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。

Cisco NX-OS リリース	Cisco NDFC リリース
9.3(5)	11.4(1)
9.3(3)	11.3(1)
9.3(1)	11.2(1)

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。
- NBM 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、NBM 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、NBM 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。
- NBM 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。
- NBM 外部リンクとして設定できるのは、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、NBM 外部リンク設定が削除されます。
- レイヤ 3 インターフェイスを NBM 外部リンクとして設定すると、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。

- NBM 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、PMN 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、PMN 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、NBM を使用した PMN 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、PMN 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、PMN 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、NBM 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。
- VXLAN 対応スイッチで実行されている NBM はサポートされていません。NBM 機能により、VXLAN アンダーレイ マルチキャスト転送が中断される場合があります。
- Cisco NX-OS リリース 10.3(1)F 以降、次の PMN 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 9200、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、NBM モード pim-active および NBM 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 nbm pim-active または nbm 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 NBM 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 NBM モード pim-active および NBM モード pim-passive で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、NBM モードの pim-active と NBM 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 NBM でサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、NBM フローポリサーは Cisco Nexus 9348GC-FX3 スイッチでサポートされます。

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 NBM 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 サーバー（NDFC Server）] > [サーバー 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 サーバー 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 サーバー 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 サーバー 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 Media Controller には、Advanced Server DCNM ライセンスが 詳細については、『Cisco DCNM インストール ガイド』を参照してくた

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。

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 NBM 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。

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 NBM 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 NBM 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 NBM 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 NBM 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、DCNM 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 NBM 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。

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 サーバー プロパティ **trap.registaddress=***dcnm-ip* under**Web UI Administrator->Server Properties** 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、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。

NBM の設定

ノンブロッキング マルチキャスト (NBM) を設定する手順は、メディア ソリューションの IP ファブリックに使用している展開方法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 NBM の設定

スパイン リーフ展開でスイッチの NBM を設定するには、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、NBM 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、スパインおよびリーフ スイッチの PIM の設定および スパイン スイッチで MSDP の設定 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**

手順の詳細

	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`	NBM 機能と PIM アクティブ モードを有効にします。これにより、NBM 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。

	コマンドまたはアクション	目的

		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**
		• **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 NBM 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） NBM 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 NBM VRF の設定 （31 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 NBM 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 NBM ホスト ポリシーを設定します。
		（注） デフォルトの NBM 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。

	コマンドまたはアクション	目的
ステップ 5	（任意） **default** {**permit** | **deny**} 例： `switch(config-nbm-host-pol-sender)# default permit`	NBM 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**}
	• 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 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。NBM 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 NBM 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：	Kbps、Mbps、または Gbps でグローバル NBM 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。

<table>
<tr><th></th><th>コマンドまたはアクション</th><th>目的</th></tr>
<tr><td></td><td>switch(config)# nbm flow bandwidth 3000 mbps</td><td><table><tr><th>範囲</th><th>デフォルト値</th></tr><tr><td>1 ～ 25,000,000 Kbps</td><td>0 Kbps</td></tr><tr><td>1 ～ 25,000 Mbps</td><td>0 Mbps</td></tr><tr><td>1 ～ 25 Gbps</td><td>0 Gbps</td></tr></table></td></tr>
<tr><td>ステップ 10</td><td>[no] nbm flow dscp value
例：
switch(config)# nbm flow dscp 10</td><td>グローバル NBM 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 NBM 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。</td></tr>
<tr><td>ステップ 11</td><td>（任意）[no] nbm flow policer
例：
switch(config)# no nbm flow policer</td><td>すべての NBM 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。</td></tr>
<tr><td>ステップ 12</td><td>[no] nbm flow-policy
例：
switch(config)# nbm flow-policy
switch(config-nbm-flow-pol)#</td><td>フローごとのフロー帯域幅を設定します。</td></tr>
<tr><td>ステップ 13</td><td>[no] policy policy-name
例：
switch(config-nbm-flow-pol)# policy nbmflow10
switch(config-nbm-flow-pol-attr)#</td><td>NBM フローポリシーを設定します。ポリシー名には最大63文字の英数字を指定できます。</td></tr>
<tr><td>ステップ 14</td><td>（任意）[no] policer
例：
switch(config-nbm-flow-pol-attr)# no policer</td><td>指定された NBM 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。</td></tr>
</table>

	コマンドまたはアクション	目的
		（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、NBM 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： `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：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 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。

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

スパインおよびリーフ スイッチの PIM の設定

スパイン スイッチで 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

NBM VRF の設定 （30 ページ）

フローの確立 (オプション)

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 NBM 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

	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 NBM 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。

	コマンドまたはアクション	目的

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。

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

	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。

	コマンドまたはアクション	目的
ステップ 4	**ip msdp peer** *peer-ip-address* **connect-source** *interface* 例： `switch(config)# ip msdp peer 2.2.1.1 connect-source loopback1`	MSDP ピアを設定してピア IP アドレスを指定します。
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 NBM 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。

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） Cisco NX-OS リリース 7.0(3)I7(2) 以降でサポートされている、、WAN リンクでは必ず **ip pim sparse-mode** コマンドを設定し NBM ファブリック インターフェイスでのみ **ip pimpassive** コマンドを実行します（外部システムに対してではありません）。

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

	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 1/49`
	`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

	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

	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。

	コマンドまたはアクション	目的
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)#`	

単一のモジュラー スイッチの NBM の設定

IP ファブリックを設定したら、スイッチで NBM 機能を有効にする必要があります。NBM 機能により、ファブリックに着信する帯域幅が発信される帯域幅と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 NBM 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**

手順の詳細

	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：	NBM 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`	（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 NBM 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） NBM 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 NBM VRF の設定 （31 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 NBM 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 NBM 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)#`
		NBM フローポリシーを設定します。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 NBM 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、NBM 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：	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
	`switch(config-nbm-flow-pol-attr-prop)# priority critical` `switch(config-nbm-flow-pol-attr-prop)#`	

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。

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

NBM VRF の設定 （30 ページ）
フローの確立 (オプション)

NBM VRF の設定

nbm feature コマンドを使用して NBM を設定すると、システムはデフォルトの NBM 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 NBM VRF を設定することもできます。

NBM 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。NBM 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、NBM 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 NBM 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 NBM VRF の設定

アクティブ フロープロビジョニング用に NBM VRF を設定できます。これにより、NBM 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

NBM を設定します。

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

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**

手順の詳細

	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`	NBM VRF を作成します。
ステップ 3	**nbm mode pim-active** 例： `switch(config)# nbm mode pim-active`	NBM 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 NBM 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。NBM VRF を PIM アクティブ モードから PIM パッシブ モードに変更できるのは、VRF でカスタム設定を最初に削除した場合だけです。もしくは、次のエラーが表示されます。「NBM 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 nbm 設定を削除し、再試行してください。

ステップ 4	（任意） [**no**] **nbm host-policy**
	例：
	`switch(config)# nbm host-policy`
	`switch(config-nbm-host-pol)#`
		スイッチの NBM ホスト ポリシーを設定します。

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 NBM ホスト ポリシーを設定します。
				（注） デフォルトの NBM 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。

	コマンドまたはアクション	目的
ステップ 6	（任意） **default** {**permit** | **deny**} 例： `switch(config-nbm-host-pol-sender)# default permit`	NBM 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。NBM 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： `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 NBM 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 10	[**no**] **nbm flow bandwidth** *flow-bandwidth* {**kbps** | **mbps** | **gbps**} 例：	Kbps、Mbps、または Gbps でグローバル NBM 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。

	コマンドまたはアクション	目的
	`switch(config)# nbm flow bandwidth 3000 mbps`	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 11	[**no**] **nbm flow dscp** *value* 例： `switch(config)# nbm flow dscp 10`	グローバル NBM 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 NBM 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 NBM 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：
	`switch(config-nbm-flow-pol)# policy nbmflow10`
	`switch(config-nbm-flow-pol-attr)#`
		NBM フローポリシーを設定します。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 16	（任意）[**no**] **policer** 例： `switch(config-nbm-flow-pol-attr)# no policer`	指定された NBM 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

	コマンドまたはアクション	目的
		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、NBM 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：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 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：
	`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 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。

	コマンドまたはアクション	目的

次のタスク

フローの確立 (オプション)

スタティック フロー プロビジョニング向け NBM VRF の設定

スタティック フロー プロビジョニング用に NBM VRF を設定できます。これにより、NBM 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 NBM 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

NBM を設定します。

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

NBM VRF を PIM アクティブ モードから PIM パッシブ モードに変更できるのは、VRF でカスタム設定を最初に削除した場合だけです。もしくは、次のエラーが表示されます。「NBM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 nbm 設定を削除し、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

	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`	NBM VRF を作成します。

	コマンドまたはアクション	目的
ステップ 3	**nbm mode pim-passive** 例： `switch(config)# nbm mode pim-passive`	NBM ファブリックが外部コントローラの支援を受けてマルチキャスト 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「

NBM サブインターフェイス タイプの設定

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 NBM 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 NBM 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 NBM 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 NBM 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

	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`	NBMサブインターフェイスの帯域幅を設定します。パーセンテージの範囲は 0 ～ 100 です。0 は、このリンクのNBM帯域幅の予約がないことを示します。 NBM 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)

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

NBM フロー定義の作成

NBM フロー定義を作成することにより、NBM フローを確立できます。

NBM は CLI と API を公開して、受信者がフローへの参加または離脱に関心があることを通知するためにIGMPを使用しない場合に、受信者にフローをプロビジョニングします。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

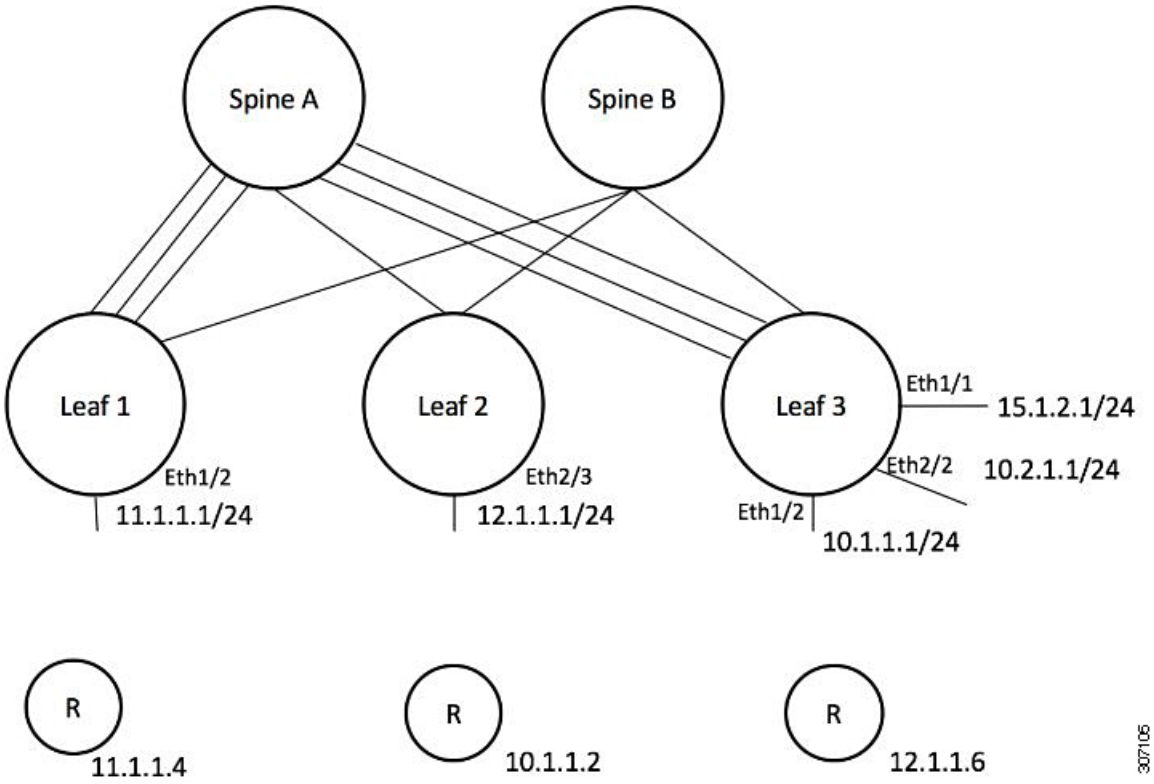
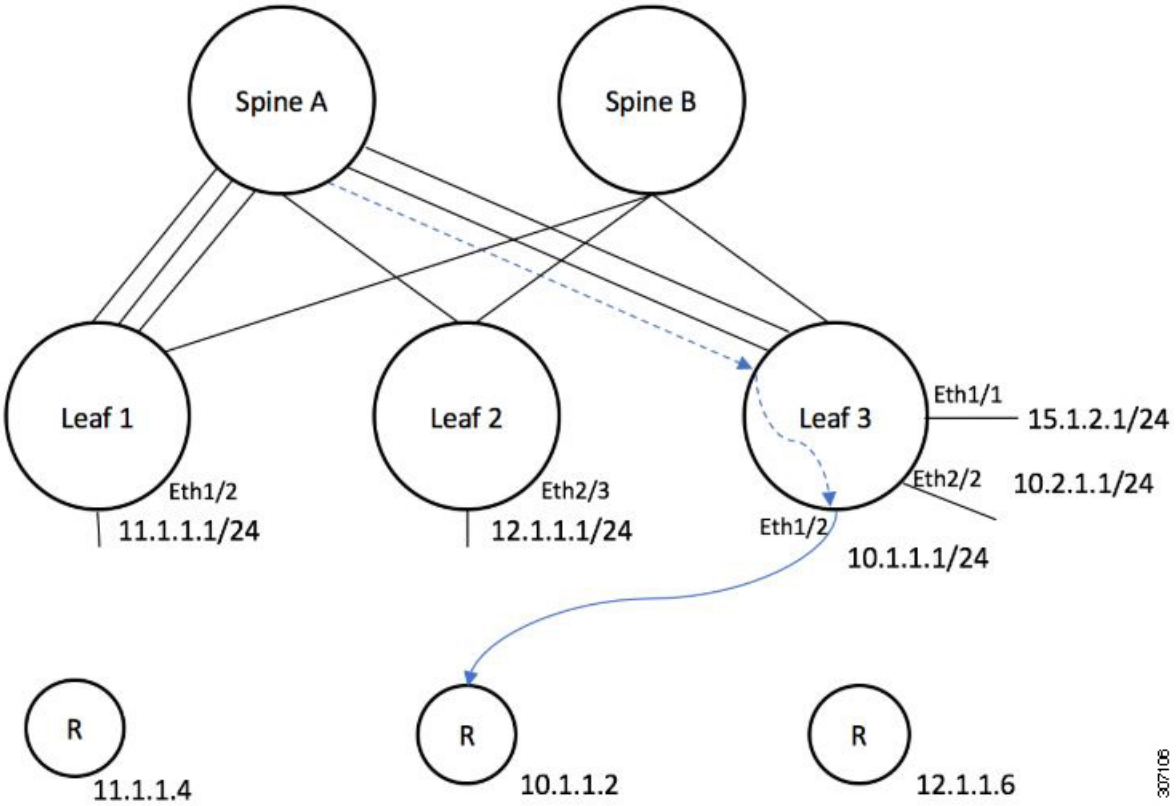


図 *2:* リーフから受信者へのトラフィック



始める前に

NBM 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

	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

	コマンドまたはアクション	目的

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)#`
		NBM フロー定義を設定します。

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、NBM 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

	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

	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 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 NBM を設定します。

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、スパイン スイッチで 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

	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`	NBM 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。
ステップ 3	**ip pim sparse mode** 例： `switch(config)# ip pim sparse mode`	NBM 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、NBM 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

	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。

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。

	コマンドまたはアクション	目的

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：
	`switch(config)# class-map type qos match-any pmn-mcast`
	`switch(config-cmap-qos)#`
		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。

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、PMN 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。

	コマンドまたはアクション	目的

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、PMN 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。

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
```

NBM 設定の確認

NBM の設定情報を表示するには、次のいずれかの作業を行います。

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*}]	NBM 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 [**vrf** {**all** | *vrf-name*}]	NBM フロー定義のスタティック 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 NBM 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*}]	NBM 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*}]	NBM 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 NBM 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 NBM ホスト ポリシーを表示します。
show nbm interface bandwidth	NBM インターフェイスの帯域幅を表示します。
show running-config nbm	NBM の実行コンフィギュレーション情報を表示します。

（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 を参照してください。

NBM フロー統計のクリア

NBM 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 NBM 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 NBM 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

	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 1/1`
	`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。
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 NBM でサポートされます。

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。