表示されます。

ステップ 3 ディレクトリの場所を選択し、ホスト ポリシーの詳細ファイルを保存します。

ステップ 4 [OK] をクリックします。

ホスト ポリシー ファイルがローカル ディレクトリにエクスポートされます。ファイル名には、ファイルがエクスポートされた日付が付加されます。エクスポート済みファイルのフォーマットは *.csv* です。

ポリシーの導入

ポリシーは、追加、編集、またはインポートされるたびにスイッチに自動的に展開されます。**[展開（Deployment）]** ドロップダウンリストで適切なアクションを選択することで、ポリシーの展開または再展開を選択できます。ポリシーの展開中にデバイスが再起動された場合、ポリシーは正しく展開されません。この場合、下の表に [ステータス（Status）] 列ぶ失敗メッセージが表示されます。

スイッチにカスタムポリシーを展開する前に、デフォルトのポリシーをスイッチに正しく展開する必要があります。そうしなかった場合、カスタムポリシーの展開に失敗します。カスタムポリシーを追加する前に、すべてのスイッチにすべてのデフォルトポリシーが正しく展開されていることを確認します。

選択したポリシーの展開

このオプションでは、デバイスに選択したポリシーのみを展開できます。必要に応じて他のポリシーを展開できます。

ポリシー名の横にある複数のチェックボックスを選択します。選択したポリシーをスイッチに展開するには、このオプションを選択します。

すべてのカスタム ポリシーの展開

このオプションでは、すべてのカスタムまたはユーザ定義ポリシーをスイッチに展開できます。スイッチがリブートしている場合でも、ポリシーは展開されます。このような場合、展開が失敗し、下の表にステータス メッセージ [失敗（Failed）] が表示されます。

1 つのインスタンスですべてのユーザ定義ポリシーを展開するには、このオプションを選択します。

選択したカスタム ポリシーの展開解除

ポリシー名の横にある複数のチェックボックスを選択します。ドロップダウンリストからこのオプションを選択して、選択したポリシーの展開解除をします。

すべてのカスタム ポリシーの展開解除

このオプションでは、1つのインスタンスですべてのカスタム ポリシーまたはユーザ定義ポリシーを展開解除できます。

Note デフォルトの設定済みポリシーを展開解除することはできません。

Note Cisco NDFC リリース 11.2(1) 以降では、デフォルト ポリシーを展開および展開解除することもできます。

すべての失敗したカスタム ポリシーのやり直し

ポリシーの展開は、さまざまな理由で失敗することがあります。このオプションを使用すると、失敗したすべてのユーザ定義ポリシーを展開できます。

以前に失敗したすべての展開は、それらのスイッチにのみ再度展開されます。以前失敗したすべての展開解除は、それらのスイッチのみから再度展開されます。

導入履歴

このオプションを使用すると、ポリシーの展開履歴を表示できます。

ポリシー名が [ポリシー名（Policy Name）] フィールドに表示されます。ドロップダウンリストから、このポリシーが展開されたスイッチを選択します。

スイッチの選択されたポリシーの展開履歴は、次の表に表示されます。

展開履歴の表には次のフィールドを表示します。

Table 8: ポリシー展開履歴の表フィールドと説明

フィールド	説明
展開ステータス	ポリシーの展開ステータスを表示します。 導入が成功したか失敗したかが表示されます。

フィールド	説明
展開アクション（Deployment Action）	ポリシーのスイッチで実行されるアクションを指定します。 **作成**：ポリシーがスイッチに展開されました。 **削除**：ポリシーがスイッチから展開解除されました。
展開の日時	ホスト ポリシーが最後に更新された日時を指定します。日時の表示形式は *Day MMM DD YYYY HH:MM:SS* タイムゾーン（*Timezone*） です。
Failed Reason	ポリシーが正常に展開されなかった理由を示します。

適用されたホスト ポリシー

Cisco NDFC リリース 11 以降、ネットワーク全体に適用したポリシーを表示できます。Cisco NDFC Web UI で、**[メディア コントローラ（Media Controller）] > [ホスト（Host）] > [適用されるホスト ポリシー（Applied Host Policies）]** に移動して、さまざまなポリシーを表示します。

テーブルには、デフォルトの PIM ポリシー、ローカル受信者ポリシー、および送信者ポリシーが表示されます。メディア コントローラは、ユーザー定義の PIM ポリシーまたはレシーバ外部ポリシーを表示しません。

次の表で、このページに表示されるフィールドを説明します。

Table 9: **適用されるホスト ポリシーのフィールドと説明**

列名	説明
ポリシー名	適用されるポリシーの名前を示します。
[ホストロール（Host Role）]	ホスト ロールを指定します。 ホスト デバイス ロールは、次のいずれかです。 • PIM • 送信者 • 受信側
スイッチ	ポリシーが適用されるスイッチの名前を指定します。

列名	説明
インターフェイス	ポリシーが適用されるインターフェイスを指定します。
アクティブ	ポリシーがアクティブかどうかを指定します。
タイム スタンプ	ポリシーが作成/展開された日時を指定します。 形式は Day, MMM DD YYYY HH:MM:SS（タイムゾーン）です。

フロー

フロー メニューには以下のサブメニューが含まれます。

Flow Status

（注） このセクションは、NDFC の IPFM と汎用マルチキャスト モードの両方に適用されます。

Cisco NDFC では、フローステータスを図的および統計的に表示できます。フロー ステータスは、**[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー ステータス（Flow Status）]** で確認できます。

汎用マルチキャスト モードでは、スイッチは受信者エンドポイントの IP アドレスではなく、受信者インターフェイスの IP アドレスを報告します。この IP は、**[フロー ステータス (Flow Status)]** および **[トポロジ (Topology)]** ウィンドウにホストとして表示されます。また、トラフィックのポリシングがないため、スイッチは「許可されたバイト/パケット」のみを報告し、「拒否されたバイト/パケット」は報告しません。

マルチキャスト NAT の可視化

NDFCでは、マルチキャストフローの既存のフロー分類（アクティブ、非アクティブ、送信者のみ、または受信者のみ）に従います。入力と出力の NAT が複数ある場合、入力アドレスと出力アドレスを同じグループに変換できます。NDFCは、送信者と受信者の組み合わせごとにこれらのフローを集約し、トポロジを介して NAT ルールを可視化します。

マルチキャスト NAT は IPFM ネットワークでサポートされます。通常のマルチキャストまたは汎用マルチキャストではサポートされません。

NATフローは、**[NAT検索 (NAT Search)]**フィールドを使用して検索できます。すべてのプレ/ポスト マルチキャストおよび送信元 IP アドレスは、**[フローステータス (Flow Status)]** ウィンドウには表示されません。アクティブなフロー ハイパーリンクをクリックすると、特定のフローの詳細をポップアップで表示できます。**NAT 検索**機能を使用すると、プレまたはポスト送信元/マルチキャスト グループの IP アドレスを入力し、関連するエントリをフィルタリング

できます。検索された IP アドレスは、対応するポップアップ ウィンドウに表示されるプレまたはポストエントリの一部である可能性があるため、フィルタリングが適用されているメインテーブルに表示されない場合があります。

入力を含む NAT タイプの NAT フローの場合、送信元とグループは NAT 返還後の送信元および NAT 返還後のグループになります。出力を含む NAT タイプの場合、送信元とグループは NAT 変換前の送信元と NAT 変換前のグループになります。NAT ルールは、**[送信者のみ (Sender Only)]** タブと **[受信者のみ (Receiver Only)]** タブに表示されます。

NAT フローの場合、トポロジ グラフのパス トレースには、入力 NAT を持つスイッチ上の **NAT** バッジと、出力 NAT の受信者へのリンク上の **NAT** ラベルが表示されます。

NAT フローの場合、トポロジ グラフ パネルの下に、関連するすべての入力 NAT または出力 NAT 情報を示す追加のテーブルがあります。NATフロー情報は、**[トポロジ (Topology)]** ウィンドウでも確認できます。

次のテーブルに、フィールドとその説明について情報を提供します。

フィールド	説明
NAT	NAT モード（入力、出力、または入力と出力）を示します。 入力 NAT タイプの場合、次の情報が表示されます。 入力 (S) (Ingress (S))：入力 NAT 変換が送信者スイッチ（ファースト ホップ ルータ（FHR）とも呼ばれる）で実行されることを示します。 入力 (R) (Ingress (R))：入力 NAT 変換が受信者スイッチ（ラスト ホップ ルータ（LHR）とも呼ばれる）で実行されることを示します。 入力 (S、R) (Ingress (S, R))：入力 NAT 変換が送信者スイッチと受信者スイッチの両方で実行されることを示します。
プレソース（Pre-Source）	NAT 変換前の送信元 IP アドレスです。
ポストソース（Post-Source）	NAT 変換後の送信元 IP アドレスです。
プレグループ（Pre-Group）	NAT 変換前のマルチキャスト グループを示します。
ポストグループ（Post-Group）	NAT 変換後のマルチキャスト グループを示します。
ポスト S ポート（Post S Port）	NAT 変換後の送信元ポートを示します。
ポスト DST ポート（Post DST Port）	NAT 変換後の宛先ポートを示します。

フィールドと説明

次の表では、[アクティブ (Active)] タブのフィールドについて説明します。

表 *10* : *[アクティブ（**Active**）]* タブ

フィールド	説明
IPFM および汎用マルチキャスト モードの共通フィールド	
マルチキャストIP	フローのマルチキャスト IP アドレスを示します。 （注） [マルチキャスト IP アドレス (Multicast IP address)] の横にあるウェーブリンクをクリックすると、フロー統計情報の図が表示されます。
NAT	フローが入力、出力、または入力および出力両方かを指定します。
フロー エイリアス (Flow Alias)	フロー エイリアスの名前を示します。
送信者	マルチキャスト グループの送信者の IP アドレスまたはホスト エイリアスを指定します。
送信者スイッチ (Sender Switch)	送信者スイッチがリーフまたはスパインのいずれであるかを示します。
送信者インターフェイス (Sender Interface)	送信者が接続しているインターフェイスを示します。
受信者スイッチ (Receiver Switch)	受信者スイッチがリーフまたはスパインのいずれであるかを示します。
受信者インターフェイス（Receiving Interface）	受信者が接続しているインターフェイスを示します。
フロー リンク ステート (Flow Link State)	フロー リンクの状態を示します。 アクティブリンクをクリックして、送信者および受信者のネットワーク図を表示します。 点線は、トラフィックのフローの方向を示します。情報を表示するには、ノードにカーソルを合わせます。右側のテーブルには、送信者と受信者に関する情報が表示されます。
送信開始時間（Sender Start Time）	送信者が参加してからの時間を表示します。
受信者参加時間（Receiver Join Time）	受信者が参加した時刻を示します。
IPFM モードに固有のフィールド	
優先度	フローのフロー プライオリティを示します。
ポリシング (Policed)	フローがポリシーの対象とされるかどうかを示します。

レシーバ	グループに参加している受信者のIPアドレスまたはホストエイリアスを示します。
帯域幅	トラフィックに割り当てられる帯域幅を示します。
QOS/DSCP	スイッチ定義の QoS ポリシーを示します。
ポリシー ID	マルチキャスト IP に適用されるポリシー ID を示します。
汎用マルチキャスト モード固有のフィールド	
受信者インターフェイス	グループに参加している受信者インターフェイスのIPアドレス示します。

次の表では、[非アクティブ (Inactive)] タブのフィールドについて説明します。

表 *11 : [*非アクティブ（*Inactive*）*]* タブ

フィールド	説明
IPFM および汎用マルチキャスト モードの共通フィールド	
マルチキャストIP	フローのマルチキャスト IP アドレスを示します。 （注） [マルチキャスト IP アドレス (Multicast IP address)] の横にあるウェーブ リンクをクリックすると、フロー統計情報の図が表示されます。
フローエイリアス (Flow Alias)	フロー エイリアスの名前を示します。
送信者	マルチキャスト グループの送信者のIPアドレスまたはホストエイリアスを指定します。
送信開始時間（Sender Start Time）	送信者が参加してからの時間を表示します。
受信者参加時間（Receiver Join Time）	受信者が参加した時刻を示します。
IPFM モードに固有のフィールド	
優先度	フローのフロー プライオリティを示します。
ポリシング (Policed)	フローがポリシーの対象とされるかどうかを示します。
レシーバ	グループに参加している受信者のIPアドレスまたはホストエイリアスを示します。
帯域幅	トラフィックに割り当てられる帯域幅を示します。
QOS/DSCP	スイッチ定義の QoS ポリシーを示します。
ポリシー ID	マルチキャスト IP に適用されるポリシー ID を示します。

障害の理由（Fault Reason）	非アクティブ フローの理由を示します。 送信者と受信者の両方の mroute が次のいずれかの組み合わせで存在する場合、Cisco NDFC は非アクティブになるフローを決定します。 • 受信者 IIF がヌル • 受信者 OIF がヌル • 送信者 IIF がヌル • 送信者 OIF がヌル このシナリオでは、スイッチに障害の理由はありません。したがって、このような非アクティブ フローの障害理由はありません。
汎用マルチキャスト モード固有のフィールド	
受信者インターフェイス	グループに参加している受信者インターフェイスの IP アドレス示します。

次の表では、[送信者のみ (Sender Only)] タブのフィールドについて説明します。

表 *12* : 送信者専用タブ

フィールド	説明
IPFM および汎用マルチキャスト モードの共通フィールド	
マルチキャストIP	フローのマルチキャスト IP アドレスを示します。
フロー エイリアス (Flow Alias)	フロー エイリアスの名前を示します。
送信者	送信者の名前を示します。
送信者スイッチ (Sender Switch)	送信者スイッチの IP アドレスを示します。
送信者入力インターフェイス（Sender Ingress Interface）	送信者入力インターフェイスの名前を示します。
フロー リンク ステート (Flow Link State)	フローリンクの状態（許可または拒否）を示します。
送信開始時間（Sender Start Time）	送信者スイッチが情報を送信してからの時間を表示します。
IPFM モードに固有のフィールド	
ポリシング (Policed)	フローがポリシーの対象とされるかどうかを示します。
ポリシー ID	マルチキャスト IP に適用されるポリシー ID を示します。

フィールド	説明
IPFM および汎用マルチキャスト モードの共通フィールド	
帯域幅	トラフィックに割り当てられる帯域幅を示します。

次の表では、[受信者のみ (Receiver Only)] タブのフィールドについて説明します。

表 *13 :* 受信者専用タブ

フィールド	説明
IPFM および汎用マルチキャスト モードの共通フィールド	
マルチキャストIP	フローのマルチキャスト IP アドレスを示します。
フロー エイリアス (Flow Alias)	フロー エイリアスの名前を示します。
名前	受信者 ID を示します。マルチキャスト受信者がリモートの場合、**[リモート (Remote)]** ラベルがその名前の横に表示されます。
受信者インターフェイス（Receiving Interface）	宛先スイッチインターフェイスの名前を示します。
受信者スイッチ (Receiver Switch)	受信者スイッチの IP アドレスを示します。
送信元固有の送信者	マルチキャスト送信者の IP アドレスを示します。
フロー リンク ステート (Flow Link State)	フロー リンクの状態（許可または拒否）を示します。
受信者参加時間（Receiver Join Time）	受信者が参加した時刻を示します。
IPFM モードに固有のフィールド	
ポリシー ID	マルチキャスト IP に適用されるポリシー ID を示します。
帯域幅	トラフィックに割り当てられる帯域幅を示します。

（注） スイッチで統計情報が有効になっている場合は、その統計情報のみがNDFCに表示されます。

統計データをさまざまな形式で表示するには、統計表示領域の **[表示 (Show)]** ドロップダウンリストをクリックします。

統計データをエクスポートするには、矢印をクリックします。`.csv` または `.pdf` 形式でエクスポートできます。

（注） Cisco NDFC はフロー統計値を NDFC サーバの内部メモリに保持します。したがって、NDFC の再起動または HA の切り替え後、フロー統計情報には以前に収集された値は表示されません。ただし、サーバの再起動または HA の切り替え後に収集されたフロー統計情報は表示できます。

NDFC で検出されたスイッチ間がアップリンクになる前に、新しいフローが参加すると、メッセージ BW_UNAVAIL が表示されます。これは、デバイスの検出後にスイッチ間のアップリンクが NDFC により検出されると、解決されます。

フロー エイリアス (Flow Alias)

（注） このセクションは、NDFC の IPFM と汎用マルチキャスト モードの両方に適用されます。

フロー エイリアス機能を使用して、マルチキャスト グループの名前を指定できます。マルチキャスト IP アドレスは覚えにくいため、マルチキャスト IP アドレスに名前を割り当てることで、名前に基づいてポリシーを検索および追加できます。

フロー エイリアスは、**[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー エイリアス（Flow Alias）]** で設定できます。

次の表で、このページに表示されるフィールドを説明します。

表 *14*：フロー エイリアス テーブルのフィールドと説明

フィールド	説明
フロー エイリアス (Flow Alias)	フロー エイリアスの名前を示します。
マルチキャストIPアドレス	トラフィックのマルチキャスト IP アドレスを指定します。
説明	フロー エイリアスに追加された説明です。
最終更新日	フロー エイリアスが最後に更新された日付を示します

この項の内容は、次のとおりです。

Add Flow エイリアス

Cisco NDFC Web UI からフロー エイリアスを追加するには、以下の手順を実行します。

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー エイリアス（Flow Alias）]** を選択します。

[フロー エイリアス（Flow Alias）] ウィンドウが表示されます。

ステップ 2 **[フロー エイリアスの追加（Add** Flow Alias）] アイコンをクリックします。

ステップ 3 **[フロー エイリアスの追加（Add Flow Alias）]** ウィンドウで、以下のフィールドのパラメータを指定します。

- **フロー名** : 固有のフロー エイリアス名を指定します。
- **マルチキャスト IP アドレス**：フロー エイリアスのマルチキャスト IP アドレスを入力します。
- **説明** : フロー エイリアスに追加する説明を指定します。

ステップ 4 **[保存 (Save)]** をクリックして、フロー エイリアスを保存します。

[キャンセル（Cancel）] をクリックして破棄します。

フロー エイリアスの編集

Cisco NDFC Web UI からフロー エイリアスを編集するには、以下の手順を実行します。

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー エイリアス（Flow Alias）]** を選択します。

[フロー エイリアス（Flow Alias）] ウィンドウが表示されます。

ステップ 2 編集する必要があるフロー エイリアス名の横にあるチェックボックスをオンにします。

ステップ 3 フロー エイリアスの **[編集（Edit）]** アイコンをクリックします。

ステップ 4 [フロー エイリアスの編集] ウィンドウで、**[名前（Name）]**、**[マルチキャスト IP（Multicast IP）]**、**[説明（Description）]** フィールドを編集します。

ステップ 5 **[保存（Save）]** をクリックして、新しい設定を保存します。

[キャンセル（Cancel）] をクリックして、変更を破棄します。

フロー エイリアスの削除

Cisco NDFC Web UI からフロー エイリアスを削除するには、以下の手順を実行します。

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー エイリアス（Flow Alias）]** を選択します。

[フロー エイリアス（Flow Alias）] ウィンドウが表示されます。

ステップ 2 削除が必要なフロー エイリアスの隣にあるチェックボックスをオンにします。

削除するフロー ポリシーを複数選択できます。

ステップ 3 フロー エイリアスの **[削除（Delete）]** アイコンをクリックします。

フロー エイリアスが削除されます。

フロー エイリアスのエクスポート

Cisco NDFC Web UI からホスト エイリアスを追加するには、以下の手順を実行します。

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー エイリアス（Flow Alias）]** を選択します。

[フロー エイリアス（Flow Alias）] ウィンドウが表示されます。

ステップ 2 フロー エイリアスの **[エクスポート（Export）]** アイコンをクリックします。

通知ウィンドウが表示されます。

ステップ 3 ディレクトリの場所を選択し、エイリアスの詳細ファイルを保存します。

ステップ 4 [OK] をクリックします。

フロー エイリアス ファイルがローカル ディレクトリにエクスポートされます。ファイル名には、ファイルがエクスポートされた日付が付加されます。エクスポート済みファイルのフォーマットは *.csv* です。

フロー エイリアスのインポート

Cisco NDFC Web UI からフロー エイリアスをインポートするには、以下の手順を実行します。

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー エイリアス（Flow Alias）]** を選択します。

[フロー エイリアス（Flow Alias）] ウィンドウが表示されます。

ステップ 2 フロー エイリアスの **[インポート（Import）]** アイコンをクリックします。

ステップ 3 ディレクトリを参照し、フロー エイリアス設定情報を含むファイルを選択します。

ステップ 4 [開く（Open）] をクリックします。

フローエイリアス設定がインポートされ、Cisco NDFC Web クライアントの **[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー エイリアス（Flow Alias）]** ウィンドウに表示されます。

フロー ポリシー

[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー ポリシー（Flow Policies）] でフロー ポリシーを設定できます。

デフォルト ポリシーが [フロー ポリシー（Flow Policy）] タブに表示されます。デフォルトでは、これらのポリシーの帯域幅は 0 です。デフォルトのフローポリシーに一致するフローがそれに応じて帯域幅と QOS/DSCP パラメータを使用するように、帯域幅を設定できます。設定を保存すると、ポリシーがすべてのデバイスに展開されます。

スイッチにカスタム フロー ポリシーを展開する前に、デフォルトのフロー ポリシーをスイッチに正常に展開する必要があります。そうしなかった場合、カスタムポリシーの展開に失敗します。カスタムポリシーを追加、編集、インポート、または展開する前に、すべてのスイッチにすべてのデフォルト ポリシーが正常に展開されていることを確認します。

（注） デフォルト ポリシーを展開解除すると、デフォルト値（Bandwidth:0gbps、DSCP:Best Effort、および Policer:Enabled）にリセットされます。

（注） ユーザがネットワーク オペレータ ロールで NDFC にログインすると、ポリシーを追加、削除、変更、インポート、エクスポート、または展開するためのすべてのボタンまたはオプションが無効になります。このユーザはポリシー、展開ステータスまたは履歴を確認することのみ、可能です。

次の表で、このページに表示されるフィールドを説明します。

表 *15 :* フロー ポリシーの操作

フィールド	説明
追加（Add）	新しいフロー ポリシーを追加できます。
編集	選択したフローポリシー パラメータを表示または編集できます。
削除	ユーザ定義のフローポリシーを削除できます。 （注） • デフォルト フロー ポリシーは削除できません。 • NDFC からそれらを削除する前に、すべてのスイッチからポリシーを展開解除します。
すべて削除	単一のインスタンスですべてのフローポリシーを削除できます。 （注） NDFC からそれらを削除する前に、すべてのスイッチからポリシーを展開解除します。
インポート	CSV ファイルからフロー ポリシーをインポートできます。 （注） インポート後、CSV ファイルからインポートされたすべてのポリシーは、すべての管理対象スイッチに自動的に適用されます。
エクスポート	CSV ファイルにフロー ポリシーをエクスポートできます。

フィールド	説明
デプロイ	

フィールド	説明
	[展開（Deployment）] ドロップダウン リストから、適切な値を選択します。 • [展開（Deploy）] • 選択したポリシー：このオプションを選択して、選択したポリシーをスイッチに展開します。 • すべてのデフォルト ポリシー：このオプションを選択して、すべてのデフォルト ポリシーをスイッチに展開します。 • すべてのカスタム ポリシー：このオプションを選択して、すべてのユーザ定義ポリシーを展開します。 • 展開解除 • 選択したポリシー：このオプションを選択して、選択したポリシーを展開解除します。 • すべてのデフォルト ポリシー：このオプションを選択して、デフォルトポリシーを展開解除します。 • すべてのカスタム ポリシー：このオプションを選択して、すべてのユーザ定義ポリシーを展開解除します。 • すべての失敗したポリシーを再試行する：このオプションを選択して、すべての失敗したポリシーを展開します。 以前にスイッチで失敗したすべての展開は、それらのスイッチにのみ再度展開されます。以前スイッチの展開解除が失敗した場合、同じスイッチからのみ再度展開解除ができます。 • 展開履歴：ドロップダウン リストからポリシーを 1 つ選択します。このオプションを選択して、選択したポリシーの展開履歴を表示します。 [展開履歴（Deployment History）] には、

フィールド	説明
	次のフィールドが表示されます。 • ポリシー名：選択したポリシー名を表示します。 • スイッチ名：ポリシーが展開されたスイッチ名を指定します。 • 展開ステータス：展開のステータスを表示します。導入が成功したか失敗したかが表示されます。 • フロー ポリシーのスイッチで実行されるアクションを指定します。 • **作成**：スイッチでポリシーが展開されていることを意味します。 • **削除**：スイッチでポリシーが展開解除されていることを意味します。 • 展開日時：ホスト ポリシーが最後に更新された日時を指定します。日時の表示形式は *Day MMM DD YYYY HH:MM:SS* タイムゾーン（*Timezone*）です。 • 失敗理由：ポリシーが正常に展開されなかった理由を示します。

表 *16 :* フロー ポリシー テーブルのフィールドと説明

フィールド	説明
ポリシー名	フロー ポシリー名を指定します。
マルチキャスト IP 範囲	トラフィックのマルチキャスト IP アドレスを指定します。
帯域幅	トラフィックに割り当てられる帯域幅を示します。
QoS/DSCP	スイッチ定義の QoS ポリシーを示します。
展開ステータス	フロー ポリシーが正常に展開されるか失敗するかを指定します。

フィールド	説明
展開アクション（Deployment Action）	ホスト ポリシーのスイッチで実行されるアクションを指定します。 • **作成**：ポリシーがスイッチで展開されます。 • **削除**：ポリシーがスイッチから展開解除されます。
使用中	フロー ポリシーが使用中かどうかを指定します。
Policer	フロー ポリシーを有効にするか無効にするかを指定します。 （注） フロー ポリシーの追加または編集では、デフォルトのポリサー状態は[有効（Enabled）]です。
最終更新日	フロー ポリシーが最後に更新された日時を指定します。 日時の表示形式は *Day MMM DD YYYY HH:MM:SS タイムゾーン（Timezone）* です。

（注） 新しいフロー ポリシーまたは編集されたフロー ポリシーは、次の状況でのみ有効です。

- 新しいフローが既存のフロー ポリシーと一致する場合。
- フローが期限切れになり、新しいポリシーがすでに追加または編集されている場合、フロー ポリシーと一致します。

この項の内容は、次のとおりです。

フロー ポリシーの追加

スイッチにカスタム ホスト ポリシーを展開する前に、デフォルトのホスト ポリシーをスイッチに正しく展開する必要があります。そうしなかった場合、カスタム ポリシーの展開に失敗します。カスタム ポリシーを追加する前に、すべてのスイッチにすべてのデフォルト ポリシーが正しく展開されていることを確認します。

Cisco NDFC Web UI からフロー ポリシーを追加するには、次の手順を実行します。

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー ポリシー（Flow Policies）]** を選択します。

[フロー ポリシー（Flow Policies）] ウィンドウが表示されます。

ステップ 2 フロー ポリシーの **[追加（Add）]** アイコンをクリックします。

ステップ 3 [フロー ポリシーの追加 (Add Flow Policy)] ウィンドウで、次のフィールドにパラメータを指定します。

- **ポリシー名**：フロー ポリシーの一意のポリシー名を指定します。
- **帯域幅**：フローポリシーに割り当てられる帯域幅を指定します。オプションボタンで、**[Gbps]** または **[Mbps]** を選択します。

ステップ 4 **[QoS/DSCP]** ドロップダウンリストから、適切な ENUM 値を選択します。

ステップ 5 **[ポリサー（Policer）]** トグル スイッチをクリックして、フローのポリサーを有効または無効にします。デフォルトでは、新しいフロー ポリシーのポリサーが有効になっています。

ステップ 6 [マルチキャスト IP 範囲 (Multicast IP Range)] のマルチキャスト範囲の開始 IP と 終了 IP のアドレスを入力します。

プラス（+） アイコンをクリックして、マルチキャスト範囲をポリシーに追加します。

ステップ 7 **[フロー プライオリティ (Flow Priority)]** ドロップダウン リストから、ポリシーのプライオリティを選択します。**[低（Low）]** または **[重大（Critical）]**.のどちらかを選択できます。デフォルトの値は **[低（Low）]** です。

フロー プライオリティは、次のシナリオで使用されます。

- エラー リカバリ：ユニキャスト ルーティング情報ベース（URIB）の到達可能性がフローに基づいて変更され、Re-Reverse-Path Forwarding（RPF）が実行されます。既存のフローのセットを再試行すると、**クリティカル (Critical)** プライオリティのフローからリカバリが開始されます。
- **[フローの再試行 (Flow Retry)]**：保留中のフローを再試行すると、クリティカル プライオリティのフローが最初に再試行されます。

（注）
[フロー プライオリティ（Flow Priority）] ドロップダウン リストは、Cisco NX-OS リリース 9.3(5) 以降のスイッチでのみ利用できます。

ステップ 8 **[展開（Deploy）]** をクリックして、新しいポリシーを展開します。

[キャンセル（Cancel）] をクリックして、変更を破棄します。

フロー ポリシーの編集

スイッチにカスタム フロー ポリシーを展開する前に、デフォルトのフロー ポリシーをスイッチに正常に展開する必要があります。そうしなかった場合、カスタムポリシーの展開に失敗します。カスタム ポリシーを編集する前に、すべてのスイッチにすべてのデフォルト ポリシーが正常に展開されていることを確認します。

Cisco NDFC Web UI からフロー ポリシーを追加するには、次の手順を実行します。

手順の概要

1. **[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー ポリシー（Flow Policies）]** を選択します。
2. 編集する必要があるフロー ポリシー名の隣にあるチェックボックスをオンにします。
3. フロー ポリシーの **[編集（Edit）]** アイコンをクリックします。
4. [フロー ポリシーの編集（Edit Flow Policy）] ウィンドウで、**[マルチキャスト IP（Multicast IP）]**、**[帯域幅（Bandwidth）]**、**[QoS/DSCP]** フィールドを編集します。
5. **[ポリサー（Policer）]** トグル スイッチをクリックして、フローポリシーのポリサーを有効または無効にします。
6. **[フロー プライオリティ (Flow Priority)]** ドロップダウン リストから、ポリシーのプライオリティを選択します。**[低（Low）]** または **[重大（Critical）]**.のどちらかを選択できます。デフォルトの値は **[低（Low）]** です。
7. **[展開（Deploy）]** をクリックして、新しいポリシーを展開します。

手順の詳細

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー ポリシー（Flow Policies）]** を選択します。

[フロー ポリシー（Flow Policies）] ウィンドウが表示されます。

ステップ 2 編集する必要があるフロー ポリシー名の隣にあるチェックボックスをオンにします。

ステップ 3 フロー ポリシーの **[編集（Edit）]** アイコンをクリックします。

ステップ 4 [フロー ポリシーの編集（Edit Flow Policy）] ウィンドウで、**[マルチキャスト IP（Multicast IP）]**、**[帯域幅（Bandwidth）]**、**[QoS/DSCP]** フィールドを編集します。

ステップ 5 **[ポリサー（Policer）]** トグル スイッチをクリックして、フロー ポリシーのポリサーを有効または無効にします。

ステップ 6 **[フロー プライオリティ (Flow Priority)]** ドロップダウン リストから、ポリシーのプライオリティを選択します。**[低（Low）]** または **[重大（Critical）]**.のどちらかを選択できます。デフォルトの値は **[低（Low）]** です。

フロー プライオリティは、次のシナリオで使用されます。

- エラー リカバリ：ユニキャスト ルーティング情報ベース（URIB）の到達可能性がフローに基づいて変更され、Re-Reverse-Path Forwarding（RPF）が実行されます。既存のフローのセットを再試行すると、**クリティカル (Critical)** プライオリティのフローからリカバリが開始されます。
- **[フローの再試行 (Flow Retry)]**：保留中のフローを再試行すると、クリティカル プライオリティのフローが最初に再試行されます。

（注）
[フロー プライオリティ（Flow Priority）] ドロップダウン リストは、Cisco NX-OS リリース 9.3(5) 以降のスイッチでのみ利用できます。

ステップ 7 **[展開（Deploy）]** をクリックして、新しいポリシーを展開します。

[キャンセル（Cancel）] をクリックして、変更を破棄します。

フロー ポリシーの削除

Cisco NDFC Web UI からフロー ポリシーを削除するには、以下の手順を実行します。

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー ポリシー（Flow Policies）]** を選択します。

[フロー ポリシー（Flow Policies）] ウィンドウが表示されます。

ステップ 2 削除する必要があるフロー ポリシー名の隣にあるチェックボックスをオンにします。

削除するフロー ポリシーを複数選択できます。

（注）
デフォルトのポリシーは削除できません。

ステップ 3 **[削除（Delete）]** アイコンをクリックして、選択したフロー ポリシーを削除します。

[すべて削除（Delete All）] アイコンをクリックして、単一インスタンスのすべてのフロー ポリシーを削除します。

フロー ポリシーのインポート

スイッチにカスタム フロー ポリシーを展開する前に、デフォルトのフロー ポリシーをスイッチに正常に展開する必要があります。そうしなかった場合、カスタム ポリシーの展開に失敗します。カスタム ポリシーをインポートする前に、すべてのスイッチにすべてのデフォルト ポリシーが正常に展開されていることを確認します。

Cisco NDFC Web UI からフロー ポリシーをインポートするには、以下の手順を実行します。

手順の概要

1. **[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー ポリシー（Flow Policies）]** を選択します。
2. **[インポート（Import）]** フロー ポリシー アイコンをクリックします。
3. ディレクトリを参照し、フロー ポリシー設定情報を含むファイルを選択します。
4. [開く（Open）] をクリックします。

手順の詳細

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー ポリシー（Flow Policies）]** を選択します。

[フロー ポリシー（Flow Policies）] ウィンドウが表示されます。

ステップ 2 **[インポート（Import）]** フロー ポリシー アイコンをクリックします。

ステップ 3 ディレクトリを参照し、フロー ポリシー設定情報を含むファイルを選択します。

ステップ 4 [開く（Open）] をクリックします。

フロー ポリシー設定がインポートされ、Cisco NDFC Web クライアントの **[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー ポリシー（Flow Policies）]** ウィンドウに表示されます。

インポートされたポリシーは、ファブリック内のすべてのスイッチに自動的に展開されます。

フロー ポリシーのエクスポート

Cisco NDFC Web UI からホスト ポリシーをエクスポートを追加するには、以下の手順を実行します。

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー ポリシー（Flow Policies）]** を選択します。

[フロー ポリシー（Flow Policies）] ウィンドウが表示されます。

ステップ 2 フロー ポリシーの **[エクスポート（Export）]** アイコンをクリックします。

通知ウィンドウが表示されます。

ステップ 3 ディレクトリの場所を選択し、フロー ポリシーの詳細ファイルを保存します。

ステップ 4 [OK] をクリックします。

フロー ポリシー ファイルがローカル ディレクトリにエクスポートされます。ファイル名には、ファイルがエクスポートされた日付が付加されます。エクスポート済みファイルのフォーマットは *.csv* です。

ポリシーの導入

ポリシーは、追加、編集、またはインポートされるたびにスイッチに自動的に展開されます。**[展開（Deployment）]** ドロップダウンリストで適切なアクションを選択することで、ポリシーの展開または再展開を選択できます。ポリシーの展開中にデバイスが再起動された場合、ポリシーは正しく展開されません。この場合、下の表に [ステータス（Status）] 列ぶ失敗メッセージが表示されます。

スイッチにカスタムポリシーを展開する前に、デフォルトのポリシーをスイッチに正しく展開する必要があります。そうしなかった場合、カスタムポリシーの展開に失敗します。カスタムポリシーを追加する前に、すべてのスイッチにすべてのデフォルトポリシーが正しく展開されていることを確認します。

選択したポリシーの展開

このオプションでは、デバイスに選択したポリシーのみを展開できます。必要に応じて他のポリシーを展開できます。

ポリシー名の横にある複数のチェックボックスを選択します。選択したポリシーをスイッチに展開するには、このオプションを選択します。

すべてのカスタム ポリシーの展開

このオプションでは、すべてのカスタムまたはユーザ定義ポリシーをスイッチに展開できます。スイッチがリブートしている場合でも、ポリシーは展開されます。このような場合、展開が失敗し、下の表にステータス メッセージ [失敗（Failed）] が表示されます。

1 つのインスタンスですべてのユーザ定義ポリシーを展開するには、このオプションを選択します。

選択したカスタム ポリシーの展開解除

ポリシー名の横にある複数のチェックボックスを選択します。ドロップダウンリストからこのオプションを選択して、選択したポリシーの展開解除をします。

すべてのカスタム ポリシーの展開解除

このオプションでは、1つのインスタンスですべてのカスタムポリシーまたはユーザ定義ポリシーを展開解除できます。

Note デフォルトの設定済みポリシーを展開解除することはできません。

Note Cisco NDFC リリース 11.2(1) 以降では、デフォルト ポリシーを展開および展開解除することもできます。

すべての失敗したカスタム ポリシーのやり直し

ポリシーの展開は、さまざまな理由で失敗することがあります。このオプションを使用すると、失敗したすべてのユーザ定義ポリシーを展開できます。

以前に失敗したすべての展開は、それらのスイッチにのみ再度展開されます。以前失敗したすべての展開解除は、それらのスイッチのみから再度展開されます。

導入履歴

このオプションを使用すると、ポリシーの展開履歴を表示できます。

ポリシー名が [ポリシー名（Policy Name）] フィールドに表示されます。ドロップダウンリストから、このポリシーが展開されたスイッチを選択します。

スイッチの選択されたポリシーの展開履歴は、次の表に表示されます。

展開履歴の表には次のフィールドを表示します。

Table 17: ポリシー展開履歴の表フィールドと説明

フィールド	説明
展開ステータス	ポリシーの展開ステータスを表示します。 導入が成功したか失敗したかが表示されます。
展開アクション（Deployment Action）	ポリシーのスイッチで実行されるアクションを指定します。 **作成**：ポリシーがスイッチに展開されました。 **削除**：ポリシーがスイッチから展開解除されました。
展開の日時	ホスト ポリシーが最後に更新された日時を指定します。日時の表示形式は *Day MMM DD YYYY HH:MM:SS* タイムゾーン（*Timezone*） です。
Failed Reason	ポリシーが正常に展開されなかった理由を示します。

スタティック フロー

[スタティックフロー（Static Flow）] ウィンドウを使用してスタティック受信機を設定します。

表 *18 :* スタティック フローの動作

フィールド	説明
スイッチ	**[範囲（SCOPE）]** に基づきスイッチを選択できます。
追加	スタティック フローを追加できます。
削除	スタティック フローを削除できます。

表 *19 :* スタティック フロー テーブルのフィールドと説明

フィールド	説明
VRF	スタティック フローの VRF を指定します。
グループ	スタティック フローのグループを指定します。
ソース言語	スタティック フローの送信元 IP アドレスを指定します。
[インターフェイス名（Interface Name）]	スタティック フローのインターフェイス名を指定します。スタティックフローの作成時に指定されていない場合は、**[N/A]** と表示されます。
展開アクション（Deployment Action）	ルールのスイッチで実行されるアクションを指定します。[作成（Create）]は、スタティック フローがスイッチに展開されたことを意味します。[Delete（削除）]は、スタティック フローがスイッチから展開解除されたことを意味します。
展開ステータス	スタティック フローが展開されているかどうかを示します。展開に失敗した場合は、情報アイコンにカーソルを合わせると、失敗の理由が表示されます。
最終更新日	スタティック フローが最後に更新された日時を示します。 日時の表示形式は Day MMM DD YYYY HH:MM:SS タイムゾーン（Timezone） です。

スタティック フローの追加

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [静的フロー（Static Flow）]** に移動します。

ステップ 2 [追加（Add）] アイコンをクリックします。

ステップ 3 **[スタティック フローの追加（Add Static Flow）]** ウィンドウで、次の情報を指定します。

スイッチ：スイッチ名を指定します。このフィールドは読み取り専用で、**[スタティック フロー（Static Flow）]** ウィンドウで選択されたスイッチに基づいています。

[グループ（Group）]：マルチキャスト グループを指定します。

[送信元（Source）]：送信元の IP アドレスを指定します。

[インターフェイス名（Interface Name）]：スタティック フローのインターフェイス名を指定します。このフィールドは任意です。インターフェイス名を指定しない場合、ホスト IP 0.0.0.0 が API に渡され、Null0 インターフェイスを使用して設定が作成されます。

ステップ 4 **[保存して展開（Save & Deploy）]** をクリックして、スタティック フローを保存します。

[キャンセル（Cancel）] をクリックして破棄します。

スタティック フローの削除

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [静的フロー（Static Flow）]** に移動します。

ステップ 2 削除する必要があるスタティック フローを選択し、**[削除（Delete）]** アイコンをクリックして、選択したスタティック フローを削除します。

RTP

（注） このセクションは、NDFC の IPFM と汎用マルチキャスト モードの両方に適用されます。

RTP メニューには、**RTP フロー モニタ** サブメニューが含まれています。

RTP フロー モニタ

Cisco NDFC では、すべてのアクティブな RTP ストリームのビューを提供しています。また、RTP のドロップがあるアクティブなフローと、同じものに関する履歴レコードも一覧表示します。アクティブ メディア フローの場合、NDFC はネットワークの損失を特定するための RTP トポロジを提供します。

（注） RTP フロー モニタを表示するには、スイッチでテレメトリを有効にする必要があります。詳細については、それぞれのプラットフォームのマニュアルを参照してください。

[RTP フロー モニタ（RTP Flow Monitor）] を表示するには、**[メディア コントローラ（Media Controller）] > [RTP] > [RTP フロー モニタ（RTP Flow Monitor）]** を選択します。

RTP フロー モニタ ウィンドウには、**[アクティブ（Active）]**、**[パケット ドロップ（Packet Drop）]**、および **[ドロップ履歴（Drop History）]**の 3 つのタブがあります。

これらのタブのフィールドの説明は次のとおりです。

フィールド	説明
スイッチ	スイッチの名前を示します。
インターフェイス	フローが検出されたインターフェイスを示します。
送信元 IP	フローの送信元 IP アドレスを示します。
送信元ポート	フローの送信元ポートを示します。
宛先 IP	フローの宛先 IP アドレスを示します。
宛先ポート	フローの宛先ポートを示します。
ビット レート	フローのビット レートを bps、kbps、mbps、gbps または tbp で示します。
パケットカウント	フローのパケット数を示します。
Packet Loss	失われたパケット数を示します。
損失開始	パケット損失が開始した時刻を示します。
損失終了	パケット損失が終了した時刻を示します。
開始時刻	フローが開始した時刻を示します。
プロトコル	フローで使用されているプロトコルを示します。

[テレメトリ スイッチ同期ステータス（Telemetry Switch Sync Status）] リンクをクリックすると、スイッチが同期しているかどうかを確認できます。**[同期ステータス（Sync Status）]** 列には、デバイスのステータスが表示されます。

アクティブ

[アクティブ（Active）] タブには、現在アクティブなフローが表示されます。これらのフローは、**[メディア コントローラ（Media Controller）] > [フロー（Flows）] > [フローステータス（Flow Status）]** に移動して表示することもできます。

テーブルの左上にある **[エクスポート（Export）]** アイコンをクリックして、アクティブ フローステータス データを .csv ファイルにエクスポートします。

パケット損失

[パケットドロップ（Packet Drop）] タブには、アクティブ フローのパケットドロップが表示されます。

テーブルの左上にある **[エクスポート（Export）]** アイコンをクリックして、パケット ドロップ データを .csv ファイルにエクスポートします。

[フロー トポロジ（Flow Topology）]

フロートポロジは、**[メディア コントローラ（Media Controller）]>[フローステータス（Flow Status）]** ウィンドウに表示されるアクティブ フローに表示されます。

エンドツーエンド フロート ポロジを表示するには、スイッチ リンクをクリックします。

フロートポロジは、送信者から受信者など、フローの方向を表示します。特定のフローに複数の受信者が存在する場合は、**[受信者の選択（Select Receiver）]** ドロップダウン リストから受信者を選択できます。

パケット ドロップが発生しているスイッチは、赤色の丸で囲まれています。

スイッチにカーソルを合わせると、次の詳細が表示されます。

- 名前
- IP address
- モデル
- パケット損失（存在する場合）

スイッチ間のリンクの横にある**ファイル**のアイコンをクリックすると、2 つのスイッチを接続しているインターフェイスのインターフェイス カウンタ エラーが表示されます。

ファイル アイコンをクリックすると、これらのスイッチ間でフローが参加しているインターフェイスに対して、**show interface <*interface name*> counters errors** コマンドが実行され、結果がポップインで表示されます。

[ドロップ履歴（Drop History）]

アクティブなRTPパケットドロップが確認されない場合、**[パケットドロップ（Packet Drop）]** タブのレコードは **[ドロップ履歴（Drop History）]** タブに移動されます。デフォルトでは、RTP ドロップ履歴は7日間保持されます。この設定をカスタマイズするには、**[管理**

（**Administration**）] > [**DCNM サーバ**（**DCNM Server**）] > [**サーバ プロパティ**（**Server Properties**）] ウィンドウで **pmn.elasticsearch.history.days** プロパティの値を更新します。

（注） **[ドロップ履歴**（**Drop History**）] タブには、最後の 100,000 レコードのみが表示されます。

テーブルの左上にある **[Server Properties]** アイコンをクリックして、.csv ファイルのパケットドロップ履歴データをエクスポートします。

AMQP ベースの通知については、『メディア展開のための Cisco NDFC IP - AMQP 通知』を参照してください。REST API については、『Cisco NDFC API リファレンス ガイド』を参照してください。

マルチキャスト NAT

Cisco NDFC リリース 11.5(1) から、NDFC IPFM モードでマルチキャスト NAT トランスレーションがサポートされています。着信トラフィック（入力）、または出力リンクまたはインターフェイスに NAT を適用できます。入力 NAT の範囲はスイッチ全体ですが、出力 NAT は特定のインターフェイス用です。同じスイッチに入力 NAT と出力 NAT の両方を設定できます。ただし、特定のスイッチの同じフロー上に存在することはできません。出力 NAT には、同じフローを最大40回複製する機能があります。この機能を実現するために、スイッチにサービス反映インターフェイスが定義されています。複数または単一の出力ポートに使用されます。

（注） 入力および/または出力 NAT 変換は、送信者スイッチ（ファースト ホップ ルータ（FHR）とも呼ばれる）と受信者スイッチ（ラスト ホップ ルータ（LHR）とも呼ばれる）でのみサポートされます。スパイン スイッチなどの中間ノードではサポートされません。

NAT について詳細は、『Cisco Nexus 9000 シリーズ NX-OS IP Fabric for Media ソリューション ガイド、リリース 9.3(x)』を参照してください。

前提条件

- PIM スパース モードでループバック インターフェイスを設定します。フローが変換される場合、RPF チェックが失敗しないように、変換後の送信元はこのループバックのセカンダリ IP アドレスである必要があります。このループバックは、NAT 用のサービス反映インターフェイスとして構成されます。VRF ごとにルックバックを設定する必要があります。

  ループバック インターフェイスを構成する例を次に示します。

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

```
ip service-reflect source-interface loopback10
```

- TCAM メモリ カービングを完了する必要があります。

  マルチキャスト NAT 用に TCAM を構成するコマンドは、次のとおりです。

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

  マルチキャスト NAT をサポートするスイッチ モデルについては、『Cisco Nexus 9000 シリーズ NX-OS IP fabric for Media ソリューションガイド』の「IPFM でマルチキャスト サービス リフレクションを構成する」を参照してください。

NAT モード

NAT モード オブジェクトは、スイッチおよび VRF ごとに作成されます。スイッチは、範囲に基づいてドロップダウンに入力されます。一覧表示するスイッチを選択し、対応する NAT モード オブジェクトを操作する必要があります。

表 *20 : NAT* モードの操作

フィールド	説明
スイッチ	**[範囲（SCOPE）]** に基づきスイッチを選択できます。
追加	新しい NAT モードを追加できます。
削除	NAT モードを削除できます。
インポート	NAT モードを CSV ファイルから NDFC にインポートできます。
エクスポート	NDFC から CSV ファイルに NAT ノードをエクスポートできます。

デプロイ	**[展開（Deployment）]** ドロップダウン リストから、適切な値を選択します。
	• [展開（Deploy）]
	  • 選択されたモード：このオプションを選択して、選択されたモードをスイッチに展開します。
	  • すべてのモード：このオプションを選択して、すべてのモードをスイッチに展開します。
	• 展開解除
	  • 選択されたモード：このオプションを選択して、選択されたモードを展開解除します。
	  • すべてのモード - このオプションを選択して、すべてのモードを展開解除します。
	• 失敗したすべてのモードを再実行：このオプションを選択して、失敗したすべてのモードを展開します。
	選択したスイッチで以前失敗したすべての展開が再度展開され、以前失敗したすべての展開解除がスイッチから再度展開解除されます。
	• 展開履歴：このオプションを選択して、選択したモード展開履歴を表示します。
	[展開履歴（Deployment History）] には、次のフィールドが表示されます。
	• スイッチ名：モードが展開されたスイッチの名前を指定します。
	• VRF：モードが展開された VRF の名前を指定します。
	• グループ：NAT モードのマルチキャスト グループを指定します。
	• モード：入力または出力の NAT モードを指定します。
	• 展開ステータス：展開のステータスを表示します。導入が成功したか失敗したかが表示されます。
	• アクション：モードのスイッチで実行されるアクションを指定します。作成は、モードがスイッチで展開されていることを意味します。削除は、モードがスイッチから展開解除されていることを意味します。
	• 展開日時：モードが最後に更新された日時を指定します。日時の表示形式は Day MMM DD YYYY HH:MM:SS タイムゾーン（Timezone） です。
	• 失敗理由：モードが正常に展開されなかった理由を示します。

表 *21 : NAT* モード フィールドと説明

フィールド	説明
VRF	NAT モードが展開されている VRF を指定します。
グループ	NAT モードのマルチキャスト アドレスを指定します。
モード	入力または出力マルチキャスト NAT モードを指定します。
展開アクション（Deployment Action）	モードのスイッチで実行されるアクションを指定します。作成は、モードがスイッチで展開されていることを意味します。削除は、モードがスイッチから展開解除されていることを意味します。
展開ステータス	モードが展開されているか否かを指定します。展開に失敗した場合は、情報アイコンにカーソルを合わせて失敗の理由を表示します。
最終更新日	モードが最後に更新された日時を指定します。 日時の表示形式は Day MMM DD YYYY HH:MM:SS タイムゾーン（Timezone） です。

NAT モードの追加

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [マルチキャスト NAT（Multicast NAT）] > [NAT モード（NAT Modes）]** に移動します。

ステップ 2 [追加（Add）] アイコンをクリックします。

ステップ 3 **[NAT モードの追加（Add NAT Mode）]** ウィンドウで、次の情報を指定します。

[モード（Mode）]：マルチキャスト NAT モード（**入力**または**出力**）を選択します。

スイッチ：スイッチ名を指定します。このフィールドは読み取り専用で、**[NAT モード（NAT Modes）]** ウィンドウで選択したスイッチに基づいています。

[VRF]：NAT モードが属する VRF を選択します。**出力** NAT モードでは、デフォルトの VRF が選択され、編集できません。

[グループ（Group/Mask）]：マスクでマルチキャスト グループを指定します。特定のスイッチでは、同じグループを出力NATにすることはできません。特定のグループまたはマスクが入力か出力かを識別する必要があります。

ステップ 4 **[保存して展開（Save＆Deploy）]** をクリックして、NAT モードを保存して展開します。

[キャンセル（Cancel）] をクリックしてこの変更を破棄します。

NAT モードの削除

NAT モードを削除しても、NAT モードはスイッチから展開解除されません。したがって、NDFC から削除する前にスイッチから NAT モードを展開解除するようにしてください。

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [マルチキャスト NAT（Multicast NAT）] > [NAT モード（NAT Modes）]** に移動します。

ステップ 2 削除する必要がある NAT モードを選択し、**[展開（Deployment）] > [展開解除（Undeploy）] > [選択したモード（Selected Modes）]** を選択します。

NAT モードが展開されていない場合、または失敗した場合は、この手順を省略できます。

ステップ 3 **[削除（Delete）]** アイコンをクリックして、選択した NAT ルールを削除します。

出力インターフェイス マッピング

表 *22:* 出力インターフェイス マッピング操作

フィールド	説明
スイッチ	**[範囲（SCOPE）]** に基づきスイッチを選択できます。
追加	出力インターフェイス マッピングを追加できます。
編集	出力インターフェイス マッピングを追加できます。
削除	出力インターフェイス マッピングを削除できます。
インポート	CSV ファイルから NDFC に出力インターフェイス マッピングをインポートできます。
エクスポート	NDFC から CSV ファイルから出力インターフェイス マッピングをエクスポートできます。

デプロイ	

[展開（Deployment）] ドロップダウン リストから、適切な値を選択します。

- [展開（Deploy）]
  - 選択した出力インターフェイス マッピング：このオプションを選択して、選択した出力インターフェイス マッピングをスイッチに展開します。
  - すべての出力インターフェイス マッピング：このオプションを選択して、すべての出力インターフェイス マッピングをスイッチに展開します。
- 展開解除
  - 選択した出力インターフェイス マッピング：このオプションを選択して、選択した出力インターフェイス マッピングを展開解除します。
  - すべての出力インターフェイス マッピング：このオプションを選択して、すべての出力インターフェイス マッピングを展開解除します。
- すべての失敗した出力インターフェイス マッピングを再試行する：このオプションを選択して、すべての失敗した出力インターフェイス マッピングを展開します。

選択したスイッチで以前失敗したすべての展開が再度展開され、以前失敗したすべての展開解除がスイッチから再度展開解除されます。

- 展開履歴：このオプションを選択して、選択した出力インターフェイスマッピングの展開履歴を表示します。

[展開履歴（Deployment History）] には、次のフィールドが表示されます。

- スイッチ名：出力インターフェイス マッピングが展開されたスイッチ名を指定します。
- 出力インターフェイス：マッピングが展開された出力インターフェイス名を指定します。
- マップインターフェイス：出力インターフェイスマッピングのマップインターフェイスを指定します。
- 最大レプリケーション：出力インターフェイスマッピングの最大レプリケーション数を指定します。
- 展開ステータス：展開のステータスを表示します。導入が成功したか失敗したかが表示されます。
- アクション：その出力インターフェイス マッピングに対してスイッチで実行されるアクションを指定します。作成は、マッピングがスイッチに展開されたことを意味します。削除は、マッピングがスイッチから展開解除されたことを意味します。

	• 展開日時：マッピングが最後に更新された日時を指定します。日時の表示形式は Day MMM DD YYYY HH:MM:SS タイムゾーン（Timezone） です。 • 失敗理由：マッピングが正常に展開されなかった理由。

表 *23 :* 出力インターフェイス マッピングのフィールドと説明

フィールド	説明
出力インターフェイス	マッピングの出力インターフェイスを指定します。
マップ インターフェイス	マップ インターフェイスを指定します。 出力インターフェイスとマップインターフェイスには、複数対1の関係があります。マッピングに複数の出力インターフェイスがある場合は、ハイパーリンクとして表示されます。インターフェイスの完全なリストを表示するには、ハイパーリンクをクリックします。
最大レプリケーション数	マップインターフェイスの最大レプリケーション数を指定します。
展開アクション（Deployment Action）	その出力インターフェイスマッピングに対してスイッチで実行されるアクションを指定します。[作成（Create）]は、出力インターフェイス マッピングがスイッチに展開されていることを意味します。[削除（Delete）] は、出力インターフェイス マッピングがスイッチから展開解除されたことを意味します。
展開ステータス	出力インターフェイスマッピングが展開されているかどうかを指定します。展開に失敗した場合は、情報アイコンにカーソルを合わせて失敗の理由を表示します。
最終更新日	出力インターフェイスマッピングが最後に更新された日時を指定します。 日時の表示形式は Day MMM DD YYYY HH:MM:SS タイムゾーン（Timezone） です。

出力インターフェイス マッピングの追加

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [マルチキャスト NAT（Multicast NAT）] > [出力インターフェイス マッピング（Egress Interface Mappings）]** に移動します。

ステップ 2 [追加（Add）] アイコンをクリックします。

ステップ 3 **[出力インターフェイス マッピングの追加/編集（Add/Edit Egress Interface Mapping）]** ウィンドウで、次の情報を指定します。

スイッチ：スイッチ名を指定します。このフィールドは読み取り専用で、**[出力インターフェイス マッピング（Egress Interface Mappings）]** ウィンドウで選択されたスイッチに基づきます。

出力インターフェイス：出力インターフェイスを指定します。1 つ以上の出力インターフェイスを選択できます。出力インターフェイスとマップ インターフェイスは、選択したスイッチに基づいて事前入力されます。

チェックボックスをオンにすることで複数の出力インターフェースを選択でき、選択したインターフェースが右側のボックスに表示されます。両方のフィールドには、使用可能な選択のみが表示されます。つまり、他のマッピングですでに定義されているインターフェイスは除外されます。すべてのインターフェイスを選択するには、**[すべて（All）]** を選択します。**[すべて（All）]** を選択すると、個々の出力インターフェイスを選択するリスト ボックスは無効になります。

[マップ インターフェイス（Map Interface）1]：マップ インターフェイスを指定します。インターフェイスは、出力インターフェイスまたはマップ インターフェイスのいずれかで、両方は使用できません。すでに出力インターフェイスとして選択されているマップ インターフェイスを選択すると、エラーが表示されます。

[最大レプリケーション（Max Replications）]：マップ インターフェイスの最大レプリケーション数を指定します。このフィールド値の範囲は 1 ～ 40 です。デフォルト値は 40 です。

ステップ 4 **[保存して展開（Save & Deploy）]** をクリックして、出力インターフェイスマッピングを保存し、展開します。

[キャンセル（Cancel）] をクリックして破棄します。

出力インターフェイス マッピングの編集

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [マルチキャスト NAT（Multicast NAT）] > [出力インターフェイス マッピング（Egress Interface Mappings）]** に移動します。

ステップ 2 出力インターフェイス マッピングを選択し、**[編集（Edit）]** をクリックします。

[出力インターフェイス マッピングの追加/編集（Add/Edit Egress Interface Mapping）] ウィンドウでは、出力インターフェイスと **[最大レプリケーション（Max Replications）]** フィールドを編集できます。**[最大レプリケーション（Max Replications）]** の新しい値を 1 ー 40 の範囲内で指定します。

ステップ 3 **[保存して展開（Save & Deploy）]** をクリックして、出力インターフェイスマッピングを保存し、展開します。

[キャンセル（Cancel）] をクリックして破棄します。

出力インターフェイス マッピングの削除

出力インターフェイス マッピングをマッピングを削除しても、出力インターフェイス マッピングはスイッチから展開解除されません。したがって、NDFCから削除する前に、スイッチから出力インターフェイス マッピングを展開解除します。

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [マルチキャスト NAT（Multicast NAT）] > [出力インターフェイス マッピング（Egress Interface Mappings）]** に移動します。

ステップ 2 削除する必要がある出力インターフェイス マッピングを選択し、**[展開（Deployment）] > [展開解除（Undeploy）] > [選択した出力インターフェイス マッピング（Selected Egress Interface Mappings）]** を選択します。

出力インターフェイス マッピングが展開されていないか、失敗した場合は、この手順をスキップできます。

ステップ 3 **[削除（Delete）]** をクリックして、選択した出力インターフェイス マッピングを削除します。

NAT ルール

NAT ルールは、イングレス NAT とエグレス NAT で同じですが、出力 NAT のレシーバ OIF も指定する必要があります。

表 *24 : NAT* ルールの操作

フィールド	説明
スイッチ	**[範囲（SCOPE）]** に基づきスイッチを選択できます。
追加	NAT ルールを追加できます。
削除	NAT ルールを削除できます。
インポート	CSV ファイルから NDFC に NAT ルールをインポートできます。
エクスポート	NDFC から CSV ファイルに NAT ルールをエクスポートできます。

デプロイ	[展開（Deployment）] ドロップダウン リストから、適切な値を選択します。
	• [展開（Deploy）]
	  • 選択したルール：このオプションを選択して、選択したNATルールをスイッチに展開します。
	  • すべてのルール：このオプションを選択して、すべてのNATルールをスイッチに展開します。
	• 展開解除
	  • 選択したルール：このオプションを選択して、選択したNATルールをスイッチに展開します。
	  • すべてのルール：このオプションを選択して、すべてのNATルールを展開解除します。
	• 失敗したすべてのルールを再実行：失敗したすべてのルールを展開するには、このオプションを選択します。
	選択したスイッチで以前失敗したすべての展開が再度展開され、以前失敗したすべての展開解除がスイッチから再度展開解除されます。
	• 展開履歴：このオプションを選択して、選択したルールの展開履歴を表示します。
	[展開履歴（Deployment History）] には、次のフィールドが表示されます。
	• スイッチ名：ルールが展開されたスイッチの名前を指定します。
	• VRF：マッピングが属する VRF を指定します。
	• 展開ステータス：展開のステータスを表示します。導入が成功したか失敗したかが表示されます。
	• アクション：ルールのスイッチで実行されるアクションを指定します。作成は、ルールがスイッチで展開されていることを意味します。削除は、ルールがスイッチから展開解除されていることを意味します。
	• 展開日時：ルールが最後に更新された日時を指定します。日時の表示形式は Day MMM DD YYYY HH:MM:SS タイムゾーン（Timezone） です。
	• 失敗理由：ルールが正常に展開されなかった理由を指定します。

表 *25 : NAT* ルールのフィールドと説明

フィールド	説明
VRF	NAT ルールの VRF を指定します。
モード	入力または出力の NAT モードを指定します。

事前変換グループ	NAT 変換前のマルチキャスト グループを示します。
変換後グループ	NAT 変換後のマルチキャスト グループを示します。
グループマスク	グループ マスクを指定します。
事前変換	NAT 変換前の送信元 IP アドレスです。
変換後の送信元	NAT 変換後の送信元 IP アドレスです。
送信元マスク	送信元マスクを指定します。
変換後の送信元ポート	NAT 変換後の送信元ポートを示します。範囲は、0 ～ 65535 です。値 0 は、UDP ソース ポートの変換がないことを意味します。
変換後の宛先ポート	NAT 変換後の宛先ポートを示します。値 0 は、UDP 宛先ポートの変換がないことを意味します。
静的 Oif	出力 NAT ルールをバインドする静的な発信インターフェイスを指定します。このドロップダウンには、**[出力インターフェイス マッピング（Egress Interface Mappings）]** ウィンドウで定義された出力インターフェイスが読み込まれます。このフィールドは入力モードには無効です。
展開アクション（Deployment Action）	ルールのスイッチで実行されるアクションを指定します。作成は、ルールがスイッチで展開されていることを意味します。削除は、ルールがスイッチから展開解除されていることを意味します。
展開ステータス	ルールが展開されているか否かを指定します。展開が失敗した場合、情報アイコンの上にマウスを置いて、失敗理由を表示します。
最終更新日	ルールが最後に更新された日時を指定します。 日時の表示形式は Day MMM DD YYYY HH:MM:SS タイムゾーン（Timezone） です。

NAT ルールの追加

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [マルチキャスト NAT（Multicast NAT）] > [NAT ルール（NAT Rules）]** に移動します。

ステップ 2 [追加（Add）] アイコンをクリックします。

ステップ 3 **[NAT ルールの追加（Add NAT Rule）]** ウィンドウで、次の情報を指定します。

スイッチ：スイッチ名を指定します。フィールドは読み取り専用で、**[NAT ルール（NAT Rules）]** ウィンドウで選択されたスイッチに基づきます。

[モード（Mode）]：NAT モード（入力または出力）を選択します。

[VRF]：NAT ルールの VRF を選択します。デフォルトでは、**デフォルト** の VRFです。

[変換前グループ（Pre-Translation Group）]：NAT の前のマルチキャスト グループを指定します。

[変換後グループ（Post-Translation Group）]：NAT 後のマルチキャスト グループを指定します。

[グループ マスク（Group Mask）]：NAT ルールのマスク値を指定します。デフォルトでは 32 です。

[変換前の送信元（Pre-Translation Source）]：NAT の前の送信元 IP アドレスを指定します。

[変換後の送信元（Post-Translation Source）]：NAT 後の送信元 IP アドレスを指定します。

（注）
RPF チェックが失敗しないようにするには、変換後の送信元 IP をループバック インターフェイスのセカンダリ IP アドレスにする必要があります。

[送信元マスク（Source Mask）]：NAT ルールの送信元マスク値を指定します。デフォルトでは 32 です。

[変換後の送信元ポート（Post-Translation Source Port）]：送信元ポートはデフォルトで 0 です。値 0 は変換なしを意味します。

[変換後の宛先ポート（Post-Translation Destination Port）]：デフォルトでは宛先ポートは 0 です。値 0 は変換なしを意味します。

[Statis Oif]：このフィールドは**入力**モードでは無効です。**出力**モードでは、定義された出力インターフェイス マッピングに基づいてインターフェイスに入力します。

ステップ 4 **[保存と展開（Save＆Deploy）]** をクリックして、NAT ルールを保存して展開します。

[キャンセル（Cancel）] をクリックして破棄します。

SG の組み合わせに対して作成できる入力ルールは 1 つだけですが、出力ルールの場合、SG に対して作成されるルールの数は、出力インターフェイス マッピングで定義された最大レプリケーション値に基づいています。

NAT ルールの削除

NAT ルールを削除しても、NAT ルールはスイッチから展開解除されません。したがって、NDFC から削除する前にスイッチから NAT ルールを展開解除するようにしてください。

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [マルチキャスト NAT（Multicast NAT）] > [NAT ルール（NAT Rules）]** に移動します。

ステップ 2 削除する必要がある NAT ルールを選択し、**[展開（Deployment）] > [展開解除（Undeploy）] > [選択した NAT ルール（Selected NAT Rules）]** を選択します。

NAT ルールが展開されていない場合、または失敗していた場合は、この手順をスキップできます。

ステップ 3 **[削除（Delete）]** アイコンをクリックして、選択した NAT ルールを削除します。

境界ルータ設定

[境界ルータ設定（Border Router Config）] ウィンドウで、ポートをマルチファブリック インターコネクトの境界ポートとして指定できます。

表 *26 :* 境界ルータ設定操作

フィールド	説明
スイッチ	**[範囲（SCOPE）]** に基づきスイッチを選択できます。
VRF	VRF を選択できます。
ステータス	境界ルータ設定のステータスを表示します。また、展開の日時、失敗の理由も表示されます。
履歴	境界ルータ設定の展開履歴を表示します。 [展開履歴（Deployment History）] には、次のフィールドが表示されます。 • スイッチ名：設定が展開されたスイッチの名前を指定します。 • VRF：設定が展開された VRF の名前を指定します。 • 展開ステータス：展開のステータスを表示します。導入が成功したか失敗したかが表示されます。 • アクション：設定のスイッチで実行されるアクションを指定します。展開は、設定がスイッチで展開されていることを意味します。展開解除は、設定がスイッチで展開解除されていることを意味します。 • 展開日時：設定が最後に更新された日時を指定します。日時の表示形式は Day MMM DD YYYY HH:MM:SS タイムゾーン（Timezone） です。 • 失敗理由：設定が正常に展開されなかった理由。
展開されているすべての境界ルータを表示する	展開されているすべての境界ルータを表示できます。
[保存（Save）]	インターフェイスに境界ルータの設定を保存できます。
[展開（Deploy）]	インターフェイスに境界ルータ設定を展開できます。
展開解除	インターフェイスの境界ルータ設定を展開解除できます。

表 *27:* 境界ルータ設定フィールドと説明

フィールド	説明
Interface Name	スイッチのインターフェイス名を指定します。
Admin Status	インターフェイスの管理ステータスを指定します。
動作ステータス	インターフェイスの操作ステータス。
境界ルータ	インターフェイスに境界ルータ設定が含まれているかどうかを指定します。
展開ステータス	境界ルータ設定が展開されているかどうかを指定します。展開に失敗した場合は、情報アイコンにカーソルを合わせると、失敗の理由が表示されます。

境界ルータ設定の展開

手順

ステップ 1 **[メディア コントローラ（Media Controller）] > [マルチキャスト NAT（Multicast NAT）] > [境界ルータ設定（Border Router Config）]** に移動します。

ステップ 2 対応するドロップダウン リストからスイッチと VRF を選択します。

ステップ 3 **境界ルータ設定テーブル**の**境界ルータ列**で、境界ルータ設定を展開する必要のあるインターフェイスに対して **[はい（Yes）]** を選択します。

ステップ 4 **[保存（Save）]** をクリックして、**[展開（Deploy）]** をクリックします。

既に指定されているポートの境界ポートの指定を削除するには、ドロップダウンから**[いいえ（No）]**を選択し、**[保存（Save）]** をクリックしてから **[展開（Deploy）]** をクリックします。すべての境界ポートの指定を削除するには、**[展開解除（Undeploy）]** をクリックします。

グローバル

グローバル メニューには次にサブメニューを含みます。

イベント

（注） このセクションは、NDFC の IPFM と汎用マルチキャスト モードの両方に適用されます。

Cisco NDFC では、ホストとフロー間のさまざまなイベントを表示および消去できます。イベントは、**[メディア コントローラ（Media Controller）] > [イベント（Events）]** に記録されます。

IPFM イベント テーブルはリアルタイムで更新されます。

保存される IPFM イベントの最大値とクリーンアップの頻度は、**[管理（Administration）] > [DCNM サーバ（DCNM Server）] > [サーバー プロパティ（Server Properties）]** ページで、**pmn.rows.limit** および **pmn.delete.interval** でそれぞれ指定できます。

次の表で、このページに表示されるフィールドを説明します。

フィールド	説明
消去	クリックして、古い/不要なイベントを削除します。 （注） NDFC サーバーが再起動すると、デフォルトでは、最大 5000 のイベント エントリが 6 時間保持されます。 ラジオ ボタンの 1 つをクリックして、[パージ（Purge）] オプションを選択します。 • **最大レコード数**：削除するレコードの最大数を入力します。 • **日数**：イベントを削除する必要がある日数を入力します。 • **前の日付からすべてのデータを削除する**：すべてのデータを削除する日付を指定します。 **[パージ（Purge）]** をクリックして、IPFM イベント情報を削除または保持します。
カテゴリ（Category）	イベント カテゴリかどうかを指定します。
シビラティ（重大度）	イベントのシビラティ（重大度）を指定します。
説明	イベントの説明を指定します。 サンプルの説明は次のように表示されます。 `FlowRequest のフローを作成しています: flowRequest は hostId 用です: <<IP_Address>> hostInterface:<<Host_Int_ID>> mcastIp:<<Multicast IP>> がスイッチから発信されていますか: <<Host IP Address>>`
影響を受けるフロー	このイベントにより影響を受けるフローを指定します。
前回の更新時刻	イベントが最後に変更された日時を指定します。 日時の表示形式は *Day MMM DD YYYY HH:MM:SS* タイムゾーン（*Timezone*） です。

フィールド	説明
エクスポート	イベントをローカル ディレクトリ パスにダウンロードできます。 ファイル名には、ファイルがエクスポートされた日付が付加されます。エクスポートされるファイルの形式は `.xls` です。

設定を実行するスイッチをスタートアップ設定にコピーする

NDFCを介したスイッチへの展開がある場合は常に、スイッチの実行コンフィギュレーションがスタートアップコンフィギュレーションに自動的に保存されます。つまり、NDFCは、展開の直後にスイッチで **copy r s** コマンドを呼び出して、スイッチのリロード間で設定が保持されるようにします。カテゴリ「CopyRS」のイベントは、**copy rs** コマンドが呼び出されたとき、およびコマンドが正常またはエラーで完了したときに、**[メディア コントローラ（Media Controller）] > [イベント（Events）]** に記録されます。

成功すると、イベントの説明が次のように記録されます。

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

失敗した場合、イベントの説明は次のように記録されます。

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

リアルタイム通知

NDFC は、イベントおよび AMQP 通知を介して障害通知を提供します。重要な障害通知は、リソースが利用できないために、フローがファブリック内でエンド ツー エンドで確立できない場合です。リアルタイムの障害通知は、次のような場合に障害が解決されると削除されます。

- フローが確立したとき。
- フローを確立するためのリクエストが完了したとき。

NDFC リリース 11.5(1) から、フローの作成と削除が成功すると、リアルタイム通知が送信されます。何らかの理由でフローがエンド ツー エンドで確立されていない場合、このイベントベースの通知は生成されません。代わりに、障害通知が生成されます。

スイッチは、IGMP Joinを受信すると、フローをプロビジョニングする前に、帯域幅、ポリサーの可用性、ホスト ポリシーの構成などのシステム リソースをチェックします。いずれかのリソースが使用できない場合、フローはエンド ツー エンドで確立されません。テレメトリを通じて、NDFC はイベントベースの通知を登録します。NDFC はさらに、通知に対応する AMQP メッセージを生成します。

AMQPの場合、イベントを取得するためのキューを作成する必要があります。このキューを交換にバインドする必要があります。この場合、それは **DCNMExchange** です。このルーティング キーを使用して、リアルタイム通知を取得します。
error.com.cisco.dcnm.event.pmn.realtime.switch。フロー イベントの作成または削除に関するリ

アルタイム通知を取得するには、ルーティング キー **information.com.cisco.dcnm.event.pmn.realtime.switch** を使用します。

これらの通知は、**[メディア コントローラ（Media Controller）] > [グローバル（Global）] > [イベント（Events）]** ウィンドウの Cisco NDFC Web UI でも利用できます。エラーが発生すると、**エラー**として表示されます。障害が削除またはクリアされるたびに、**情報**として表示されます。**[説明（Description）]** 列のエントリには、ファブリックまたはスコープ名、スイッチ ID、および一意の障害識別子が含まれています。**[最終更新時刻（Last Update Time）]** 列には、イベントが生成された時刻が表示されます。

しきい値通知

NDFC は、次のシナリオでしきい値通知を生成します。

- インターフェイス使用率が特定のしきい値に達した。
- アンダー/オーバーのフローが割り当てられた帯域幅を利用した。

条件が解決されると、通知は削除されます。

スイッチにフローをプロビジョニングすると、NDFC はインターフェイスの使用状況をチェックし、次の使用状況に基づいてアラートを生成します。

- 60% ～ 74% ：警告
- 75% ～ 89%：深刻
- 90% 以上：重大

フロー帯域幅通知は、スイッチが 1 分ごとにフロー統計をチェックし、統計を比較することでレートを計算します。シナリオは次のとおりです。

- レートが設定されたフロー ポリシー帯域幅の 60 % 未満の場合、通知が生成されます。
- レートが構成された帯域幅を超える場合、つまり 100 % を超える場合、通知が生成されます。
- 率が 60 % から 100 % の範囲に戻ると、通知が削除されます。

設定

設定メニューには以下のサブメニューが含まれます。

NDFC 向け SNMP サーバーの設定

スイッチを NDFC インベントリに追加すると、スイッチが SNMP トラップの送信先を認識できるように、NDFC は自動的に次の設定でスイッチを設定します：snmp-server host dcnm-host-IP traps version 2c public UDP port - 2162

コントローラ展開を計画している場合は、次の手順に従って、スイッチからNDFCへの接続を確立します。

Procedure

ステップ 1 NDFCがスイッチからSNMPトラップを確実に受信するには、**[管理者（Administrator）]>[サーバー プロパティ（Server Properties）]** でNDFCサーバー プロパティ `trap.registaddress=dcnm-ip` を設定して、スイッチがSNMPトラップを送信するIPアドレス(またはネイティブHAのVIPアドレス)を指定します。

ステップ 2 インバンド環境の場合、Cisco NDFCアプリケーションと一緒にパッケージ化されている `pmn_telemetry_snmp` CLIテンプレートを使用して、スイッチでさらに多くのSNMP設定を構成します。詳細については、「スイッチのグローバル設定, on page 174」を参照してください。

AMQP 通知

すべてのNDFC操作(ホストエイリアス、ホストポリシーなど)について、AMQP通知が送信されます。スイッチによってトリガされ、テレメトリを介して受信されたすべての操作（たとえば、フロー確立）の場合、Cisco NDFCは定期的に新しいイベントをチェックし、適切な通知を生成します。この期間は、`server.properties` で「AMQP_POLL_TIME」値を設定することで構成できます。

`server.properties` ファイルを更新してAMQPポーリング間隔を変更するには、次の手順を実行します。

1. 次の場所にある `server.properties` ファイルを見つけます。

   ```
   /usr/local/cisco/dcm/fm/conf/
   ```

2. 必要なポーリング間隔に基づいて、AMQP_POLL_TIME行を編集します。ポーリング間隔は分単位です。

   ```
   AMQP_POLL_TIME=5
   ```

   ポーリング間隔は5分に設定されています。デフォルトでは、ポーリング間隔は2分間に設定されています。

3. 次のコマンドを使用して、NDFCサーバーを再起動して、`server.properties` ファイルで行った変更を適用します。

   appmgr restart dcnm：スタンドアロン展開

   appmgr restart ha-apps：ネイティブHA展開の場合

Note NDFC 11.5(1) より前は、AMQP クライアントが HTTP でアクセスできるように、セキュリティで保護されていない AMQP ブローカー ポート 5672 がデフォルトで開いており、NDFC の iptables.save ファイルに保存されていました。NDFC 11.5(1) 以降、ポート 5672 はデフォルトで閉じられており、AMQP クライアントは HTTP でアクセスできます。

AMQP 通知コンポーネント

- **ルーティングキー**

  ルーティング キーは、交換がメッセージのルーティング方法を決定するために使用できるアドレスです。これは HTTP の URL に似ています。ほとんどの交換タイプはルーティング キーを使用してルーティング ロジックを実装しますが、ユーザはそれを無視して、メッセージ コンテンツなどの他の基準でフィルタリングすることを選択できます。NDFC IPFM には、さらにメッセージ ヘッダ プロパティにルーティング キー基準が含まれています。

- **ルーティング キーの形式**

  オブジェクト通知用の NDFC IPFM AMQPのルーティング キーの形式は次のとおりです：`Severity.Operation.ObjectType`

  例: `info.com.cisco.dcnm.event.pmn.create.host`

キー識別子	詳細
重大度	メッセージのシビラティ（重大度） (情報/警告/エラー)
オペレーション	作成/更新/削除/検出/適用/確立/展開/スイッチリロード/NDFC
オブジェクトタイプ	通知に関係するオブジェクトには、ホスト エイリアス、ホスト、ホスト ポリシー、フロー ポリシー、フロー、スイッチ、NDFC が含まれます。

- **メッセージ プロパティ**

  メッセージには、コンテンツの解析に使用できる次のプロパティとヘッダが含まれます。

プロパティ	値
プライオリティ	メッセージの優先度デフォルト値は 0 です。
delivery_mode	メッセージに使用される配信モード。デフォルト値は 2 (永続) です。これは、メッセージがメモリ内とディスクの両方に保存されることを意味します。

プロパティ	値
content_encoding	UTF-8
content_type	メッセージ コンテンツの MIME タイプ。デフォルト値は application/json です。
headers	メッセージに関する名前と値のペアのリスト。 • シビラティ（重大度）―メッセージのシビラティ（重大度）（情報/警告/エラー）。 • 操作ステータス―成功/失敗。 • 操作：作成/更新/削除/検出/適用/確立/展開/スイッチリロード/NDFC。 • 一括：True/False は、一括操作を示します。 • タイプ：ホスト エイリアス、ホスト、ホストポリシー、フローポリシー、フロー、スイッチ、NDFC などの通知に関連するオブジェクト。 • ユーザー：アクションを実行したログイン ユーザ。 • イベント：メッセージが送信されました (下位互換性のため)。
message_id	メッセージID

- **通知本文**

  NDFC 通知ペイロードには、通知をトリガーするリソースを識別するために必要な情報と、詳細情報を取得するためのリンクが含まれています。操作が失敗した場合、通知には詳細な理由とともにエラー メッセージが含まれます。

スイッチのグローバル設定

リリース 11 より前のリリースでは、Cisco NDFC メディア コントローラは、帯域幅の管理、フローのステッチ、ホスト リンク帯域幅などの操作を実行していました。リリース 11 以降、NDFC では 2 つの主要な操作が可能です。

- ネットワークを監視します。

- ホストおよびフロー ポリシーを構成します。

NDFCは、テレメトリを使用して、フローステータス、検出されたホスト、適用されたホストポリシー、およびその他の操作をモニタします。スイッチによってトリガされ、テレメトリを介して受信されたすべての操作（たとえば、フロー確立）の場合、NDFCは定期的に新しいイベントをチェックし、適切な通知を生成します。

スイッチ リロード中に `pmn.deploy-on-import-reload.enabled` サーバ プロパティがtrueに設定されている場合、NDFCがスイッチのcoldStartSNMPtrapを受信すると、「Deployment Status=Successes」を示すグローバル設定、およびホストとフローポリシーが自動的にスイッチにプッシュされます。スイッチ テレメトリおよびSNMP設定は、**[設定（Configure）] > [テンプレート（Templates）] > [テンプレート ライブラリ（Template Library）]** 経由でNDFCパッケージ化された `pmn_telemetry_snmp` CLIテンプレートを使用して展開できます。

[Cisco DCNM Web UI] > [メディア コントローラ（Media Controller）] > [グローバル（Global）] > [設定（Config）] に移動して、スイッチ グローバル設定およびWANリンクを設定または変更できます。

NDFCがメディア コントローラ展開モードでインストールされている場合、**[Web UI] > [メディア コントローラ（Media Controller）] > [グローバル（Global）] > [設定（Config）]** を使用して、ユニキャスト帯域幅、任意のソース マルチキャスト(ASM)範囲、およびWANリンクのポリシーを展開できます。

メディア コントローラ モードのNDFCを展開した後、帯域幅とASMを設定します。帯域幅の残りの割合は、マルチキャスト トラフィックによって使用されます。NDFCはマスター コントローラのように動作し、ファブリック内のすべてのスイッチに帯域幅とASMの構成を展開します。

[Cisco DCNM Web UI] > [メディア コントローラ（Media Controller）] > [グローバル（Global）] > [設定（Config）] > [スイッチ グローバル設定（Switch Global Config）] に移動して、グローバル パラメータを設定します。

Note NDFCのネットワーク オペレータ ロールを持つユーザーは、ASMを保存、展開、展開解除、追加または削除したり、ユニキャスト帯域幅予約の割合を編集したりすることはできません。

AMQP通知

Cisco NDFCはファブリックからデータを取得するためにテレメトリを使用するため、フローステータスとAMQP通知にリアルタイムの現在の状態が反映されない場合があります。定期的に新しいイベントをチェックし、適切な通知を生成します。また、フローは単一のスパインに限定されなくなり、NまたはWまたはMの形状を取ることができます。ホスト ポリシーは、ジャストインタイム(JIT)ではなく、スイッチインターフェイス構成に基づいて適用されます。これらすべてのアーキテクチャの変更は、現在のAMQPメッセージとトリガ時間に影響します。デフォルトで、投票間隔は2分間に設定されています。詳細については、「AMQP通知, on page 172」を参照してください。

ユニキャスト帯域幅予約

帯域幅の専用のパーセンテージをユニキャストトラフィックに割り当てるようにサーバを構成できます。残りのパーセンテージは、マルチキャストトラフィックに自動的に予約されます。

[ユニキャスト帯域幅予約 (%)] フィールドに、数値を入力して帯域幅を設定します。

受信者のみに帯域幅を予約する

以前の NDFC リリースでは、スイッチは常に ASM トラフィックをスパインにプルして、フローのセットアップ時間を短縮していました。ただし、アクティブなレシーバがない場合、これは不必要にスパイン帯域幅を占有します。Cisco NDFC リリース 11.4(1) 以降では、**[受信者のみに対する帯域幅の予約（Reserve Bandwidth to Receiver Only）]** チェックボックスをオンにして、受信者がいる場合にのみ ASM トラフィックをスパインにプッシュできます。この機能は、Cisco NX-OS リリース 9.3(5) 以降のスイッチに適用できます。

ASM 範囲

Any Source Multicast（ASM）は PIM ツリー構築モードの 1 つです。新しい送信元および受信者を検出する場合には共有ツリーを、受信者から送信元への最短パスを形成する場合は送信元ツリーを使用します。ASM はマルチキャスト送信元を検出します。

IP アドレスとサブネット マスクを指定して、ASM 範囲を構成できます。

[ASM/マスク（ASM/Mask）] フィールドに、マルチキャスト ソースを定義する IP アドレスとサブネット マスクを入力します。**[追加（Delete）]** アイコンをクリックして、マルチキャストアドレスを ASM 範囲に追加します。複数の ASM 範囲を追加できます。ASM 範囲を削除するには、テーブルの ASM/マスクの横にあるチェック ボックスをオンにして、**[削除（Delete）]** アイコンをクリックします。

ユニキャスト帯域幅予約と ASM 範囲を設定したら、次の操作を実行して、これらの設定をスイッチに展開できます。

Table 28: **グローバル設定画面の操作**

アイコン	説明
保存（Save）	[保存（Save）] をクリックして、設定を保存します。

アイコン	説明
[展開（Deploy）]	設定を展開するには、ドロップダウン リストから次のいずれかを選択できます。 • **すべて**：ASM、ユニキャスト帯域幅、および予約済み帯域幅の設定をすべてのスイッチに展開します。 • **ユニキャスト BW** ：ユニキャスト帯域幅設定のみを展開します。 • **予約 BW**：予約帯域幅設定のみを展開します。 • **ASM**：ASM 設定のみを展開します。 • **すべて失敗**：失敗したすべての展開を展開します。 テーブル内の各 ASM 範囲の横に、成功または失敗のメッセージが表示されます。
展開解除	設定を展開解除するには、ドロップダウン リストから次のいずれかを選択します。 • **すべて**：ASM、ユニキャスト帯域幅、および予約済み帯域幅の設定をすべてのスイッチに展開解除します。 • **ユニキャスト BW** ：ユニキャスト帯域幅設定のみを展開解除します。 • **予約 BW**：予約帯域幅設定のみを展開解除します。 • **ASM**：ASM設定のみを展開解除します。
ステータス	帯域幅予約ステータスは、帯域幅の展開が成功したか、失敗したか、展開されていないかを示します。 [ASM/マスク ステータス（ASM/Mask Status）] フィールドには、ASM とマスクの設定が正常に展開されたか、失敗したか展開されていないかが表示されます。
履歴	それぞれの [履歴（History）] リンクをクリックして、ユニキャスト帯域幅と ASM の展開の展開履歴を表示します。

次のテーブルは、[展開履歴（Deployment History）] で表示されるフィールドを説明しています。

Table 29: [*展開履歴（Deployment History***）*** *] フィールドと説明***

フィールド	説明
スイッチ名	設定が展開されたファブリックのスイッチ名を指定します。
アクション	スイッチで実行されるアクションを指定します。**[展開（Deploy）]** または **[展開解除（Undeploy）]**
展開ステータス	展開のステータスを表示します。導入が成功したか失敗したかが表示されます。
展開の日時	展開が初期化される日時を表示します。
Failed Reason	展開が失敗した理由を指定します。

フィールド	説明
表示	ドロップダウン リストから適切なフィルタを選択します。 • クイック フィルタ：すべての列に検索フィールドが表示されます。フィルタリングする検索文字列を入力できます。 • 高度なフィルタ：[高度なフィルタ（Advanced Filter）] 画面で、[一致（Match）] フィールドの [すべて（All）] または [すべて（Any）] ラジオ ボタンを選択します。[検索フィルタ（Select Filter）] フィールドで、ドロップダウン リストからカテゴリを選択します。次のフィールドのドロップダウン フィールドから適切な条件を選択します。次のフィールドに検索文字列を入力します。 **[追加（Add）]**アイコンをクリックし、別のフィルタを追加します。**[削除（Remove）]**アイコンをクリックし、フィルタを削除します。すべてのフィルタをクリアするには、**[消去（Clear）]** をクリックします。**[適用（Apply）]**をクリックしてフィルタをアクティブにし、フィルタ処理されたイベントを表示します。**[保存（Save）]** をクリックし、適切されたフィルタを保存します。高度なフィルターを破棄するには、**[キャンセル（Cancel）]** をクリックします。 • すべて - すべてのフィルタを削除し、完全な展開履歴を表示します。 • プリセット フィルタの管理 - ドロップダウン リストから適切なフィルタを選択します。 [編集（Edit）] をクリックして、フィルタパラメータを変更します。**[削除（Remove）]** をクリックし、フィルタを削除します。**[キャンセル（Cancel）]** をクリックして変更を破棄し、展開履歴に戻ります。

フィールド	説明
合計	[展開履歴（Deployment History）] ページにイベントの総数を表示します。

グローバル設定を展開したら、ネットワーク内の各スイッチの WAN を設定します。

インターフェイス設定

リリース 11 以降、Cisco NDFC Web UI では、ファブリック内の各スイッチに WAN リンクを設定できます。

外部エンド デバイスは、ボーダー リーフおよび PIM ルータを介してネットワークに接続できます。PIM ルータをボーダー リーフに接続するインターフェイスは、WAN リンクと呼ばれます。

Note NDFC 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。

1. **[スイッチの選択（Select a Switch）]** ドロップダウン リストから、WAN リンクを確立するか、ユニキャスト帯域幅を予約するファブリック内のスイッチを選択します。

   スイッチのインターフェイスのリストは、次の表に入力されています。

Note ファブリックの一部であるスイッチがドロップダウン リストに表示されます。

2. [WAN リンク（WAN Links）] 列で、ドロップダウン リストから **[はい（Yes）]** または **[いいえ（No）]** を選択して、インターフェイスを WAN リンクとして指定します。
3. **[展開されたすべてのインターフェイスを表示（View All Deployed Interfaces）]** をクリックして、WAN リンクとして設定されているか、帯域幅を予約されているスイッチ名、スイッチの IP アドレス、およびインターフェイス名を表示します。適切なフィルターを選択して、展開されたインターフェースを表示できます。
4. **[ユニキャスト帯域幅 %（Unicast BW %）]** 列では、ユニキャスト トラフィックに専用の帯域幅の割合を割り当てるようにインターフェイスを設定できます。残りのパーセンテージは、マルチキャスト トラフィックに自動的に予約されます。インターフェイスのこの列に数値またはデフォルトの**該当しない**値を入力します。

   インターフェイスごとにユニキャスト帯域幅を設定すると、グローバル ユニキャスト帯域幅予約よりも優先されます。
5. **[保存（Save）]** をクリックして、選択したインターフェイスを WAN リンクとして保存し、その他の設定変更を保存します。

6. **[展開（Deploy）]** をクリックし、WAN リンクとしてインターフェイスを設定します。
7. **[展開解除（Undeploy）]** をクリックして、WAN リンクを削除するか、スイッチからユニキャスト帯域幅を構成解除します。

次の表で、このページに表示されるフィールドを説明します。

***Table 30: WAN* リンク テーブル フィールドおよび説明**

フィールド	説明
ステータス	選択したスイッチで WAN リンクまたはユニキャスト帯域幅を展開するか展開しないかを指定します。
履歴	このリンクをクリックして、展開履歴を表示します。 このページに表示されるフィールドの説明については、以下の表を参照してください。
[インターフェイス名（Interface Name）]	エンド デバイスに WAN リンクとして接続されているインターフェイスを指定します。このインターフェイスはレイヤ 3 になります。
Admin Status	上矢印はステータスが上がっていることを示しています。下矢印はステータスが下がっていること意味します。
動作ステータス	上矢印はインターフェイスの稼働状態が上がっていることを示しています。下矢印はステータスが下がっていること意味します。
WAN リンク	ドロップダウン リストから、WAN リンクとしてこのインターフェイスを指定するように選択できます。 • **[はい（Yes）]** を選択し、WAN リンクとしてインターフェイスを設定します。 • **[いいえ（No）]** を選択し、WAN リンクとしてインターフェイスを削除します。
ユニキャスト帯域幅 %	帯域幅の専用パーセンテージをユニキャスト トラフィックに指定します。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。デフォルトの値は **n/a** です。

フィールド	説明
展開ステータス	インターフェイスが展開されているかどうかを指定します。

次のテーブルは、[展開履歴（Deployment History）] で表示されるフィールドを説明しています。

Table 31: [*展開履歴（Deployment History***）*] *フィールドと説明***

フィールド	説明
スイッチ名	設定が展開されたファブリックのスイッチ名を指定します。
アクション	スイッチで実行されるアクションを指定します。**[展開（Deploy）]** または **[展開解除（Undeploy）]**
展開ステータス	展開のステータスを表示します。導入が成功したか失敗したかが表示されます。
展開の日時	展開が初期化される日時を表示します。
Failed Reason	展開が失敗した理由を指定します。

フィールド	説明
表示	ドロップダウン リストから適切なフィルタを選択します。 • クイック フィルタ：すべての列に検索フィールドが表示されます。フィルタリングする検索文字列を入力できます。 • 高度なフィルタ：[高度なフィルタ（Advanced Filter）] 画面で、[一致（Match）] フィールドの [すべて（All）] または [すべて（Any）] ラジオ ボタンを選択します。[検索フィルタ（Select Filter）] フィールドで、ドロップダウン リストからカテゴリを選択します。次のフィールドのドロップダウン フィールドから適切な条件を選択します。次のフィールドに検索文字列を入力します。 **[追加（Add）]**アイコンをクリックし、別のフィルタを追加します。**[削除（Remove）]**アイコンをクリックし、フィルタを削除します。すべてのフィルタをクリアするには、**[消去（Clear）]** をクリックします。**[適用（Apply）]**をクリックしてフィルタをアクティブにし、フィルタ処理されたイベントを表示します。**[保存（Save）]** をクリックし、適切されたフィルタを保存します。高度なフィルターを破棄するには、**[キャンセル（Cancel）]** をクリックします。 • すべて - すべてのフィルタを削除し、完全な展開履歴を表示します。 • プリセット フィルタの管理 - ドロップダウン リストから適切なフィルタを選択します。 [編集（Edit）]をクリックして、フィルタパラメータを変更します。**[削除（Remove）]** をクリックし、フィルタを削除します。**[キャンセル（Cancel）]** をクリックして変更を破棄し、展開履歴に戻ります。

フィールド	説明
合計	[展開履歴（Deployment History）] ページにイベントの総数を表示します。

メディア コントローラの NDFC 読み取り専用モード

Cisco NDFC リリース 11.1(1) 以降、NDFC で **pmn.read-only-mode.enabled** サーバー プロパティを使用できます。このプロパティを使用すると、NDFC メディア コントローラの展開を、ポリシー マネージャとしてではなく、監視目的のみに使用できます。このプロパティは、**true** または **false** に設定できます。デフォルトでは、**pmn.read-only-mode.enabled** サーバー プロパティは **false** に設定されています。

pmn.read-only-mode.enabled サーバー プロパティを変更したら、**appmgr restart DCNM** コマンドを使用して NDFC を再起動し、プロパティを有効にします。

NDFC ネイティブ HA セットアップでは、サーバー プロパティ ファイルを変更する標準的な方法に従う必要があります。

1. `server.properties` ファイルでサーバ プロパティを設定します。
2. セカンダリ アプライアンスで **appmgr stop all** コマンドを使用してから、プライマリ アプライアンスで使用します。
3. プロパティを有効にするには、プライマリ アプライアンスで **appmgr start all** コマンドを使用し、次にセカンダリ アプライアンスで有効にします。

Cisco NDFC リリース 11.3(1) 以降、ホスト ポリシー、フロー ポリシー、およびグローバル メニュー項目は、NDFC 読み取り専用モードのメディア コントローラ展開に表示されます。NDFC は、ファブリック内の各スイッチからホスト ポリシー、フロー ポリシー、およびグローバル設定に関する情報を取得し、取得した情報を表示します。表示される情報は、各スイッチに固有です。

読み取り専用モードの静的レシーバーは、デバイスから静的レシーバ構成を読み取らず、データベースに入力しません。スイッチで構成された静的レシーバーを確認するには、既存の GET 静的レシーバー API を使用するか、新しい REST API GET **/pmn/switches/static-receiver-discovery/{switchIp}** を使用して、特定のスイッチ IP アドレスから静的レシーバを取得します。

NDFC の新規インストールを実行するときは、読み取り専用 (RO) または読み取り/書き込み (RW) モードのいずれかで NDFC を使用するかどうかを決定することをお勧めします。ポリシーを設定した後、またはポリシーを NDFC にインポートした後、またはポリシーをスイッチに展開した後は、NDFC を RO から RW に、またはその逆に変更しないでください。最初に NDFC およびスイッチのポリシー設定を削除してから、NDFC モードを RO または RW に変換します。つまり、展開を解除し（デフォルトおよびカスタムのホストポリシー、デフォルトおよびカスタムのフローポリシー、およびグローバル設定）、NDFC からすべてのカスタム ポリシーを削除します。同様に、スイッチ上の NDFC によって展開された既存のポリシーを削除しま

す。NDFC が RO モードになったら、スイッチに直接ポリシーを適用できます。RW モードで設定されている NDFC の場合、NDFC GUI からポリシーを展開できます。

次のいずれかの場合に該当する場合、ユーザは NDFC を RO または RW モードに変換する必要はありません。

- NDFC にすでにポリシー、つまり、ホスト ポリシー、フロー ポリシー、およびグローバル設定が含まれている場合。
- NDFC インスタンスがスイッチにポリシーを展開している場合。
- NDFC で管理されているスイッチにポリシーがすでに設定されている場合。

ホスト ポリシー：NDFC 読み取り専用モード

スイッチのホスト ポリシーを表示するには、NDFC 読み取り専用モードで **[メディア コントローラ（Media Controller）] > [ホスト（Host）] > [ホスト ポリシー（Host Policies）]** に移動します。デフォルトでは、**[スイッチの選択（Select Switch）]** ドロップダウン リストの最初のスイッチの情報が表示されます。このドロップダウン リストから、情報を表示する別のスイッチを選択できます。

表 *32 :* ホスト ポリシー テーブルのフィールドと説明

フィールド	説明
VRF	ポリシーが定義されているスイッチの VRF インスタンスを指定します。
Sequence #	ポリシーのシーケンス番号を指定します。このフィールドには、デフォルトのホスト ポリシーの 20000000 が表示されます。
ホスト名	ホスト ID を指定します。
レシーバ	受信側デバイスの IP アドレスを指定します。
マルチキャスト IP / マスク	ホストのマルチキャスト IP アドレスとマスクを指定します。
送信者	送信者の IP アドレスを指定します。
[ホストロール（Host Role）]	ホストデバイス ロールを指定します。ホストデバイス ロールは、次のいずれかです。 • 送信者 • 受信者 - 外部（Receiver-External） • 受信者 - ローカル（Receiver-Local）

フィールド	説明
オペレーション	ホスト ポリシーの動作かどうかを指定します。ポリシーには次の操作があります。 • 許可 • 拒否
最終更新日	ホスト ポリシーが最後に更新された日時を指定します。 日時の表示形式は *Day MMM DD YYYY HH:MM:SS* タイムゾーン（*Timezone*） です。

フロー ポリシー：NDFC 読み取り専用モード

NDFC 読み取り専用モードで**[メディア コントローラ（Media Controller）] > [フロー（Flow）] > [フロー ポリシー（Flow Policies）]** に移動して、スイッチのフロー ポリシーを表示します。デフォルトでは、**[スイッチの選択（Select Switch）]** ドロップダウン リストの最初のスイッチの情報が表示されます。このドロップダウン リストから、情報を表示する別のスイッチを選択できます。

表 *33*：フロー ポリシー テーブルのフィールドと説明

フィールド	説明
ポリシー名	フロー ポシリー名を指定します。
マルチキャスト IP 範囲	トラフィックのマルチキャスト IP アドレスを指定します。
帯域幅	トラフィックに割り当てられる帯域幅を示します。
QoS/DSCP	スイッチ定義の QoS ポリシーを示します。
Policer	フロー ポリシーを有効にするか無効にするかを指定します。
最終更新日	フロー ポリシーが最後に更新された日時を指定します。 日時の表示形式は *Day MMM DD YYYY HH:MM:SS* タイムゾーン（*Timezone*） です。

スイッチ グローバル設定 - 読み取り専用モード

[メディア コントローラ（Media Controller）] > [グローバル（Global）] > [設定（Config）] に移動して、NDFC 読み取り専用モードでスイッチのグローバル設定を表示します。**[スイッチの選択（Select a Switch）]** ドロップダウン リストからスイッチを選択して、そのスイッチに現在展開されているスイッチのグローバル設定を表示できます。**[VRF の選択（Select a VRF）]** ドロップダウン リストから特定の VRF を選択することもできます。

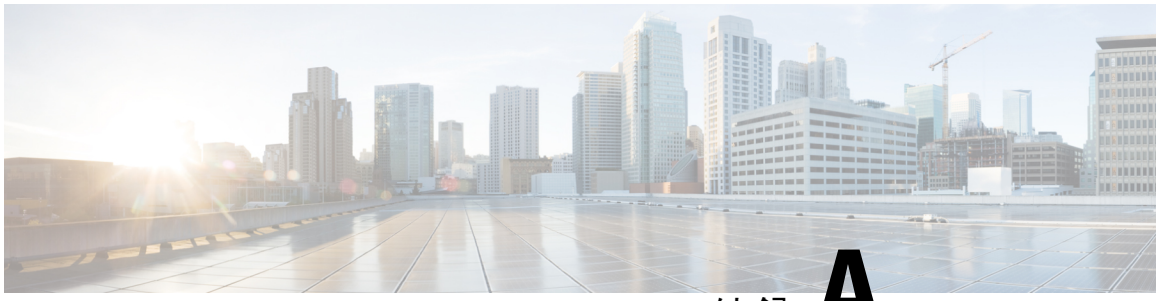
WAN リンク：読み取り専用モード

[メディア コントローラ（Media Controller）] > [グローバル（Global）] > [設定先（Config to）] に移動し、**[WAN リンク（WAN Links）]** をクリックして、NDFC 読み取り専用モードで WAN リンクを表示します。**[スイッチの選択（Select a Switch）]** ドロップダウン リストからスイッチを選択して、そのスイッチに現在展開されている WAN リンクを表示できます。

次のテーブルは、[WAN リンク（WAN Links）] タブのフィールドについて説明します。

表 *34 : WAN* リンク テーブル フィールドおよび説明

フィールド	説明
Interface Name	エンド デバイスに WAN リンクとして接続されているインターフェイスを指定します。
Admin Status	上矢印はステータスが上がっていることを示しています。下矢印はステータスが下がっていること意味します。
動作ステータス	上矢印はインターフェイスの稼働状態が上がっていることを示しています。下矢印はステータスが下がっていること意味します。
WAN リンク	ドロップダウン リストから、WAN リンクとしてこのインターフェイスを指定するように選択できます。 • **[はい（Yes）]** を選択し、WAN リンクとしてインターフェイスを設定します。 • **[いいえ（No）]** を選択し、WAN リンクとしてインターフェイスを削除します。
展開ステータス	インターフェイスがWANリンクとして展開されているかどうかを指定します。



付録 A

Show コマンドのサンプル出力

この付録では、メディア **show** コマンドの IP ファブリックの出力例を示します。

show コマンドの出力例 (スパイン リーフ展開)

このセクションでは、スパイン リーフ展開のスイッチの出力例を示します。

（注） **vrf** *vrf-name* オプションを使用して VRF を指定しない場合、これらのコマンドはデフォルトの VRF の出力を表示します。

次に、**show nbm defaults vrf all** コマンドの出力例を示します。

```
switch# show nbm defaults vrf all
----------------------------------------
 Defaults for VRF default (1)
 ----------------------------------------

  Default Flow Policy:

    Bandwidth                : 1000 Kbps
    DSCP                     : 0
    Queue ID                 : 7
    Policer                  : Enabled
    Operation mode (cache)   : EOR_PIM_A
    Operation mode           : EOR_PIM_A
    Unicast Fabric Bandwidth : 1
    Number of ASM groups     : 1
      Group 1 :  224.0.0.0/8

  Default Host Policies:

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


 ----------------------------------------
```

Show コマンドのサンプル出力

```
 Defaults for VRF red (3)
 ----------------------------------------

  Default Flow Policy:

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

  Default Host Policies:

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

次に、**show nbm flow-policy vrf all** コマンドの出力例を示します。

```
switch# show nbm flow-policy vrf all
Flow Policy for VRF 'blue'
 ------------------------------------------------

 Total Group Ranges Found = 0
 Total Policies Defined = 0

 Flow Policy for VRF 'default'
 ------------------------------------------------

 Default BW (Kbps)  : 1890
 Default DSCP       : 36
 Default QOS        : 7
 Default Policer    : Enabled

 ---------------------------------------------------------------------------------------------

 | Group Range                    | BW (Kbps)  | DSCP | QOS | Policer  | Policy Name
 ---------------------------------------------------------------------------------------------

 | 235.1.1.1-235.1.2.255          | 30         | 0    | 7   | Enabled  | Dynamic_IGMP
 | 238.4.1.1-238.4.1.1            | 3000000    | 0    | 7   | Enabled  | NBM_Static_2
 | 238.4.1.2-238.4.1.10           | 3000000    | 0    | 7   | Enabled  | NBM_Static_2
 | 238.4.1.11-238.4.1.11          | 3000000    | 0    | 7   | Enabled  | NBM_Static_2
 | 238.4.1.12-238.4.1.100         | 3000000    | 0    | 7   | Enabled  | NBM_Static_2
 | 238.4.1.101-238.4.1.255        | 3000000    | 0    | 7   | Enabled  | NBM_Static_2
 | 239.1.1.2-239.1.1.2            | 100        | 0    | 7   | Disabled | SVI_239
 | 239.1.1.3-239.1.1.9            | 100        | 0    | 7   | Disabled | SVI_239
 | 239.1.1.10-239.1.1.10          | 100        | 0    | 7   | Disabled | SVI_239
 | 239.1.1.11-239.1.1.30          | 100        | 0    | 7   | Disabled | SVI_239
 | 239.1.1.1-239.1.1.1            | 200        | 0    | 7   | Enabled  | SVI_239.1.1.1
 | 227.1.1.51-227.1.1.51          | 1000       | 0    | 7   | Enabled  | Dynamic_227.1
 | 227.1.1.52-227.1.1.200         | 1000       | 0    | 7   | Enabled  | Dynamic_227.1
 | 229.1.1.1-229.1.1.100          | 1000       | 0    | 7   | Disabled | NBM_229
 | 234.1.1.1-234.1.1.100          | 30         | 0    | 7   | Disabled | NBM_234
 | 234.1.1.101-234.1.1.200        | 30         | 0    | 7   | Disabled | NBM_234
 | 237.1.1.1-237.1.1.200          | 3000       | 0    | 7   | Disabled | NBM_Static_237.1

 | 237.1.2.1-237.1.2.200          | 3000       | 0    | 7   | Disabled | NBM_Static_237.1
...
 | 237.1.1.201-237.1.1.255        | 3000       | 0    | 7   | Enabled  | NBM_Static_237_2
```

Show コマンドのサンプル出力

```
 | 237.1.2.201-237.1.2.255        | 3000       | 0    | 7   | Enabled  | NBM_Static_237_2

 | 237.1.3.201-237.1.3.255        | 3000       | 0    | 7   | Enabled  | NBM_Static_237_2

 | 237.1.4.201-237.1.4.255        | 3000       | 0    | 7   | Enabled  | NBM_Static_237_2

 | 232.1.1.9-232.1.1.200          | 200        | 0    | 7   | Enabled  | NBM_Static_232_2

 | 232.1.1.5-232.1.1.7            | 200        | 0    | 7   | Enabled  | NBM_Static_232_2

 | 232.1.1.8-232.1.1.8            | 200        | 0    | 7   | Enabled  | NBM_Static_232_2

 | 235.2.2.2-235.2.2.10            | 3000000    | 24   | 7   | Disabled | Test_R_V
 ------------------------------------------------------------------------------------------


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

次に、**show nbm flows detail vrf all** コマンドの出力例を示します。

```
switch# show nbm flows detail vrf all
 ------------------------------------------------------------
 NBM Flows for VRF 'default'
 ------------------------------------------------------------

 Active Source-Group-Based Flow(s)  :

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

 Active Source-Group-Based Flow(s)  :

Mcast-Group      Src-IP           Uptime   Src-Intf     Nbr-Device         LID Profile
Status  Num Rx  Bw Mbps   CFG Bw Slot Unit Slice DSCP QOS Policed FHR Policy-name
   Rcvr-Num Rcvr-slot Unit    Num-Rcvrs    Rcvr-ifidx  IOD Rcvr-Intf  Nbr-Device

225.1.1.11      10.1.4.2        00:00:11   Vlan100   not-applicable         *     *
ACTIVE       0    1.500    1.500    0    0     0    0   7 Yes     Yes Default


225.1.7.228     10.1.4.2        00:00:12   Vlan100   not-applicable         *     *
ACTIVE       0    1.500    1.500    0    0     0    0   7 Yes     Yes Default


225.1.6.193     10.1.4.2        00:00:12   Vlan100   not-applicable         *     *
ACTIVE       0    1.500    1.500    0    0     0    0   7 Yes     Yes Default


...

225.1.19.52     10.2.3.2        00:02:13   Eth1/31   gretta-r10-eor2       349     962
ACTIVE       1    1.500    1.500    1    5     0    0   7 Yes     Yes Default

          1         0    0            1    0x09010064    2 Vlan100    not-applicable
225.1.23.31     10.2.3.2        00:35:04   Eth1/31   gretta-r10-eor2      1119     962
ACTIVE       1    1.500    1.500    1    5     0    0   7 Yes     Yes Default

          1         0    0            1    0x09010064    2 Vlan100    not-applicable
```

Show コマンドのサンプル出力

```
...
225.1.0.23      10.1.4.2        02:20:38   Vlan100   not-applicable         *     *
ACTIVE       1    1.500    1.500    0    0     0    0   7 Yes     Yes Default

          1         1    5            1    0x1a003c00   48 Eth1/31   gretta-r10-eor2

225.1.0.10      10.1.4.2        02:20:38   Vlan100   not-applicable         *     *
ACTIVE       1    1.500    1.500    0    0     0    0   7 Yes     Yes Default

          1         1    5            1    0x1a003e00   49 Eth1/32   gretta-r10-eor2
...
225.1.0.3       10.1.4.2        02:20:38   Vlan100   not-applicable         *     *
ACTIVE       1    1.500    1.500    0    0     0    0   7 Yes     Yes Default

          1         1    5            1    0x1a003c00   48 Eth1/31   gretta-r10-eor2
```

次に、**show nbm flows static vrf all** コマンドの出力例を示します。

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

Show コマンドのサンプル出力

```
+------------------------------------------------------------------------+
```

次に、**show nbm flows statistics vrf all** コマンドの出力例を示します。

```
switch# show nbm flows statistics vrf all
 ------------------------------------------------------------
 NBM Flow Statistics for VRF 'default'
 ------------------------------------------------------------

 Source-Group-Based Flow Statistics  :

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

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

 Source-Group-Based Flow Statistics  :

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

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

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

Show コマンドのサンプル出力

```
 ------------------------------------------------------

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

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

次に、**show nbm flows summary vrf all** コマンドの出力例を示します。

```
switch# show nbm flows summary vrf all
 ------------------------------------------------
 NBM Flow Summary for VRF 'default'
 ------------------------------------------------

 IIF = Incoming Interface
 OIF = Outgoing Interface
 ------------------------------------------------------------------------
 | Category                  |   (*,G)    |   (S,G)    |    Total     |
 ------------------------------------------------------------------------
 | All Flows                 |          0 |          0 |            0 |
 | Flows with No receivers   |          0 |          0 |            0 |
 | Flows with OIF            |          0 |          0 |            0 |
 | Flows with SVI IIF        |          0 |          0 |            0 |
 | Flows with PHY IIF        |          0 |          0 |            0 |
 | Flows (SVI) with Policing |          0 |          0 |            0 |
 | Flows (PHY) with Policing |          0 |          0 |            0 |
 ------------------------------------------------------------------------


 ------------------------------------------------
 NBM Flow Summary for VRF 'red'
 ------------------------------------------------

 IIF = Incoming Interface
 OIF = Outgoing Interface
 ------------------------------------------------------------------------
 | Category                  |   (*,G)    |   (S,G)    |    Total     |
 ------------------------------------------------------------------------
 | All Flows                 |          0 |         72 |           72 |
 | Flows with No receivers   |          0 |          0 |            0 |
 | Flows with OIF            |          0 |         72 |           72 |
 | Flows with SVI IIF        |          0 |         24 |           24 |
 | Flows with PHY IIF        |          0 |         48 |           48 |
 | Flows (SVI) with Policing |          0 |         24 |            0 |
 | Flows (PHY) with Policing |          0 |         48 |            0 |
 ------------------------------------------------------------------------

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

次に、**show nbm flows vrf all** コマンドの出力例を示します。

```
switch# show nbm flows vrf all
 ------------------------------------------------------------
 NBM Flows for VRF 'default'
 ------------------------------------------------------------
```

Show コマンドのサンプル出力

```
 Active Source-Group-Based Flow(s)  :

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

 ------------------------------------------------------------
 NBM Flows for VRF 'red'
 ------------------------------------------------------------

 Active Source-Group-Based Flow(s)  :

Mcast-Group      Src-IP           Uptime   Src-Intf     Nbr-Device        Num Rx  Bw
Mbps Slot Unit Slice DSCP QOS Policed Policy-name
225.1.2.48       10.2.3.2         02:16:27   Eth1/31   gretta-r10-eor2          1    1.001
    1    5     0    1   0 Yes     pol1
225.1.2.47       10.2.3.2         02:16:27   Eth1/32   gretta-r10-eor2          1    1.500
    1    5     0    0   7 Yes     Default
225.1.2.46       10.2.3.2         02:16:27   Eth1/32   gretta-r10-eor2          1    2.002
    1    5     0    3   0 Yes     pol2
225.1.2.45       10.2.3.2         02:16:27   Eth1/31   gretta-r10-eor2          1    1.500
    1    5     0    0   7 Yes     Default
225.1.2.44       10.2.3.2         02:16:27   Eth1/32   gretta-r10-eor2          1    1.500
    1    5     0    0   7 Yes     Default
225.1.2.43       10.2.3.2         02:16:27   Eth1/31   gretta-r10-eor2          1    1.500
    1    5     0    0   7 Yes     Default
225.1.2.42       10.2.3.2         02:16:27   Eth1/32   gretta-r10-eor2          1    1.500
    1    5     0    0   7 Yes     Default
...
225.1.0.2        10.1.4.2         02:16:48   Vlan100   not-applicable           1    1.500
    0    0     0    0   7 Yes     Default
225.1.0.1        10.1.4.2         02:16:48   Vlan100   not-applicable           1    1.500
    0    0     0    0   7 Yes     Default
225.1.0.24       10.1.4.2         02:16:48   Vlan100   not-applicable           1    1.500
    0    0     0    0   7 Yes     Default
225.1.0.23       10.1.4.2         02:16:48   Vlan100   not-applicable           1    1.500
    0    0     0    0   7 Yes     Default
225.1.0.22       10.1.4.2         02:16:48   Vlan100   not-applicable           1    1.500
    0    0     0    0   7 Yes     Default
225.1.0.21       10.1.4.2         02:16:48   Vlan100   not-applicable           1    1.500
    0    0     0    0   7 Yes     Default
225.1.0.20       10.1.4.2         02:16:48   Vlan100   not-applicable           1    1.500
    0    0     0    0   7 Yes     Default
225.1.0.19       10.1.4.2         02:16:48   Vlan100   not-applicable           1    1.500
    0    0     0    0   7 Yes     Default
225.1.0.18       10.1.4.2         02:16:48   Vlan100   not-applicable           1    1.500
    0    0     0    0   7 Yes     Default
225.1.0.17       10.1.4.2         02:16:48   Vlan100   not-applicable           1    1.500
    0    0     0    0   7 Yes     Default
225.1.0.16       10.1.4.2         02:16:48   Vlan100   not-applicable           1    1.500
    0    0     0    0   7 Yes     Default
225.1.0.15       10.1.4.2         02:16:48   Vlan100   not-applicable           1    1.200
    0    0     0   11   0 Yes     bw10
225.1.0.14       10.1.4.2         02:16:48   Vlan100   not-applicable           1    1.200
    0    0     0   11   0 Yes     bw10
225.1.0.13       10.1.4.2         02:16:48   Vlan100   not-applicable           1    1.200
    0    0     0   11   0 Yes     bw10
225.1.0.12       10.1.4.2         02:16:48   Vlan100   not-applicable           1    1.200
    0    0     0   11   0 Yes     bw10
225.1.0.11       10.1.4.2         02:16:48   Vlan100   not-applicable           1    1.200
    0    0     0   11   0 Yes     bw10
225.1.0.10       10.1.4.2         02:16:48   Vlan100   not-applicable           1    1.500
    0    0     0    0   7 Yes     Default
```

Show コマンドのサンプル出力

```
...
```

次に、**show nbm host-policy all receiver external vrf all** コマンドの出力例を示します。

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

 Default External Receiver Policy: Deny

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

 Total Policies Found = 7

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

 Default External Receiver Policy: Allow

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

 Total Policies Found = 601
```

次に、**show nbm host-policy all receiver local vrf all** コマンドの出力例を示します。

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

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

 Default Local Receiver Policy: Allow


 Total Policies Found = 0


 ------------------------------------------------------
```

Show コマンドのサンプル出力

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

 Default Local Receiver Policy: Allow


 Total Policies Found = 0


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

 Default Local Receiver Policy: Allow

 ------------------------------------------------------------------------------------
 Seq Num       Source           Group            Group Mask  Reporter         Permission

 ------------------------------------------------------------------------------------
 256           0.0.0.0          228.1.1.246      32          70.30.1.102      Allow
 512           0.0.0.0          228.1.2.247      32          70.30.1.102      Allow
 768           0.0.0.0          228.1.3.248      32          70.30.1.102      Allow
 4864          0.0.0.0          228.1.2.30       32          100.1.1.101      Allow
 100096        0.0.0.0          231.1.1.106      32          0.0.0.0          Deny
 100352        0.0.0.0          236.1.1.112      32          0.0.0.0          Deny
 257           0.0.0.0          228.1.1.247      32          70.30.1.102      Allow
 513           0.0.0.0          228.1.2.248      32          70.30.1.102      Allow
 769           0.0.0.0          228.1.3.249      32          70.30.1.102      Allow
...
 511           0.0.0.0          228.1.2.246      32          70.30.1.102      Allow
 767           0.0.0.0          228.1.3.247      32          70.30.1.102      Allow
 4863          0.0.0.0          228.1.2.29       32          100.1.1.101      Allow
 100095        0.0.0.0          231.1.1.105      32          0.0.0.0          Deny
 100351        0.0.0.0          236.1.1.111      32          0.0.0.0          Deny
 ------------------------------------------------------------------------------------

 Total Policies Found = 1470
```

次に、**show nbm host-policy all sender vrf all** コマンドの出力例を示します。

```
switch# show nbm host-policy all sender vrf all
 ----------------------------------------------------
 VRF 'blue': Sender Policy Table
 ----------------------------------------------------

 Default Sender Policy: Allow

 Total Policies Found = 0

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

 Default Sender Policy: Allow

 ------------------------------------------------------------------------
 Seq Num       Source           Group            Group Mask  Permission
 ------------------------------------------------------------------------
 776           70.20.10.201     234.1.1.1        32          Allow
 777           70.20.10.201     234.1.1.2        32          Allow
 778           70.20.10.201     234.1.1.3        32          Allow
 779           70.20.10.201     234.1.1.4        32          Allow
 780           70.20.10.201     234.1.1.5        32          Allow
 781           70.20.10.201     234.1.1.6        32          Allow
```

Show コマンドのサンプル出力

```
 782           70.20.10.201     234.1.1.7        32          Allow
 783           70.20.10.201     234.1.1.8        32          Allow
 784           70.20.10.201     234.1.1.9        32          Allow
...

 3970          70.20.10.215     234.1.1.195      32          Allow
 3971          70.20.10.215     234.1.1.196      32          Allow
 3972          70.20.10.215     234.1.1.197      32          Allow
 3973          70.20.10.215     234.1.1.198      32          Allow
 3974          70.20.10.215     234.1.1.199      32          Allow
 3975          70.20.10.215     234.1.1.200      32          Allow
 ------------------------------------------------------------------

 Total Policies Found = 3000
```

次に、**show nbm host-policy applied receiver external vrf all** コマンドの出力例を示します。

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

 Default External Receiver Policy: Deny

 Applied policy for interface 'ALL':

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

 Total Policies Found = 7

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

 Default External Receiver Policy: Allow

 Applied policy for interface 'ALL':

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

Show コマンドのサンプル出力

```
 4573          70.30.1.105      235.1.1.199      32          Allow       0
 4574          70.30.1.105      235.1.1.200      32          Allow       0
 ----------------------------------------------------------------------------

 Total Policies Found = 601
```

次に、**show nbm host-policy applied receiver local all vrf all** コマンドの出力例を示します。

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

 Default Local Receiver Policy: Allow

 Total Policies Found = 0

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

 Default Local Receiver Policy: Allow

 Applied policy for interface 'Vlan1001':

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

 Applied policy for interface 'Wildcard':

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

 Total Policies Found = 705
```

Show コマンドのサンプル出力

次に、**show nbm host-policy applied receiver local interface** *interface* **vrf** *vrf-name* コマンドの出力例を示します。

```
switch# show nbm host-policy applied receiver local interface vlan 1001
 ------------------------------------------------------
 VRF 'blue': Applied Local Receiver Policy Table
 ------------------------------------------------------

 Default Local Receiver Policy: Allow


 Applied policy for interface 'Vlan1001':

 ------------------------------------------------------------------------------------
 Seq Num       Source          Group           Group Mask  Permission  Deny Counter
 ------------------------------------------------------------------------------------
 4831          0.0.0.0         228.1.2.1       32          Allow       0
 4836          0.0.0.0         228.1.2.2       32          Allow       0
 4837          0.0.0.0         228.1.2.3       32          Allow       0
 4838          0.0.0.0         228.1.2.4       32          Allow       0
 4839          0.0.0.0         228.1.2.5       32          Allow       0
 4840          0.0.0.0         228.1.2.6       32          Allow       0
 4841          0.0.0.0         228.1.2.7       32          Allow       0

...

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

 Total Policies Found = 255
```

次に、**show nbm host-policy applied receiver local wildcard vrf default** コマンドの出力例を示します。

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

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

 Default Local Receiver Policy: Allow


 Applied policy for interface 'Wildcard':

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

Show コマンドのサンプル出力

```
 10301         0.0.0.0          237.1.1.1        32          Allow       0
 10401         0.0.0.0          238.1.0.0        16          Deny        0
 10402         0.0.0.0          238.1.1.1        32          Allow       0
 ------------------------------------------------------------------------------

 Total Policies Found = 450
```

次に、**show nbm host-policy applied sender all vrf all** コマンドの出力例を示します。

```
switch# show nbm host-policy applied sender all vrf all
------------------------------------------------------
VRF 'default': Applied Sender Policy Table
------------------------------------------------------

Default Sender Policy: Allow


Total Policies Found = 0


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

Default Sender Policy: Allow


Applied policy for interface 'Ethernet1/32':

------------------------------------------------------------------------
Seq Num       Source           Group            Group Mask  Permission
------------------------------------------------------------------------
20            10.1.31.10       228.31.1.1       32          Allow
------------------------------------------------------------------------
------------------------------------------------------------------------

Total Policies Found = 1


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

Default Sender Policy: Allow


Applied policy for interface 'Ethernet1/31':

------------------------------------------------------------------------
Seq Num       Source           Group            Group Mask  Permission
------------------------------------------------------------------------
 10            10.1.31.10       228.31.1.1       32          Allow
 11            10.1.31.10       228.31.1.2       32          Allow
 12            10.1.31.10       228.31.1.3       32          Allow
 13            10.1.31.10       228.31.1.4       32          Allow
------------------------------------------------------------------------
------------------------------------------------------------------------

Total Policies Found = 4
```

次に、**show nbm host-policy applied sender interface** *interface* **vrf** *vrf-name* コマンドの出力例を示します。

Show コマンドのサンプル出力

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

Default Sender Policy: Allow


Applied policy for interface 'Ethernet1/31':

------------------------------------------------------------------------
Seq Num       Source           Group            Group Mask  Permission
------------------------------------------------------------------------
 10            10.1.31.10       228.31.1.1       32          Allow
 11            10.1.31.10       228.31.1.2       32          Allow
 12            10.1.31.10       228.31.1.3       32          Allow
 13            10.1.31.10       228.31.1.4       32          Allow
------------------------------------------------------------------------
------------------------------------------------------------------------

Total Policies Found = 4
```

次に、**show nbm host-policy applied sender wildcard vrf all** コマンドの出力例を示します。

```
switch# show nbm host-policy applied sender wildcard vrf all
------------------------------------------------------
VRF 'default': Applied Sender Policy Table
------------------------------------------------------

Default Sender Policy: Allow


Total Policies Found = 0

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

Default Sender Policy: Allow


Applied policy for interface 'Wildcard':

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

Total Policies Found = 5
```

次の例は、静的フロープロビジョニングが有効になっている場合の **show nbm flows static** コマンドの出力例を示しています。

```
switch# show nbm flows static                                                  |

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

Show コマンドのサンプル出力

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

この例は、静的フロープロビジョニングが有効になっている場合の **show nbm flows static group** コマンドの出力例を示しています。障害の理由列には、発生したエラーの理由が表示されます。

```
switch# show nbm flows static group 231.1.1.2

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

次に、**show running-config nbm** コマンドの出力例を示します。

```
switch# show running-config nbm
!Command: show running-config nbm
!Running configuration last done at: Fri Mar 29 05:21:38 2019
!Time: Fri Mar 29 10:09:24 2019

version 9.3(1) Bios:version 08.35
feature nbm

nbm mode pim-active
nbm host-policy
  sender
    default permit
  receiver
    default permit
```

```
  pim
    default permit
nbm reserve unicast fabric bandwidth 2
nbm flow asm range 225.0.0.0/8 234.80.0.0/16 232.6.0.0/16 233.80.0.0/16
nbm flow asm range 235.6.0.0/16 239.80.0.0/16 227.0.0.0/8 238.80.0.0/16
nbm flow asm range 238.100.0.0/16 239.100.0.0/16
nbm flow bandwidth 1002 kbps
nbm flow-policy
  policy v2.leaf1.1.225.50
    bandwidth 1001 kbps
    dscp 26
    ip group-range 225.50.1.6 to 225.50.1.10
  policy v2.leaf1.1.225.80
    bandwidth 1001 kbps
    dscp 24
    ip group-range 225.80.1.1 to 225.80.1.5
nbm vrf mars
  nbm mode pim-active
  nbm host-policy
    sender
      default permit
    receiver
      default permit
    pim
      default permit
  nbm reserve unicast fabric bandwidth 1
  nbm flow asm range 225.0.0.0/8 227.0.0.0/8 234.80.0.0/16 233.80.0.0/16
  nbm flow asm range 235.6.0.0/16 239.80.0.0/16 232.6.0.0/16 238.80.0.0/16
  nbm flow asm range 238.100.0.0/16 239.100.0.0/16
  nbm flow bandwidth 1004 kbps
  nbm flow-policy
    policy static.v2.leaf3.1.238.80
      bandwidth 1001 kbps
      dscp 35
      ip group-range 238.80.1.1 to 238.80.1.5
    policy static.v2.leaf4.1.239.80
      bandwidth 1001 kbps
      dscp 35
      ip group-range 239.80.1.1 to 239.80.1.5
  nbm flow-definition 233.80.1.1 0.0.0.0
    egress-interface eth6/20/3
    egress-interface vlan851
    stage-flow
    egress-host 21.7.1.2
  nbm flow-definition 233.80.1.2 0.0.0.0
    egress-interface eth6/20/3
    stage-flow
    egress-host 21.7.1.2
```

サンプル show コマンド出力 (単一のモジュラ スイッチ)

このセクションでは、Nexus ダッシュボード ファブリック コントローラ のない単一のモジュラ スイッチの出力例を示します。コントローラベースの展開では、統計はNexus ダッシュボード ファブリック コントローラ GUI で使用できます。

次に、**show nbm defaults** コマンドのサンプル出力例を示します。

```
switch# show nbm defaults
Default Flow Policy:
```

Show コマンドのサンプル出力

```
Bandwidth : 1000 Kbps
DSCP      : 0
QID       : 0

Default Host Policies:
Sender    : Permit
Receiver  : Permit
PIM       : Permit

Default Unicast Fabric Bandwidth : 1
```

次に、**show nbm flows** コマンドの出力例を示します。

```
switch# show nbm flows
NBM Active Source-Group-Based Flows :
Mcast-Group Src-IP Start-Time Src-Intf L4-S L4-D LID Status Num Rx Bw Mbps CFG Bw Mbps
Src-slot Unit Slice DSCP QOS
228.2.10.3 10.12.85.10 08/21 18:45:27.429 Vlan1000 0 0 0 ACTIVE 7 66.000 66.000 1 0 0
48 7
228.1.3.3 10.10.85.10 08/21 18:45:27.324 Vlan1000 0 0 0 ACTIVE 8 18.000 18.000 1 0 0 24
 7
228.1.4.1 10.10.85.10 08/21 18:45:27.068 Vlan1000 0 0 0 ACTIVE 8 19.000 19.000 1 0 0 32
 7
228.1.9.1 10.10.85.10 08/21 18:45:26.732 Vlan1000 0 0 0 ACTIVE 8 31.000 31.000 1 0 0 32
 7
```

次に、**show nbm flows group** *multicast-group* コマンドのサンプル出力例を示します。

```
switch# show nbm flows group 228.2.10.3
NBM Active Source-Group-Based Flows :
Mcast-Group Src-IP Start-Time Src-Intf L4-S L4-D LID Status Num Rx Bw Mbps CFG Bw Mbps
Src-slot Unit Slice DSCP QOS
228.2.10.3 10.12.85.10 08/21 18:45:27.429 Vlan1000 0 0 0 ACTIVE 7 66.000 66.000 1 0 0
48 7
```

次に、**show ip igmp groups** コマンドの出力例を示します。

```
switch# show ip igmp groups
IGMP Connected Group Membership for VRF "default" - 61520 total entries
Type: S - Static, D - Dynamic, L - Local, T - SSM Translated
Group Address      Type Interface           Uptime    Expires   Last Reporter
225.3.5.1          D    Ethernet3/5         11:48:07  00:03:36  3.5.1.6
225.3.5.2          D    Ethernet3/5         11:48:07  00:03:36  3.5.1.6
225.3.5.3          D    Ethernet3/5         11:48:07  00:03:36  3.5.1.6
225.3.5.4          D    Ethernet3/5         11:48:07  00:03:36  3.5.1.6
```

次に、**show ip igmp groups** *interface* コマンドの出力例を示します。

```
switch# show ip igmp groups eth3/5
IGMP Connected Group Membership for Interface "Eth3/5" - 1165 total entries
Type: S - Static, D - Dynamic, L - Local, T - SSM Translated
Group Address      Type Interface      Uptime    Expires   Last Reporter
225.3.5.1          D    Ethernet3/5    11:51:22  00:02:24  3.5.1.6
225.3.5.2          D    Ethernet3/5    11:51:22  00:02:24  3.5.1.6
225.3.5.3          D    Ethernet3/5    11:51:22  00:02:24  3.5.1.6
225.3.5.4          D    Ethernet3/5    11:51:22  00:02:24  3.5.1.6
```

次に、**show ip igmp groups** *multicast-group* コマンドのサンプル出力例を示します。

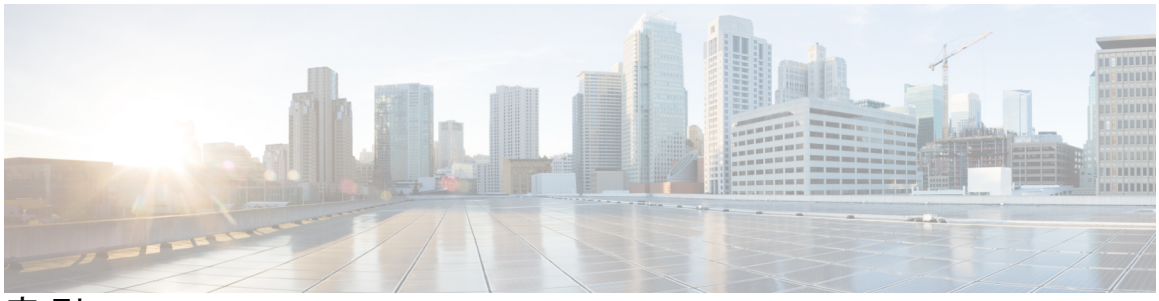
```
switch# show ip igmp groups 225.3.5.1
IGMP Connected Group Membership for VRF "default" - matching Group "225.3.5.1"
```

Show コマンドのサンプル出力

```
Type: S - Static, D - Dynamic, L - Local, T - SSM Translated
Group Address  Type  Interface    Uptime    Expires   Last Reporter
225.3.5.1      D     Ethernet3/5  00:05:20  00:10:10  3.5.1.6
```

次に、**show running-config nbm** コマンドの出力例を示します。

```
switch# show running-config nbm
!Command: show running-config nbm
!Running configuration last done at: Thu May 10 08:53:37 2018
!Time: Thu May 10 09:33:23 2018

version 9.2(1) Bios:version 07.50
feature nbm

nbm mode pim-active
nbm host-policy
  sender
    default deny
  receiver
    default deny
    5 host 1.0.0.5 source 1.2.3.4 group 232.1.2.0/24 permit
    6 host 1.0.3.5 source 1.2.3.77 group 224.1.2.0/24 permit
    7 host 1.0.0.5 source 1.2.3.88 group 224.1.2.0/24 permit
  pim
    default deny
nbm reserve unicast fabric bandwidth 10
nbm flow asm range 237.1.1.0/24
nbm flow bandwidth 123 kbps
nbm flow-policy
  policy BLAH
  policy POL
  policy POL_1
    bandwidth 123 kbps
    dscp 10
    ip group-range 237.1.1.0 to 238.1.1.0
  policy POL_A
  policy flow
  policy nbm1_1
    bandwidth 1000000 kbps
    dscp 11
    ip group-range 224.1.0.1 to 224.1.255.255
    ip group-range 225.1.0.1 to 225.1.255.255
```



索引

数字

B

C

D

E

F

H

I

M

N

P

R

S

V

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。