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 7.0(3)I4(5)、7.0(3)I6(1)、および 7.0(3)F2(1)

初版：2016 年 12 月 22 日

最終更新：2017 年 05 月 15 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。

© 2016-2017 Cisco Systems, Inc. All rights reserved.

目 次

新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

Cisco IP Fabric for Media ソリューションの概要 3

IP Fabric for Media ソリューションについて 3

導入タイプ 4

DCNM メディア コントローラ使用のスパイン リーフのトポロジ 4

DCNM メディア コントローラ使用のシングル モジュラ型スイッチのトポロジ 5

DCNM メディア コントローラ不使用のシングル モジュラ型スイッチのトポロジ 5

IP Fabric for Media ソリューションのコンポーネント 5

Cisco Nexus 9000 シリーズ スイッチ 5

DCNM メディア コントローラ 7

障害処理 7

IP Fabric for Media ソリューションの利点 7

関連資料 8

IP Fabric for Media のセットアップ 11

IP ファブリックで必要なリーフ スイッチの数とタイプの判定 11

IP ファブリックで実行可能なフロー数の判定 14

IP Fabric for Media の設定 15

前提条件 15

注意事項と制約事項 16

ユニキャスト PTP の注意事項と制約事項 17

DCNM メディア コントローラの注意事項と制約事項 18

ライセンス要件 19

NBM の設定 19

スパイン リーフ展開に向けた NBM の設定 20

DCNM 使用のシングル モジュラ型スイッチに向けた NBM の設定 21
DCNM 不使用のシングル モジュラ型スイッチに向けた NBM の設定 23
NBM 設定の確認 25
show コマンドの出力例 26
Cisco NX-OS 7.0(3)F2(1) 以降を実行するスイッチでの出力例 26
Cisco NX-OS 7.0(3)I6(1) 以降を実行するスイッチでの出力例 27
ファブリック インターフェイスとホスト インターフェイスの設定 28
ファブリック インターフェイスの設定 28
ホスト インターフェイスの設定 30
メディアに向けた PTP の設定（任意） 31
ユニキャスト PTP ピアの設定 35
メディア コントローラ 39
メディア コントローラのトポロジ 40
PMN ホスト 41
PMN ホストの追加 42
PMN ホストの編集 43
PMN ホストの削除 43
PMN ホストのインポート 44
PMN ホストのエクスポート 44
フロー エイリアス 44
フロー エイリアスの追加 45
フロー エイリアスの編集 46
フロー エイリアスの削除 46
フロー エイリアスのエクスポート 46
フロー エイリアスのインポート 47
ポリシー 47
ホストポリシー 47
ホスト ポリシーの追加 49
ホスト ポリシーの編集 50
ホスト ポリシーの削除 50
ホスト ポリシーのインポート 51
ホスト ポリシーのエクスポート 51

フロー ポリシー 51
フロー ポリシーの追加 53
フロー ポリシーの編集 53
フロー ポリシーの削除 54
フロー ポリシーのインポート 54
フロー ポリシーのエクスポート 55
フローの状態 55
Event 58

第 1 章

新機能および変更された機能に関する情報

この章では、『*Cisco Nexus 9000 Series NX-OS IP Fabric for Media Solution Guide*』に記載されている新機能および変更された各機能について、リリース固有の情報を示します。

- 新機能および変更された機能に関する情報，1 ページ

新機能および変更された機能に関する情報

次の表は、『*Cisco Nexus 9000 Series NX-OS IP Fabric for Media Solution Guide*』に記載されている新機能および変更機能をまとめたものです。それぞれの説明が記載されている箇所も併記されています。

表 *1*：新機能および変更された機能

機能	説明	変更されたリリース	参照先
IP Fabric for Media	Cisco Nexus 9508 スイッチ（N9K-X9636C-R および N9K-X9636Q-R ライン カードを使用）の、スパイン スイッチまたはシングル モジュラ型スイッチとしてのサポートが追加されました。	7.0(3)F2(1)	Cisco IP Fabric for Media ソリューションの概要，（3 ページ） IP Fabric for Media の設定，（15 ページ）

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
IP Fabric for Media	Cisco Nexus 9500 シリーズ スイッチ（N9K-X9732C-EX、N9K-X9736C-EX、および N9K-X97160YC-EX ライン カードを使用）の、スパインスイッチまたはシングルモジュラ型スイッチとしてのサポートが追加されました。	7.0(3)I6(1)	Cisco IP Fabric for Media ソリューションの概要, （3 ページ） IP Fabric for Media の設定, （15 ページ）
フロー エイリアスと帯域幅のトラッキング	これらの機能が追加されました。	DCNM 10.2.1	メディア コントローラ
IP Fabric for Media	DCNM メディア コントローラを伴う初回リリース。	7.0(3)I4(5)	

第 2 章

Cisco IP Fabric for Media ソリューションの概要

この章には、Cisco IP Fabric for Media ソリューションに関する情報が記載されています。

- IP Fabric for Media ソリューションについて，3 ページ
- IP Fabric for Media ソリューションのコンポーネント，5 ページ
- 障害処理，7 ページ
- IP Fabric for Media ソリューションの利点，7 ページ
- 関連資料，8 ページ

IP Fabric for Media ソリューションについて

現在、ブロードキャスト業界では、ビデオおよび音声トラフィックの転送に、シリアル デジタル インターフェイス（SDI）ルータと SDI ケーブルが使用されています。SDI ケーブルで伝送できるのは、単一の単方向の信号のみです。その結果、多数のケーブルが必要で、ケーブルを長く延長する必要があることも多いため、SDI ベースのインフラストラクチャの拡張または変更は難しく、時間が掛かります。

Cisco IP Fabric for Media ソリューションは、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 本のケーブルで双方向のトラフィック フローを複数伝送でき、物理的な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 サイズに対応することができます。

IP Fabric for Media ソリューションは、柔軟なスパイン リーフのアーキテクチャ、またはシングル モジュラ型スイッチのトポロジで構成されます。このソリューションは、Cisco Nexus 9000 シリーズ スイッチを Cisco Non-blocking Multicast（NBM）アルゴリズム（インテリジェントなトラフィック管理アルゴリズム）と併せて使用します。Cisco Data Center Network Manager（DCNM）メディア コントローラは任意で使用します。オープン API を使用すると、Cisco DCNM メディア コントローラをさまざまなブロードキャスト コントローラと統合することができます。このソリュー

ションにより、信頼性（ゼロ ドロップのマルチキャスト）、可視性、安全性、および可用性がいずれも高いネットワークが実現されます。

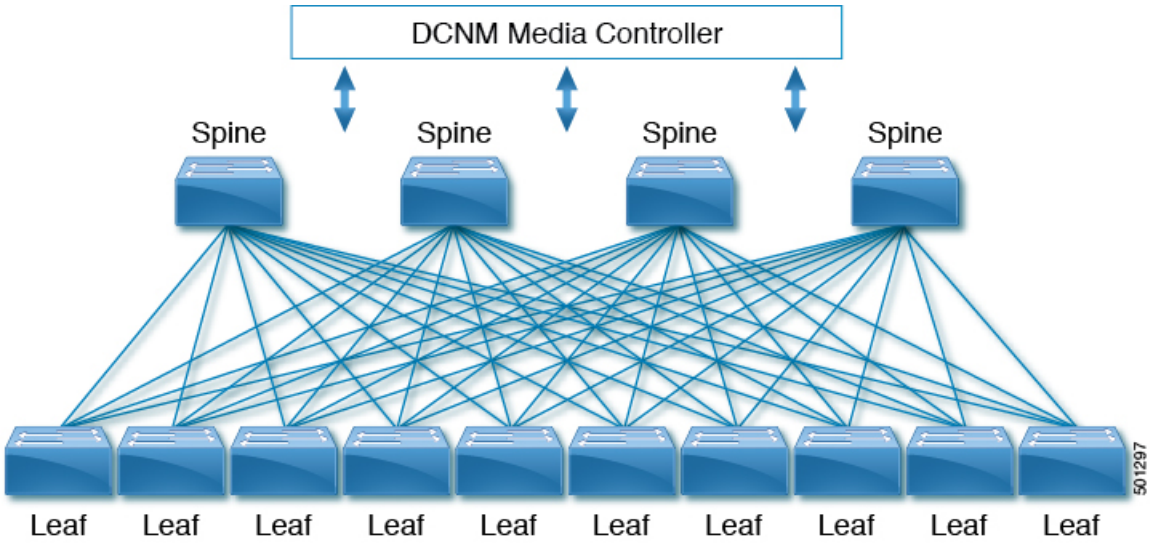
導入タイプ

Cisco IP Fabric for Media ソリューションは、次のタイプの展開をサポートしています。

- DCNM メディア コントローラ使用のスパイン リーフのトポロジ：IP スタジオによく見られる、大規模な展開に適した柔軟なアーキテクチャ。
- DCNM メディア コントローラ使用のシングル モジュラ型スイッチ：コントローラによってフローの可視性、セキュリティ、およびモニタリングなどの機能が提供される、固定的な展開に適したアーキテクチャ。
- DCNM メディア コントローラ不使用のシングル モジュラ型スイッチ：局外中継（OB）車のような環境に適したシンプルな展開方法。

DCNM メディア コントローラ使用のスパイン リーフのトポロジ

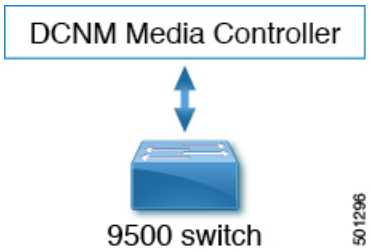
Cisco IP Fabric for Media ソリューションは、複数のスパイン スイッチおよびリーフ スイッチと DCNM メディア コントローラで構成される、スパイン リーフのトポロジをサポートします。このトポロジは、あらゆるリーフ スイッチの組み合わせをサポートし、1 つのタイプのリーフ スイッチのみを使用することも可能です。



メディア送信元と受信者は、リーフ スイッチに接続します。受信者は、メディア トラフィックを受信するため、リーフ スイッチへの IGMP Join 要求を開始します。

DCNM メディア コントローラ使用のシングル モジュラ型スイッチのトポロジ

Cisco IP Fabric for Media ソリューションは、Cisco NX-OS リリース 7.0(3)I6(1) 以降のリリースを実行し、DCNM メディア コントローラを使用している 1 台の Cisco Nexus 9500 シリーズ スイッチで構成されるシングル モジュラ型スイッチのトポロジをサポートします。



DCNM メディア コントローラ不使用のシングル モジュラ型スイッチのトポロジ

Cisco IP Fabric for Media ソリューションは、Cisco NX-OS リリース 7.0(3)F2(1) 以降のリリースまたは Cisco Nexus 7.0(3)I6(1) 以降のリリースを実行し、DCNM メディア コントローラを使用していない 1 台の Cisco Nexus 9500 シリーズ スイッチで構成されるシングル モジュラ型スイッチのトポロジをサポートします。

IP Fabric for Media ソリューションのコンポーネント

Cisco Nexus 9000 シリーズ スイッチ

IP ファブリック経由のビデオおよび音声トラフィックの転送には、次の Cisco Nexus 9000 シリーズ スイッチが使用されています。

Cisco Nexus 9000 シリーズ スイッチ	ポートの数とサイズ	初期の Cisco NX-OS リリース	トポロジにおける役割
Cisco Nexus 9236C スイッチ	36 個の 40/100 Gbps ポート	7.0(3)I4(5)*	DCNM メディア コントローラ使用のスパイン リーフのトポロジにおける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	初期の Cisco NX-OS リリース	トポロジにおける役割
Cisco Nexus 9272Q スイッチ	72 個の 40 Gbps ポート	7.0(3)I4(5)*	DCNM メディア コントローラ使用のスパイン リーフのトポロジにおけるスパインまたはリーフ
Cisco Nexus 92160YC-X スイッチ	48 個の 1/10/25 Gbps ポート	7.0(3)I4(5)*	DCNM メディア コントローラ使用のスパイン リーフのトポロジにおけるリーフ
Cisco Nexus 93108TC-EX スイッチ	48 個の 1/10 Gbps ポート	7.0(3)I4(5)*	DCNM メディア コントローラ使用のスパイン リーフのトポロジにおけるリーフ
Cisco Nexus 93180YC-EX スイッチ	48 個の 1/10/25 Gbps ポート	7.0(3)I4(5)*	DCNM メディア コントローラ使用のスパイン リーフのトポロジにおけるリーフ
次のライン カードを備えた Cisco Nexus 9508 スイッチ • N9K-X9636C-R • N9K-X9636Q-R	36 個の 100 Gbps ポート（N9K-X9636C-R ライン カードの場合）** 36 個の 40 Gbps ポート（N9K-X9636Q-R ライン カードの場合）**	7.0(3)F2(1)	DCNM メディア コントローラ使用のスパイン リーフのトポロジにおけるスパイン DCNM メディア コントローラ不使用のシングル モジュラ型スイッチ
次のラインカードを備えた Cisco Nexus 9500 シリーズ スイッチ • N9K-X9732C-EX • N9K-X9736C-EX • N9K-X97160YC-EX	32 個の 40/100 Gbps ポート（N9K-X9732C-EX ライン カードの場合） 36 個の 40/100 Gbps ポート（N9K-X9736C-EX ライン カードの場合） 48 個の 10/25 Gbps ポート（N9K-X97160YC-EX ライン カードの場合）	7.0(3)I6(1)	DCNM メディア コントローラ使用のスパイン リーフのトポロジにおけるスパイン DCNM メディア コントローラ使用または不使用のシングル モジュラ型スイッチ

* リーフ スイッチは、Cisco NX-OS リリース 7.0(3)F2(1) 以降のリリースを実行するスパイン スイッチと一緒に使用する場合、Cisco NX-OS 7.0(3)I6(1) 以降のリリースを実行している必要があります。

** 最新のブレークアウトおよびオプティクスのサポートについては、https://www.cisco.com/c/en/us/support/interfaces-modules/transceiver-modules/products-device-support-tables-list.html を参照してください。

DCNM メディア コントローラ

オープン API を使用すると、Cisco DCNM メディア コントローラをブロードキャスト コントローラとシームレスに統合することができ、同様のオペレータ ワークフローでIPベースのインフラストラクチャの利点をすべて享受できます。DCNM メディア コントローラには直観的な GUI が備わっており、メディア ネットワークのために設計された事前定義のテンプレートを使用して IP ファブリックを設定することができます。

DCNM メディア コントローラでは、次のことができます。

- 個々のホストに対して汎用またはマルチキャスト固有のセキュアなポリシーを設定し、ホストをそれぞれの役割に基づいて許可または拒否すること。
- 複数のホストとフローに対し、セキュアなマルチキャスト固有のポリシーを設定すること。
- エンドツーエンドのトラフィック フローと帯域幅の使用率を表示し、ファブリックにおける問題の領域（リンク障害やオーバーサブスクリプションなど）を迅速に特定すること。
- 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すること。
- 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すること。

サポートされる DCNM リリースの一覧については、前提条件, （15 ページ）の項を参照してください。

障害処理

Cisco IP Fabric for Media ソリューションは、確実性の高い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の際は、十分な帯域幅が使用可能であれば、影響を受けるフローが代替リンクに移動されます。SMPTE 2022-7 を使用すると、エンドポイントに冗長性ができ、リンクまたはスイッチの障害が実稼働トラフィックに影響しなくなります。

IP Fabric for Media ソリューションの利点

Cisco IP Fabric for Media ソリューションには、次の利点があります。

- 特化されたハードウェア（SDI ルータ）を汎用のスイッチング インフラストラクチャで代替します。
- さまざまな種類およびサイズのブロードキャスト機器のエンドポイントを最大 100 Gbps のポート スピードでサポートします。
- 4K および 8K Ultra HD を含む最新のビデオ テクノロジーをサポートします。
- 水平的な拡張が可能です。容量の増加が必要になった場合は、リーフ スイッチを追加することで、さらに多くのエンドポイントをサポートできます。
- パケット損失がなく、遅延がきわめて少なく、ジッターが最小限の確実性の高いネットワークを提供します。
- すべてのメディア送信元と受信者を同期できます。
- 確実性の高い障害処理を提供し、リーフとスパインの間でリンク障害が発生してもトラフィックを受信者に送信します。
- ポスト プロダクション作業に向け、ライブとファイル ベースのトラフィック フローの共存をサポートします。
- 高いネットワーク セキュリティを提供します。
- ノンブロッキングのネットワーク設計を提供し、リンクのオーバーサブスクリプションを防ぎます。
- 既存のオペレータ ワークフローの変更が不要です。

関連資料

関連項目	マニュアル タイトル
IP Fabric for Media	『Cisco IP Fabric for Media Solution video』
Cisco DCNM メディア コントローラ	『Cisco DCNM Installation Guide』 『Cisco DCNM online help』 『Cisco DCNM API Reference』
Cisco NX-OS リリース情報	『Cisco Nexus 9000 Series NX-OS IP Fabric for Media Release Notes, Release 7.0(3)F2(1)』 『Cisco Nexus 9000 Series NX-OS IP Fabric for Media Release Notes, Release 7.0(3)I6(1)』 『Cisco Nexus 9000 Series NX-OS IP Fabric for Media Release Notes, Release 7.0(3)I4(5)』
Cisco NX-OS ソフトウェアのアップグレード	『Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide』

関連項目	マニュアル タイトル
PTP	『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』
TCAM カービング	『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』

関連資料

- 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 7.0(3)I4(5)、7.0(3)I6(1)、および 7.0(3)F2(1)

第 3 章

IP Fabric for Media のセットアップ

この章では、メディア ネットワーク用の IP ファブリックをセットアップする方法について説明します。

- IP ファブリックで必要なリーフ スイッチの数とタイプの判定，11 ページ
- IP ファブリックで実行可能なフロー数の判定，14 ページ

IP ファブリックで必要なリーフ スイッチの数とタイプの判定

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、放送センター内のエンドポイントの数とタイプによって決まります。

必要なリーフ スイッチの数を判定するには、次の手順を実行します。

1. 放送センター内のエンドポイント（カメラ、マイクなど）の数を数えます（たとえば、10 Gbps のエンドポイント 360 個、40 Gbps のエンドポイント 50 個）。
2. 放送センター内のエンドポイントのタイプを基に、必要なリーフ スイッチのタイプを判定します。
   - 10 Gbps のエンドポイントについては、Cisco Nexus 92160YC-X、93108TC-EX、または 93180YC-EX のリーフ スイッチを使用する必要があります。
   - 40 Gbps のエンドポイントについては、Cisco Nexus 9236C または 9272Q のリーフ スイッチが使用できます。
3. エンドポイントと各リーフ スイッチがサポートするアップリンクの数を基に、必要なリーフ スイッチの数を判定します。

表 *2*：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

リーフ スイッチ	エンドポイントの容量	アップリンクの容量
Cisco Nexus 9236C スイッチ	25 個の 40 Gbps エンドポイント	10 個の 100 Gbps アップリンク（1000 Gbps）
Cisco Nexus 9272Q スイッチ	36 個の 40 Gbps エンドポイント	36 個の 40 Gbps アップリンク（1440 Gbps）
Cisco Nexus 92160YC-X スイッチ	40 個の 10 Gbps エンドポイント	4 個の 100 Gbps アップリンク（400 Gbps）
Cisco Nexus 93108TC-EX スイッチ	48 個の 10 Gbps エンドポイント	6 個の 100 Gbps アップリンク（600 Gbps）
Cisco Nexus 93180YC-EX スイッチ	48 個の 10 Gbps エンドポイント	6 個の 100 Gbps アップリンク（600 Gbps）

次に例を示します。

- 360 個の 10 Gbps エンドポイントの場合、Cisco Nexus 93180YC-EX リーフ スイッチは、1 台当り最大 48 個 の 10 Gbps エンドポイントをサポートできるため、8 台必要です。
- 50 個の 40 Gbps エンドポイントの場合、Cisco Nexus 9236C リーフ スイッチは、1 台当り最大 25 個 の 40 Gbps エンドポイントをサポートできるため、2 台必要です。

4 アップリンクの帯域幅（スパイン スイッチ方向）は必ず、ダウンストリームの帯域幅（エンドポイント方向）と同じまたはそれより大きくします。

a アップリンクの帯域幅を判定するには、次の等式を使用します。

リーフ スイッチごとのアップリンクの容量 x リーフスイッチの数 = アップリンクの帯域幅

次に例を示します。

600 Gbps（Cisco Nexus 93180YC-EX スイッチ 1 台のアップリンクの容量）X Cisco Nexus 93180YC-EX リーフ スイッチ 8 台 = アップリンクの帯域幅 4800 Gbps

1000 Gbps（Cisco Nexus 9236C スイッチ 1 台のアップリンクの容量）X Cisco Nexus 9236C リーフ スイッチ 2 台 = アップリンクの帯域幅 2000 Gbps

アップリンクの帯域幅 4800 Gbps（Cisco Nexus 93180YC-EX のリーフ スイッチ 8 台）+ アップリンクの帯域幅 2000 Gbps（Cisco Nexus 9236C のリーフ スイッチ 2 台）= アップリンクの帯域の幅合計 6800 Gbps

b ダウンストリームの帯域幅を判定するには、次の等式を使用します。

リーフ スイッチごとのエンドポイントの容量 x リーフスイッチの数 = ダウンストリームの帯域幅

次に例を示します。

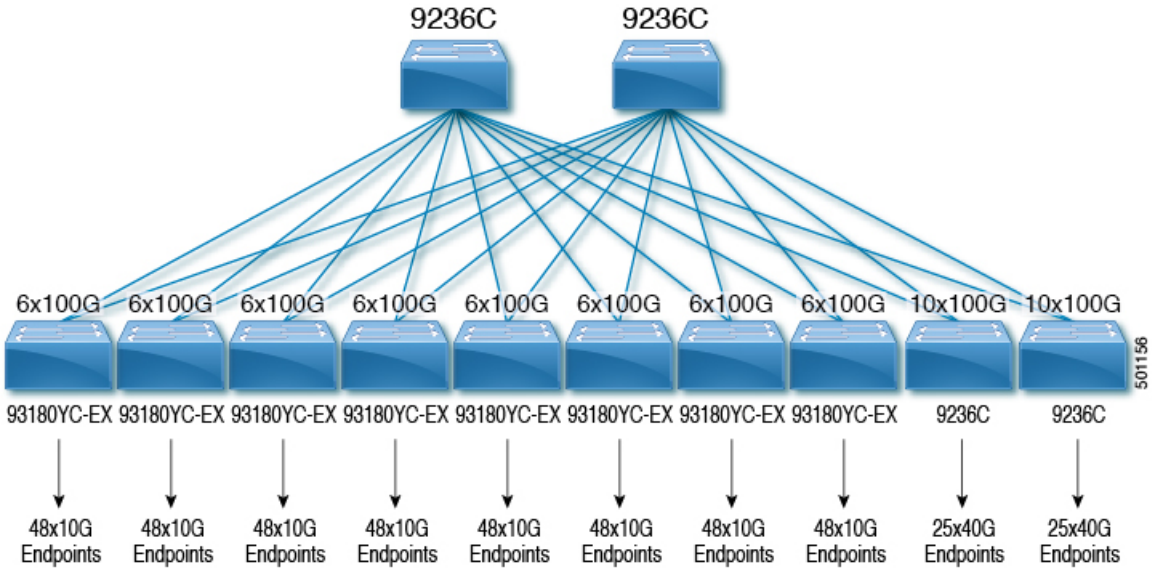
Cisco Nexus 93180YC-EX リーフ スイッチ 1 台 あたり 48 X 10 Gbps（エンドポイントの容量 480 Gbps）X リーフ スイッチ 8 台 = ダウンストリームの帯域幅 3840 Gbps

Cisco Nexus 9236C リーフ スイッチ 1 台 あたり 25 X 40 Gbps（エンドポイントの容量 1000 Gbps）X リーフ スイッチ 2 台 = ダウンストリームの帯域幅 2000 Gbps

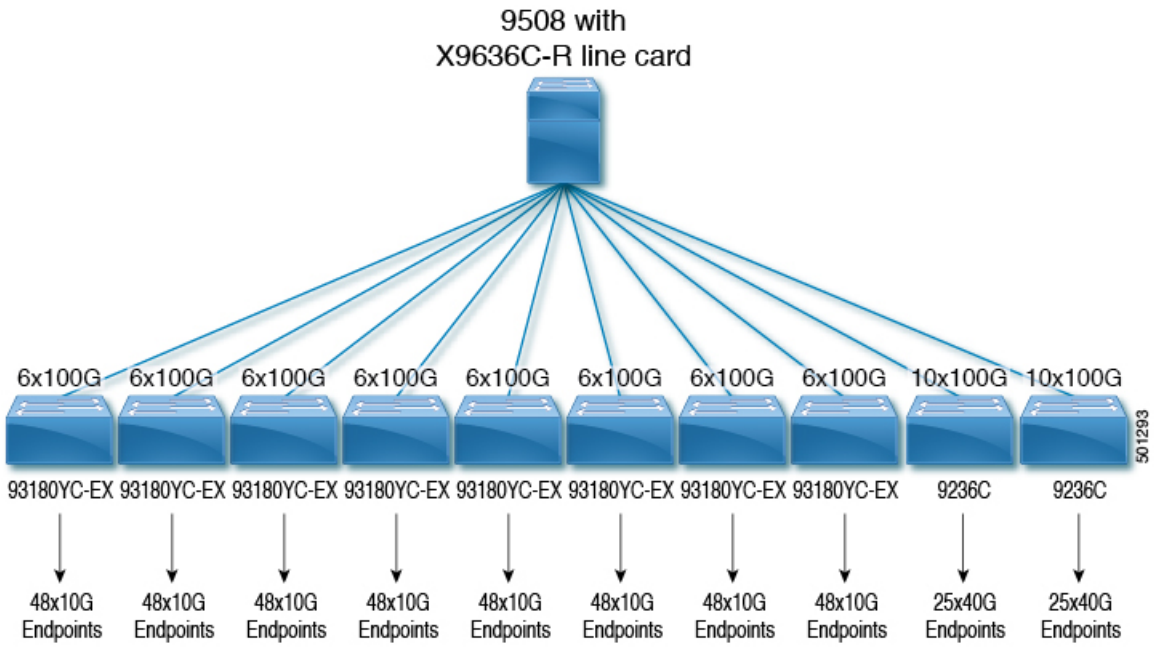
ダウンストリームの帯域幅 3840 Gbps（Cisco Nexus 93180YC-EX のリーフ スイッチ 8 台）+ ダウンストリームの帯域幅 2000 Gbps（Cisco Nexus 9236C のリーフ スイッチ 2 台）= ダウンストリームの帯域幅合計 5840 Gbps

5 アップリンクの帯域幅の合計がダウンストリームの帯域幅の合計と同じまたはそれより大きければ、トポロジは有効です。これで、実行可能なフローの数を判定できます。アップリンクの帯域幅がダウンストリームの帯域幅より小さい場合、シスコは、ベストプラクティスとして、アップストリームの帯域幅がダウンストリームの帯域幅と同じまたはそれより大きくなるまでトポロジを修正することを推奨します。

この項で提示した例を使用すると、トポロジは次のようになります。



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



IP ファブリックで実行可能なフロー数の判定

IP ファブリックで実行可能なフローの数を判定するには、次の等式を使用します。

合計帯域幅 ÷ フロー サイズ = 実行可能なフロー数

フローサイズは設定可能で、通常は、放送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*：各ビデオ テクノロジーのフロー 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	3 Gbps（3000 Mbps）
4K Ultra HD ビデオ	12 Gbps（12,000 Mbps）
8K Ultra HD ビデオ	48 Gbps（48,000 Mbps）

次に例を示します。

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

第 4 章

IP Fabric for Media の設定

この章では、Cisco IP Fabric for Media ソリューションに向けて 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，15 ページ
- 注意事項と制約事項，16 ページ
- ライセンス要件，19 ページ
- NBM の設定，19 ページ
- ファブリック インターフェイスとホスト インターフェイスの設定，28 ページ
- メディアに向けた PTP の設定（任意），31 ページ
- ユニキャスト PTP ピアの設定，35 ページ

前提条件

Cisco IP Fabric for Media ソリューションには、次の前提条件があります。

- Cisco Nexus 9200 および 9300 シリーズのリーフ スイッチおよびスパイン スイッチでは、Cisco NX-OS リリース 7.0(3)I4(5) 以降のリリースを実行している必要があります。

（注） リーフ スイッチは、Cisco NX-OS リリース 7.0(3)F2(1) 以降のリリースを実行するスパイン スイッチと一緒に使用する場合、Cisco NX-OS 7.0(3)I6(1) 以降のリリースを実行している必要があります。

- Cisco Nexus 9500 シリーズのスパイン スイッチ（N9K-X9732C-EX、N9K-X9736C-EX、および N9K-X97160YC-EX ライン カードを使用）は、NX-OS リリース 7.0(3)I6(1) 以降のリリースを実行している必要があります。

- Cisco Nexus 9508 のスパイン スイッチ（N9K-X9636C-R および N9K-X9636Q-R ライン カードを使用）は、Cisco NX-OS リリース 7.0(3)F2(1) 以降のリリースを実行している必要があります。
- TCAM カービングは、リーフ スイッチに対し、**hardware access-list tcam region ing-racl 768** コマンドおよび **hardware access-list tcam region ing-l3-vlan-qos 1536** コマンドを使用して設定する必要があります。TCAM カービングの詳細については、『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』を参照してください。
- Cisco Nexus 9500 シリーズ スイッチで N9K-X9732C-EX、N9K-X9736C-EX、および N9K-X97160YC-EX ライン カードを使用している場合は、**system routing template-multicast-nbm** コマンドを使用して、マルチキャスト NBM テンプレートをイネーブルにします。詳細については、『Cisco Nexus 9000 Series Multicast Routing Configuration Guide』を参照してください。
- コントローラ ベースの展開には、次の Cisco DCNM リリースのいずれか 1 つをインストールする必要があります。インストール手順については、お使いの DCNM リリースの『Cisco DCNM Installation Guide』を参照してください。

スイッチ上で実行されている Cisco NX-OS リリース	Cisco DCNM リリース
7.0(3)I4(5)	10.1
7.0(3)F2(1) または 7.0(3)I6(1)	10.2.1 以降

- DCNM OVA ファイルがインストールされたら、SSH でルートとして DCNM VM にログオンし、DCNM サーバに **appmgr set-mode media-controller** コマンドを入力して、DCNM メディア コントローラをイネーブルにする必要があります。

注意事項と制約事項

Cisco IP Fabric for Media ソリューションには、次の注意事項と制約事項が適用されます。

- 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 スイッチ上で使用可能なポートの数によって決まります。
- コントローラへの接続が常に可能になるよう、冗長パスを確保してください。
- Cisco Nexus 9508 スイッチを N9K-X9636C-R および N9K-X9636Q-R ライン カードと一緒に使用する場合、PTP、ポリシング、DSCP 再マーク、およびフロー統計はサポートされません。
- ノンブロッキングなパフォーマンスを確保するため、各リーフ スイッチからのアップリンクの帯域幅は、エンドポイントに与えられた帯域幅以上を確保してください。
- 可能であれば、エンドポイントをリーフ スイッチ間で分散させ、すべてのリーフ スイッチ上で送信者と受信者の分布を均等化してください。

- シスコでは、障害に対応できるよう、可能であればオーバープロビジョニングのアップリンクをお勧めします。
- 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接続するレイヤ 3 ポートを使用してください。IP アドレスは、エンドポイントに 1 つ、スイッチ インターフェイスに別の 1 つを割り当てます。
- 冗長な IP ネットワーク（2022-7）を設計します。2 つのネットワークを一緒に接続しないでください。これらは、互いから完全に独立している必要があります。
- ネットワークは、基本的にマルチキャスト フローを伝送するように設計されています。帯域幅管理ではユニキャストのフローをトラッキングしていないため、ユニキャストのトラフィックは最小限に留めてください。
- このソリューションは、IGMPv2 および IGMPv3 の Join をサポートしていますが、PIM SSM はサポートしていません。したがって、2 つの送信元が同一のマルチキャスト グループに同時に送信を行うことはできません。
- 統計情報は、送信者が接続されているスイッチでのみ使用できます。
- ホストはスパインに接続できません。
- ファブリックのセットアップに必要な場合以外は、カスタムの ACL ポリシーまたは QoS ポリシーを使用しないでください。このようなポリシーは、DCNM のホスト ポリシーまたはフロー ポリシーから適用する必要があります（CLI コマンドからではなく）。
- DCNM から適用されるポリシーを変更する際には、CLI コマンドを使用しないでください。変更は、すべて DCNM を使用して行う必要があります。
- コントローラ不使用の展開からコントローラ使用の展開に移行する際は、事前にスイッチから既存の設定を削除（**write erase** コマンドおよび **reload** コマンドを使用）し、POAP または IP Fabric for Media の設定, （15 ページ）で説明する CLI コマンドを使用してスイッチを再設定する必要があります。

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、次の注意事項と制約事項が適用されます。

- 個々のユニキャスト PTP インターフェイスには、一意の PTP ユニキャスト送信元アドレスを設定する必要があります。
- グローバルな PTP 送信元とユニキャスト インターフェイスの PTP 送信元は、同一であってはいけません。
- 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ません。
- ユニキャスト PTP をサポートするスイッチは、Cisco Nexus 9236C、9272Q、92160YC-X スイッチと、N9K-X9732C-EX、N9K-X9736C-EX、および N9K-X97160YC-EX ラインカードを備えた Cisco Nexus 9500 シリーズ スイッチのみです。

DCNM メディア コントローラの注意事項と制約事項

フローのセットアップには、次の注意事項と制約事項が適用されます。

- ブロードキャスト コントローラまたはユーザに再試行を要求する API コールが失敗した場合、DCNM は、ブロードキャスト コントローラまたはユーザに通知します。
- 受信側リーフ スイッチがリロードすると、スイッチのブートアップ後に、API コールを再度開始することでフローを再度セットアップする必要があります。この内容は DCNM 10.1 にのみ該当します。
- 静的 API は、SVI ではサポートされません。
- VM スナップショットはサポートされません。以前の DCNM 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。

フロー ポリシーには、次の注意事項と制約事項が適用されます。

- ベストプラクティスとして、デフォルトのポリシーの変更は、フローがファブリック内でアクティブになる前に行う必要があります。
- フローポリシーは、フローがアクティブであるときは変更できません。変更は、送信者がフローを停止し、すべての受信者がフローの受信を停止しているときに可能になります。
- ベストプラクティスとして、フローがポリシングされることなくある程度のバーストに対応できるよう、フローのビット レートに対して 5 % の余裕を持たせてください。3G のフローは 3.15 Gbps としてプロビジョニングする必要があります。
- デフォルトのフローポリシーに対するすべての変更は、フローがネットワーク内でアクティブになる前に完了してください。

ホスト ポリシーには、次の注意事項と制約事項が適用されます。

- 送信者のホストポリシーが「allow」から「deny」に変更されると、フローはただちに削除されます。
- 受信者のホストポリシーがレイヤ 2 ポートおよび SVI 経由で接続されているホストに適用されると、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 Join に適用され、単一の受信者に適用することはできません。
- ホワイトリスト ポリシーがインストールされているときにホストから ARP 要求または応答が来ない場合、そのホストは DCNM に追加されず、IGMP パケットは破棄されます。ホワイトリスト ポリシーについては、IGMP Join を送信する前に ARP を通じてホストを追加する必要があります。
- デフォルトのホストポリシーに対するすべての変更は、ネットワーク上でアクティブなホストが検出される前に完了してください。デフォルトのホストポリシー定義をホワイトリストとブラックリストのいずれにするか（すべてのデフォルトを拒否するか、すべてのデフォルトを許可するか）は、ホストがネットワークに追加される前に定義する必要があります。ホ

ストごとのポリシーは、いつでも変更できます。ただし、デフォルトのポリシーの編集は、ホストが DCNM システムに導入される前のみ可能です。

ネットワークおよび DCNM 接続には、次の注意事項と制約事項が適用されます。

- スイッチは、ホストが検出される前、またはファブリック内でフローがセットアップされる前に DCNM によって検出されるようにしてください。
- DCNM HA ペアは、同じ VLAN 上にある必要があります。
- 相互接続として MGMT を使用する利点は、管理プレーンまたは制御プレーンとデータ プレーンを分離できることです。
- INBAND を使用する利点は、冗長性が強化されることです。
- スイッチと DCNM の間の遅延は、フロー プログラミングが許容される遅延範囲内で実行されるよう、1 ミリ秒未満である必要があります。

ライセンス要件

製品	ライセンス要件
Cisco NX-OS	IP Fabric for Media ソリューションには、LAN Enterprise Services ライセンスと、Network Services ライセンスが必要です。Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『Cisco NX-OS Licensing Guide』を参照してください。
Cisco DCNM	Cisco DCNM メディア コントローラには、Advanced Server DCNM ライセンスが必要です。このライセンスの詳細については、『Cisco DCNM Installation Guide』を参照してください。

NBM の設定

Non-blocking Multicast（NBM）を設定する手順は、IP Fabric for Media ソリューションにいずれの展開方法を使用しているかによって異なります。

- スパイン リーフのトポロジ
- シングル モジュラ型スイッチ

スパイン リーフ展開に向けた NBM の設定

IP ファブリックをセットアップした後は、Non-blocking Multicast（NBM）機能をイネーブルにし、DCNM サーバへの接続を確立する必要があります。NBM 機能により、ファブリックに入る帯域幅は、ファブリックから出る帯域幅と完全に同じになります。

スパイン リーフ展開におけるスイッチに向けて NBM を設定するには、次の手順に従います。

手順の概要

1. **configure terminal**
2. [**no**] **feature nxapi**
3. [**no**] **feature nbm**
4. **nbm mode controller**
5. **controller ip***dcnm-server-ip-or-vip***vrf management**
6. **controller-credentials username***username***password** [**0** | **7**] *password*
7. （任意） **show nbm controller**

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**] **feature nxapi** 例： `switch(config)# feature nxapi`	NX-API 機能をイネーブルにします。このコマンドの **no** 形式を使用すると、この機能がディセーブルになります。
ステップ 3	[**no**] **feature nbm** 例： `switch(config)# feature nbm`	NBM 機能をイネーブルにします。このコマンドの **no** 形式を使用すると、この機能がディセーブルになります。

ステップ 4	**nbm mode controller**
	
	例：
	`switch(config)# nbm mode controller`
	`switch(config-nbm-controller)#`
		DCNM メディア コントローラの存在をスイッチに通知します。

ステップ 5	**controller ip***dcnm-server-ip-or-vip***vrf management** 例： `switch(config-nbm-controller)# controller ip 10.1.1.1 vrf management`	DCNM サーバの IP アドレスまたは DCNM ネイティブ HA サーバの仮想 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	**controller-credentials username***username***password** [**0** | **7**] *password* 例： `switch(config-nbm-controller)# controller-credentials username admin password 7 7h56ab9`	DCNM サーバのログイン情報を設定します。 オプションの **0** は、パスワードがクリアテキストであることを、**7** は、パスワードが暗号化されていることを意味します。デフォルトは 0（クリア テキスト）です。

ステップ 7	**show nbm controller**
	
	例：
	`switch(config-nbm-controller)# show nbm controller`
	`VRF IP Role Status Online-Since`
	`--- --- ---- ------ ------------`
	`management 10.10.10.1 ACTIVE ONLINE 2016-11-04 17:08:33.080791`
		（任意）
		DCNM メディア コントローラの状態を表示します。

DCNM 使用のシングル モジュラ型スイッチに向けた NBM の設定

IP ファブリックをセットアップした後は、Non-blocking Multicast（NBM）機能をイネーブルにし、DCNM サーバへの接続を確立する必要があります。NBM 機能により、ファブリックに入る帯域幅は、ファブリックから出る帯域幅と完全に同じになります。

DCNM メディア コントローラを使用するシングル モジュラ型スイッチに向けて NBM を設定するには、次の手順に従います。

手順の概要

1. **configure terminal**
2. [**no**] **feature nxapi**
3. [**no**] **feature nbm**
4. **nbm mode controller**
5. **controller ip***dcnm-server-ip-or-vip***vrf management**
6. **controller-credentials username***username***password** [**0** | **7**] *password*
7. （任意） **show nbm controller**

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**] **feature nxapi** 例： `switch(config)# feature nxapi`	NX-API 機能をイネーブルにします。このコマンドの **no** 形式を使用すると、この機能がディセーブルになります。
ステップ 3	[**no**] **feature nbm** 例： `switch(config)# feature nbm`	NBM 機能をイネーブルにします。このコマンドの **no** 形式を使用すると、この機能がディセーブルになります。

ステップ 4	**nbm mode controller**
	
	例：
	`switch(config)# nbm mode controller`
	`switch(config-nbm-controller)#`
		DCNM メディア コントローラの存在をスイッチに通知します。

ステップ 5	**controller ip***dcnm-server-ip-or-vip***vrf management** 例： `switch(config-nbm-controller)# controller ip 10.1.1.1 vrf management`	DCNM サーバの IP アドレスまたは DCNM ネイティブ HA サーバの仮想 IP アドレスを指定します。
ステップ 6	**controller-credentials username***username***password** [**0** | **7**] *password* 例： `switch(config-nbm-controller)# controller-credentials username admin password 7 7h56ab9`	DCNM サーバのログイン情報を設定します。 オプションの **0** は、パスワードがクリアテキストであることを、**7** は、パスワードが暗号化されていることを意味します。デフォルトは 0（クリアテキスト）です。

ステップ 7	**show nbm controller**
	
	例：
	`switch(config-nbm-controller)# show nbm controller`
	`VRF IP Role Status Online-Since`
	`--- --- ---- ------ ------------`
	`management 10.10.10.1 ACTIVE ONLINE 2016-11-04 17:08:33.080791`
		（任意）
		DCNM メディア コントローラの状態を表示します。

DCNM 不使用のシングル モジュラ型スイッチに向けた NBM の設定

IP ファブリックをセットアップした後は、スイッチ上で NBM 機能をイネーブルにする必要があります。NBM機能により、ファブリックに入る帯域幅は、ファブリックから出る帯域幅と完全に同じになります。

DCNM メディア コントローラを使用しないシングル モジュラ型スイッチに向けて NBM を設定するには、次の手順に従います。

（注） 次の手順のステップ 3 から 8 は、N9K-X9636C-R および N9K-X9636Q-R ライン カードを備えた Cisco Nexus 9508 スイッチには該当しません。

手順の概要

1. **configure terminal**
2. [**no**] **feature nbm**
3. [**no**] **nbm flow bandwidth***flow-bandwidth*
4. [**no**] **nbm mode flow**
5. [**no**] **policy***policy-name*
6. [**no**] **bandwidth***flow-bandwidth*
7. [**no**] **ip group***ip-address*
8. [**no**] **ip group-range***ip-address***to***ip-address*
9. （任意） **show nbm flows bandwidth**

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**] **feature nbm** 例： `switch(config)# feature nbm`	NBM機能をイネーブルにします。このコマンドの **no** 形式を使用すると、この機能がディセーブルになります。
ステップ 3	[**no**] **nbm flow bandwidth***flow-bandwidth* 例： `switch(config)# nbm flow bandwidth 150`	グローバル NBM フローの帯域幅を Mbps 単位で設定します。有効範囲は 1 ～ 25,000 Mbps で、デフォルト値は 3000 Mbps です。

	コマンドまたはアクション	目的
		（注） NBM フローの帯域幅は、IP ファブリックを最初にセットアップするときに設定する必要があります。この値は、任意に変更しないでください。また、フロー帯域幅の既存の値に対する変更は、デバイスがリブートされないと適用されません。

ステップ 4	[**no**] **nbm mode flow**
	
	例：
	`switch(config)# nbm mode flow`
	`switch(config-nbm-flow)#`
		フローごとのフロー帯域幅を設定します。

ステップ 5	[**no**] **policy***policy-name*
	
	例：
	`switch(config-nbm-flow)# policy 1.5gbps`
	`switch(config-nbm-flow-policy)#`
		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 6	[**no**] **bandwidth***flow-bandwidth* 例： `switch(config-nbm-flow-policy)# bandwidth 1500`	このポリシーに一致するマルチキャスト グループのフロー帯域幅を Mbps 単位で設定します。有効範囲は 1 ～ 25,000 Mbps です。

ステップ 7	[**no**] **ip group***ip-address*
	
	例：
	`switch(config-nbm-flow-policy)# ip group 228.0.0.15`
	`switch(config-nbm-flow-policy)# 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 8	[**no**] **ip group-range***ip-address***to***ip-address*
	
	例：
	`switch(config-nbm-flow-policy)# ip group-range 239.255.255.121 to 239.255.255.130`
	`switch(config-nbm-flow-policy)# ip group-range 239.255.255.131 to 239.255.255.140`
	`switch(config-nbm-flow-policy)# ip group-range 239.255.255.141 to 239.255.255.150`
	`switch(config-nbm-flow-policy)# 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 9	**show nbm flows bandwidth** 例： `switch(config-nbm-flow-policy)# show nbm flows bandwidth`	（任意） フローごとに、設定および適用されている NBM 帯域幅を表示します。

次の例は、設定サンプルを示しています。

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

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。

show nbm controller	DCNM メディア コントローラの状態を表示します。
show nbm flows [**active** [**interface***type slot/port*] | **all** [**interface***type slot/port*] | **detail** [**interface***type slot/port*] | **group***multicast-group* | **group-based** [**interface***type slot/port*] | **inactive** [**interface***type slot/port*] | **interface***type slot/port* | **m-group***multicast-group* | **no-receiver** [**interface***type slot/port*] |**source***ip-address*]	NBM フローを表示します。
show nbm flows bandwidth	フローごとに、設定および適用されている NBM 帯域幅を表示します。 （注） このコマンドは、N9K-X9636C-R および N9K-X9636Q-R ライン カードを備えた Cisco Nexus 9508 スイッチでは、サポートされていません。
show nbm flows statistics	NBM フローの統計情報を表示します。 （注） このコマンドは、スパイン リーフ トポロジにおけるスパイン スイッチと、Cisco NX-OS リリース 7.0(3)F2(1) を実行するシングル モジュラ型スイッチでは、サポートされていません。

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。

show コマンドの出力例

この項では、DCNM メディア コントローラ不使用のシングル モジュラ型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、統計情報は、DCNM メディア コントローラ GUI で表示できます。

Cisco NX-OS 7.0(3)F2(1) 以降を実行するスイッチでの出力例

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 :
Start-Time         Src-Intf  Mcast-Group   Src-IP      LID   Status  Num Rx  Bw Mbps  CFG
Bw Mbps  Src-slot  Unit  Slice
04/27 05:32:01.536 Eth3/13/1 230.13.2.244  210.1.1.2   1070  ACTIVE  1       3000.000
3000.000     3         1     0
04/27 05:32:01.535 Eth3/13/1 230.13.2.243  210.1.1.2   582   ACTIVE  1       3000.000
3000.000     3         1     0
04/27 05:32:01.535 Eth3/13/1 230.13.2.242  210.1.1.2   1298  ACTIVE  1       3000.000
3000.000     3         1     0
04/27 05:32:01.534 Eth3/13/1 230.13.2.241  210.1.1.2   1407  ACTIVE  1       3000.000
3000.000     3         1     0
```

次に、**show nbm flows group***multicast-group* コマンドの出力例を示します。

```
switch# show nbm flows group 230.13.2.244
NBM Active Source-Group-Based Flows :
Start-Time         Src-Intf  Mcast-Group   Src-IP     LID   Status  Num Rx  Bw Mbps  CFG
Bw Mbps  Src-slot  Unit  Slice
04/27 05:32:01.536 Eth3/13/1 230.13.2.244  210.1.1.2  1070  ACTIVE  1      3000.000 3000.000
     3         1     0
```

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" - 500 total entries
Type: S - Static, D - Dynamic, L - Local, T - SSM Translated
Group Address      Type  Interface           Uptime    Expires   Last Reporter
230.13.2.241         D   Ethernet4/25/1      00:08:16  00:02:54  210.13.1.2
230.13.2.242         D   Ethernet4/25/1      00:08:16  00:02:58  210.13.1.2
230.13.2.243         D   Ethernet4/25/1      00:08:16  00:02:56  210.13.1.2
230.13.2.244         D   Ethernet4/25/1      00:08:16  00:02:54  210.13.1.2
```

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 eth4/25/1
IGMP Connected Group Membership for Interface "Eth4/25/1" - 500 total entries
Type: S - Static, D - Dynamic, L - Local, T - SSM Translated
Group Address      Type  Interface         Uptime    Expires   Last Reporter
230.13.2.241         D   Ethernet4/25/1    00:08:16  00:02:54  210.13.1.2
230.13.2.242         D   Ethernet4/25/1    00:08:16  00:02:58  210.13.1.2
230.13.2.243         D   Ethernet4/25/1    00:08:16  00:02:56  210.13.1.2
230.13.2.244         D   Ethernet4/25/1    00:08:16  00:02:54  210.13.1.2
```

次に、**show ip igmp groups***multicast-group* コマンドの出力例を示します。

```
switch# show ip igmp groups 230.13.2.244
IGMP Connected Group Membership for VRF "default" - matching  Group "230.13.2.244"
Type: S - Static, D - Dynamic, L - Local, T - SSM Translated
Group Address      Type Interface           Uptime    Expires   Last Reporter
230.13.2.244       D    Ethernet4/25/1      00:09:09  00:03:55  210.13.1.2
```

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
!Time: Thu Apr 27 05:39:23 2017

version 7.0(3)F2(1)
feature nbm
```

Cisco NX-OS 7.0(3)I6(1) 以降を実行するスイッチでの出力例

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 :

Flags: * - Flows are not truely in Guaranteed mode as one of the FM is down
NBM Active Source-Group-Based Flows :
Start-Time         Src-Intf Mcast-Group  Src-IP   L4-S  L4-D  LID   Status  Num Rx  Bw Mbps
  CFG Bw Mbps  Src-slot  Unit  Slice
05/06 11:24:03.117 Eth5/5   225.3.5.1    5.5.1.2  0     0     840   ACTIVE  1       55.000
   55.000       8         2     0
05/06 11:24:03.094 Eth5/5   225.3.5.2    5.5.1.2  0     0     196   ACTIVE  1       55.000
   55.000       8         2     0
05/06 11:24:03.092 Eth5/5   225.3.5.3    5.5.1.2  0     0     641   ACTIVE  1       55.000
   55.000       8         2     0
05/06 11:24:03.088 Eth5/5   225.3.5.4    5.5.1.2  0     0     529   ACTIVE  1       55.000
   55.000       8         2     0
```

次に、**show nbm flows group***multicast-group* コマンドの出力例を示します。

```
switch# show nbm flows group 225.3.5.1
NBM Active Source-Group-Based Flows :
Start-Time         Src-Intf  Mcast-Group  Src-IP    L4-S  L4-D  LID   Status  Num Rx  Bw
Mbps  CFG Bw Mbps  Src-slot  Unit  Slice
05/06 11:25:15.142 Eth5/5    225.3.5.1    5.5.1.2   0     0     840   ACTIVE  1       55.000
    55.000        8         2     0
```

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"
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
!Time: Sat May  6 23:10:33 2017

version 7.0(3)I6(1)
feature nbm

nbm flow bandwidth 55
nbm mode flow
  policy 0mbps
    bandwidth 2
    ip group 225.3.5.1
    ip group-range 225.3.5.2 to 225.3.5.255
  policy 3000
    bandwidth 130
    ip group-range 228.255.255.1 to 228.255.255.255
```

ファブリックインターフェイスとホストインターフェイスの設定

ファブリックおよびホストのインターフェイスを設定するには、この項の CLI コマンドを使用します。または、DCNM メディア コントローラを使用すると、これらの設定をすべて自動で設定することができます。

ファブリック インターフェイスの設定

各リーフ スイッチに、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 スイッチへのインターフェイスです。

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. **ip pim passive**
7. **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 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	**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	**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	**ip pim passive** 例： `switch(config-if)# ip pim passive`	スイッチに対し、このインターフェイス上で PIM メッセージを送信することと、このインターフェイス経由で他のスイッチから PIM メッセージを受信することを禁止します。このコマンドが必要なのは、フローへのエンドツーエンドでの静的なプロビジョニングを（PIM プロトコルではなく）DCNM メディア コントローラが行っているためです。
ステップ 7	**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。

ホスト インターフェイスの設定

各リーフ スイッチに、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へのインターフェイスです。

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. **ip pim passive**
7. **ip igmp immediate-leave**
8. **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 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	**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	**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 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。

	コマンドまたはアクション	目的
ステップ 6	**ip pim passive** 例： `switch(config-if)# ip pim passive`	スイッチに対し、このインターフェイス上でPIMメッセージを送信することと、このインターフェイス経由で他のスイッチからPIMメッセージを受信することを禁止します。このコマンドが必要なのは、フローへのエンドツーエンドでの静的なプロビジョニングを（PIM プロトコルではなく）DCNMメディアコントローラが行っているためです。
ステップ 7	**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。
ステップ 8	**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。

メディアに向けた PTP の設定（任意）

Cisco IP Fabric for Media ソリューションは、次の IEEE 1588 PTP プロファイルをサポートしています。

- Audio Engineering Society 67 プロファイル（AES67）：IP ベースの高パフォーマンス音声ストリーミング向け
- Professional Broadcast Environment プロファイル（SMPTE-2059-2）：IP ベースの高パフォーマンス ビデオ ストリーミング向け

ソリューションでは、マルチキャスト同期およびアナウンス メッセージのほか、ユニキャスト遅延要求/応答メッセージも備えた混合モードの PTP サポートも導入しています。

PTP をメディアに向けて設定するには、これらのプロファイルのいずれかを使用する必要があります。

（注） メディアに向けたPTP設定は、メディア ネットワーク以外に向けたPTP設定とは異なります。ただし、PTP の詳細については、『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』の参照が可能です。

はじめる前に

PTP 境界モード機能をスイッチ上でイネーブルにします。PTP パケットをファブリック内で通常のマルチキャスト パケットとしてルーティングすることはできません。

手順の概要

1. **configure terminal**
2. [**no**] **feature ptp**
3. [**no**] **ptp source***ip-address* [**vrf***vrf*]
4. （任意） [**no**] **ptp offload**
5. **interface ethernet***slot/port*
6. [**no**] **ptp**
7. （任意） [**no**] **ptp announce interval** [**aes67** | **smpte-2059**] *log-seconds*
8. （任意） [**no**] **ptp announce timeout** [**aes67** | **smpte-2059**] *count*
9. （任意） [**no**] **ptp delay-request minimum interval** [**aes67** | **smpte-2059**] *log-seconds*
10. （任意） [**no**] **ptp sync interval** [**aes67** | **smpte-2059**] *log-seconds*
11. （任意） [**no**] **ptp vlan***vlan-id*
12. （任意） **show ptp brief**
13. （任意） **show ptp port interface***interface slot/port*
14. （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	[**no**] **feature ptp** 例： `switch(config)# feature ptp`	デバイス上で PTP をイネーブルまたはディセーブルにします。 （注） スイッチの PTP をイネーブルにしても、各インターフェイスの PTP はイネーブルになりません。
ステップ 3	[**no**] **ptp source***ip-address* [**vrf***vrf*] 例： `switch(config)# ptp source 10.10.10.1`	すべての PTP パケットの送信元 IPv4 アドレスを設定します。
ステップ 4	[**no**] **ptp offload** 例： `switch(config)# ptp offload`	（任意） いくつかのタイマーをライン カードにオフロードすることにより、PTP セッションの数を増やします。

	コマンドまたはアクション	目的
		（注） このコマンドは、Cisco NX-OS リリース 7.0(3)I6(1) 以降、X9700-EX ライン カードを備えた Cisco Nexus 9500 シリーズ スイッチでのみサポートされています。

ステップ 5	**interface ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		PTP をイネーブル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 6	[**no**] **ptp** 例： `switch(config-if)# ptp`	インターフェイスで PTP をイネーブルまたはディセーブルにします。
ステップ 7	[**no**] **ptp announce interval** [**aes67** | **smpte-2059**] *log-seconds* 例： `switch(config-if)# ptp announce interval aes67 3`	（任意） インターフェイス上の PTP アナウンス メッセージの送信間隔を設定します。 **表 *4*：*PTP* アナウンスメントの送信間隔範囲とデフォルト値** **オプション** / **範囲** / **デフォルト値** **aes67** / 0 ～ 4 ログ秒 / 1 ログ秒 **smpte-2059** / -3 ～ 1 ログ秒 / 1 ログ秒 **aes67** または **smpte-2059** オプションなし / 0 ～ 4 ログ秒 / 1 ログ秒
ステップ 8	[**no**] **ptp announce timeout** [**aes67** | **smpte-2059**] *count* 例： `switch(config-if)# ptp announce timeout aes67 2`	（任意） インターフェイス上でタイムアウトが発生するまでの PTP 間隔の数を設定します。 **表 *5*：*PTP* アナウンスメントのタイムアウト範囲とデフォルト値** **オプション** / **範囲** / **デフォルト値** **aes67** / 2 ～ 10 間隔 / 3 間隔 **smpte-2059** / 2 ～ 10 間隔 / 3 間隔

	コマンドまたはアクション	目的
		オプション / **範囲** / **デフォルト値** **aes67** または **smpte-2059** オプションなし / 2 ～ 4 間隔 / 3 間隔
ステップ 9	[**no**] **ptp delay-request minimum interval** [**aes67** | **smpte-2059**] *log-seconds* 例： `switch(config-if)# ptp delay-request minimum interval aes67 -1`	（任意） ポートがマスターステートの場合にPTP遅延メッセージ間で許可される最小間隔を設定します。 **表 *6*：*PTP* 遅延要求の最小間隔範囲とデフォルト値** **オプション** / **範囲** / **デフォルト値** **aes67** / -4 ～ 5 ログ秒 / 0 ログ秒 **smpte-2059** / -4 ～ 5 ログ秒 / 0 ログ秒 **aes67** または **smpte-2059** オプションなし / –1 ～ 6 ログ秒（ここで、–1 = 1 フレーム毎秒） / 0 ログ秒
ステップ 10	[**no**] **ptp sync interval** [**aes67** | **smpte-2059**] *log-seconds* 例： `switch(config-if)# ptp sync interval aes67 1`	（任意） インターフェイス上の PTP 同期メッセージの送信間隔を設定します。 **表 *7*：*PTP* 同期の間隔範囲とデフォルト値** **オプション** / **範囲** / **デフォルト値** **aes67** / -4 ～ 1 ログ秒 / -2 ログ秒 **smpte-2059** / -4 ～ -1 ログ秒 / -2 ログ秒 **aes67** または **smpte-2059** オプションなし / -3 ～ 1 ログ秒 / -2 ログ秒

	コマンドまたはアクション	目的
ステップ 11	[**no**] **ptp vlan***vlan-id* 例： `switch(config-if)# ptp vlan 1`	（任意） PTP をイネーブルにするインターフェイスの VLAN を指定します。インターフェイス上の 1 つの VLAN でイネーブルにできるのは、1 つの PTP のみです。 指定できる範囲は 1 ～ 4094 です。
ステップ 12	**show ptp brief** 例： `switch(config-if)# show ptp brief`	（任意） PTP のステータスを表示します。
ステップ 13	**show ptp port interface***interface slot/port* 例： `switch(config-if)# show ptp port interface ethernet 2/1`	（任意） PTP ポートのステータスを表示します。
ステップ 14	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 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。

ユニキャスト PTP ピアの設定

マスターおよびスレーブ両方の 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 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	**interface ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		ユニキャスト PTP をイネーブル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の ユニキャスト PTP 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	**show ptp brief** 例： `switch(config-if)# show ptp brief`	（任意） PTP のステータスを表示します。
ステップ 7	**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`	（任意） ユニキャスト PTP カウンタを表示します。
ステップ 8	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 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。

次の例は、マスターおよびスレーブの PTP ピアの設定方法を示します。

```
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
---------------------------------------------------------------------
```

第 5 章

メディア コントローラ

このセクションでは、DCNM メディア コントローラについて説明します。

（注） この機能は、Cisco DCNM OVA/ISO のインストールの完了後、メディア コントローラの機能を明示的にイネーブルにしたときにのみ使用できます。詳細については、『*Cisco DCNM Installation Guide*』を参照してください。

メディア コントローラ機能をイネーブルにするには、SSH 経由で DCNM OVA/ISO にログオンし、**appmgr set-mode media-controller** コマンドを使用します。**appmgr set-mode media-controller** コマンドを実行する前には必ず、**appmgr stop dcnm** コマンドを使用して DCNM アプリケーションを停止させてください。

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 DCNM の [Web Client] > [Configure] > [Deploy] > [POAP Definitions] を通じて POAP 定義をパブリッシュする必要があります。詳細については、「POAP 起動パッド」の項を参照してください。

（注） メディア コントローラ展開のためのリーフおよびスパインに向けた個別の POAP テンプレートは、Cisco DCNM ソフトウェアにパッケージされています。

Cisco DCNM サーバを **appmgr set-mode media-controller** コマンドを使用してメディア コントローラ モードに設定し、「POAP 起動パッド」の項に記載する手順を実行している場合は、メディア コントローラのテンプレートを表示することができます。Cisco DCNM Web クライアントでは、必要なテンプレートを選択し、それらを必要に応じて編集することで、POAP 定義をパブリッシュすることができます。

メディア コントローラ API の詳細については、Cisco DevNet の『Cisco DCNM Media Controller API reference』を参照してください。

- メディア コントローラのトポロジ，40 ページ
- PMN ホスト，41 ページ
- フロー エイリアス，44 ページ

- ポリシー，47 ページ
- フローの状態，55 ページ
- Event，58 ページ

メディア コントローラのトポロジ

メディア コントローラのトポロジは、[Web Client] > [Media Controller] > [Topology] ページで表示できます。このトポロジは、メディア コントローラに特有です。

（注） この機能が使用可能なのは、インストール処理時に、DCNM メディア コントローラ設定の一部として、Cisco DCNM サーバ上で **appmgr set-mode media-controller** コマンドを使用し、メディアコントローラをイネーブルにしている場合のみです。

クイック検索

検索文字列を入力すると、関連デバイスが強調表示されます。

検索には、条件として次のフィールドが使用できます。[switch or hostname]、[switch or host IP address]、[switch MAC]、および [switch serial number]。

マルチキャスト グループ

フィールド上で右クリックします（またはリターンキーを押します）。マルチキャストアドレスのリストが表示されます。トポロジの表示が必要なマルチキャスト IP アドレスを選択できます。

そのマルチキャスト IP アドレスのデバイスと、スパインおよびリーフへのリンクが強調表示されます。動く点線は、メディア コントローラのトポロジにおけるトラフィックの流れを表します。

フロー エイリアス名により、トポロジ内の検索またはフィルタリングができます。マルチキャスト グループを検索するときは、IP アドレスまたはフロー エイリアス名が使用できます。

[Show Panel] > [Bandwidth]

[Bandwidth] チェックボックスをオンにすると、スパインおよびリーフによって消費されている帯域幅が色で表示されます。

- 緑：40 % 未満
- 黄色：40 ～ 80 %
- 赤：80 % 超

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、リーフとスパインとの間に ISL リンクが設定されます。ISL リンクにより、Cisco DCNM は、フローのスティッチングに必要な帯域幅を計算す

ることができます。設定に問題があると、Cisco DCNM Bandwidth Manager によって誤ったリンクが特定されることがあります。

Cisco DCNM の帯域幅計算アルゴリズムは、送信者と受信者間で共通するノードの検出を試行します。

ホスト側リンクでの帯域幅トラッキング

送信者と受信者は、PMNファブリックのリーフスイッチに接続できます。送信者はマルチキャストフローを開始し、受信者は、そのマルチキャストフローを受信します。マルチキャストが使用されているため、1 つのフローを複数の受信者が受信することができます。送信者は、カメラ、マイク、再生デバイスなどのデバイスです。受信者は、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。

（注） ホスト ポートの帯域幅のトラッキングは、[Web Client] > [Administration] > [DCNM Server] > [Server Properties] ページの [pmn.host.port.policing.enabled] フィールドでイネーブルまたはディセーブルにできます。デフォルトでは、ホスト ポートの帯域幅トラッキングはディセーブルになっています。

ホスト側の帯域幅をトラッキングすることができます。この機能を使用して、DCNM は、ホスト側のリンクで使用可能な帯域幅を超えて、受信者がフローを要求したり、送信者がフローを送信したりすることを防ぎます。

PMN ホスト

Cisco DCNM では、メディア コントローラのホストを作成することができます。送信および受信を行うアクティブなデバイスは、ホストと呼ばれます。ホストは、[Cisco Web Client] > [Media Controller] > [Hosts] で設定できます。

（注） [PMN Hosts] テーブルは、トラフィックが開始すると、自動的に入力されます。

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 *8*：*PMN* ホストに対する操作

フィールド	説明
Add	新規ホストを追加できます。
Edit	選択されたホスト パラメータの表示または編集ができます。
Delete	ファブリックからホストを削除できます。

フィールド	説明
Import	ローカル ディレクトリからホスト パラメータをインポートできます。
Export	ローカル ディレクトリにホスト パラメータをエクスポートできます。 エクスポートされるファイルは、*.csv* 形式です。

表 *9*：*PMN* ホスト テーブルのフィールドと説明

フィールド	説明
Hostname	ホストデバイスに設定されている名前を指定します。
IP Address	ホストの IP アドレスを指定します。
MAC Address	ホスト スイッチの MAC アドレスを指定します。
Switch Name	スイッチの名前を指定します。
Interface Name	ホストが関連付けられているスイッチインターフェイスの名前を指定します。

この項の構成は、次のとおりです。

PMN ホストの追加

ホストを追加するには、次の手順を実行します。

ステップ 1 メニュー バーから、[Media Controller] > [Hosts] の順に選択します。

ステップ 2 [Add] ホスト アイコンをクリックします。

ステップ 3 [Add Hosts] ウィンドウで、次のフィールドのパラメータを指定します。

- Name：ホスト デバイスの一意の名前を指定します。
- IP Address：ホスト デバイスの IP アドレスを指定します。
- （任意）MAC Address：ホスト デバイスの MAC アドレスを指定します。

ステップ 4 [Save] をクリックしてホストを設定します。

PMN ホストの編集

ホスト パラメータを編集または表示するには、次の手順を実行します。

ステップ 1 メニュー バーから、[Media Controller] > [Hosts] の順に選択します。

ステップ 2 編集が必要なホスト名の隣のチェックボックスをオンにします。

ステップ 3 [Edit] ホスト アイコンをクリックします。

ステップ 4 [Edit Hosts] ウィンドウで、[Name] フィールドおよび [MAC Address] フィールドのパラメータを編集します。

ステップ 5 [Save] をクリックして変更を保存します。ホストのパラメータを元に戻すには、[Cancel] をクリックします。

PMN ホストの削除

ホストを削除するには、次の手順を実行します。

ステップ 1 メニュー バーから、[Media Controller] > [Hosts] の順に選択します。

ステップ 2 削除が必要なホスト名の隣のチェックボックスをオンにします。
削除対象のホストは、複数選択できます。

ステップ 3 [Delete] ホスト アイコンをクリックします。

ステップ 4 削除の通知で [Yes] をクリックし、ホストを削除します。このアクションをキャンセルするには、[No] をクリックします。
ホスト削除成功のメッセージがページの下部に表示されます。

PMN ホストのインポート

ホストをインポートするには、次の手順を実行します。

ステップ 1 メニュー バーから、[Media Controller] > [Hosts] の順に選択します。

ステップ 2 [Import] ホスト 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、ホスト設定情報を含むファイルを選択します。

ステップ 4 [Open] をクリックします。
ホスト設定は、Cisco DCNM Web クライアントの [Media Controller] > [Hosts] にインポートされ、表示されます。

PMN ホストのエクスポート

ホストをエクスポートするには、次の手順を実行します。

ステップ 1 メニュー バーから、[Media Controller] > [Hosts] の順に選択します。

ステップ 2 [Export] ホスト 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 自分のディレクトリ上で、ホスト設定ファイルを保存する場所を選択します。

ステップ 4 [OK] をクリックします。
ホスト設定ファイルは、ローカルディレクトリにエクスポートされます。ファイル名の後ろには、ファイルがエクスポートされた日付が付きます。エクスポートされるファイルの形式は、*.csv* です。

フロー エイリアス

フロー エイリアス機能を使用すると、マルチキャスト グループの名前を指定することができます。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、その名前に基づいてポリシーを検索および追加できるようになります。

フロー エイリアスの設定は、[Cisco Web Client] > [Media Controller] > [Flow Alias] で行えます。

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 *10* : *[Flow Alias]* テーブルのフィールドと説明

フィールド	説明
Flow Alias	フロー エイリアスの名前を指定します。
Multicast IP Address	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。
Description	フロー エイリアスに追加されている説明。
Last Updated at	フローエイリアスが最後に更新された日付を指定します。

この項の構成は、次のとおりです。

フロー エイリアスの追加

フロー エイリアスを追加するには、次の手順を実行します。

ステップ 1 メニュー バーから、[Media Controller] >[Flow Alias] の順に選択します。

ステップ 2 [Add] フロー エイリアス アイコンをクリックします。

ステップ 3 [Add Flow Alias] ウィンドウで、次のフィールドのパラメータを指定します。

- Flow Name：一意のフロー エイリアス名を指定します。
- Multicast IP Address：フロー エイリアスにマルチキャスト IP アドレスを指定します。
- Description：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 [Save] をクリックしてフロー エイリアスを保存します。

フロー エイリアスの編集

フロー エイリアスを編集するには、次の手順を実行します。

ステップ 1 メニュー バーから、[Media Controller] >[Flow Alias] の順に選択します。

ステップ 2 編集が必要なフロー エイリアス名の隣のチェックボックスをオンにします。

ステップ 3 [Edit] フロー エイリアス アイコンをクリックします。

ステップ 4 [Edit Flow Alias] ウィンドウで、[Name] フィールド、[Multicast IP] フィールド、および [Description] フィールドを編集します。

ステップ 5 [Save] をクリックして新しい設定を保存します。

フロー エイリアスの削除

フロー エイリアスを削除するには、次の手順を実行します。

ステップ 1 メニュー バーから、[Media Controller] >[Flow Alias] の順に選択します。

ステップ 2 削除が必要なフロー エイリアスの隣のチェックボックスをオンにします。
削除対象のフロー エイリアスは、複数選択できます。

ステップ 3 [Delete] フロー エイリアス 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

ホスト エイリアスをエクスポートするには、次の手順を実行します。

ステップ 1 メニュー バーから、[Media Controller] >[Flow Alias] の順に選択します。

ステップ 2 [Export] フロー エイリアス 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 自分のディレクトリ上で、エイリアス詳細ファイルを保存する場所を選択します。

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は、ローカルディレクトリにエクスポートされます。ファイル名の後ろには、ファイルがエクスポートされた日付が付きます。エクスポートされるファイルの形式は、*.csv* です。

フロー エイリアスのインポート

フロー エイリアスをインポートするには、次の手順を実行します。

ステップ 1 メニュー バーから、[Media Controller] >[Flow Alias] の順に選択します。

ステップ 2 [Import] フロー エイリアス 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 [Open] をクリックします。
フロー エイリアス設定は、Cisco DCNM Web クライアントの [Media Controller] > [Flow Alias] にインポートされ、表示されます。

ポリシー

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。ホスト ポリシーは、[Cisco Web Client] > [Media Controller] > [Policies] > [Host Policies] で設定できます。

（注） デフォルト以外のホスト ポリシーは、既知のホストに対してのみ作成できます。

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 *11*：ホスト ポリシーの操作

フィールド	説明
Add	新規ホスト ポリシーを追加できます。
Edit	選択されたホスト ポリシー パラメータの表示または編集ができます。

フィールド	説明
Delete	ユーザ定義のホスト ポリシーを削除できます。 （注） デフォルトのポリシーは、すでにデバイスに適用されている場合、編集できません。
Import	自分のディレクトリからホスト ポリシーをインポートできます。
Export	ローカル ディレクトリにホスト ポリシーをエクスポートできます。

表 *12* : 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
Policy Name	ホストのポリシー名を指定します。 デフォルトでは、デフォルトのホスト ポリシーの [Operation] は [permit] に設定されています。
Host	ホスト ID を指定します。
Multicast IP	ホストのマルチキャスト IP アドレスを指定します。
Host Acting As	ホスト デバイスの役割を指定します。ホスト デバイスの役割は、次のいずれかです。 • Sender • Receiver
Operation	ホスト ポリシーの動作を指定します。ポリシーには、次の動作があります。 • Permit • Deny
Devices Applied To	このポリシーが適用されているデバイスの数を指定します。
Last Updated	ホスト ポリシーが最後に更新された日付と時刻を指定します。 形式は、曜日 *MMM DD YYYY HH:MM:SS* タイムゾーンです。

この項の構成は、次のとおりです。

ホスト ポリシーの追加

ホスト ポリシーを追加するには、次の手順を実行します。

手順の概要

1. メニュー バーから、[Media Controller] > [Policies] > [Host Policies] の順に選択します。
2. [Add] ホスト ポリシー アイコンをクリックします。
3. [Add Host Policy] ウィンドウで、次のフィールドのパラメータを指定します。
4. [Save] をクリックしてホスト ポリシーを設定します。

手順の詳細

ステップ 1 メニュー バーから、[Media Controller] > [Policies] > [Host Policies] の順に選択します。

ステップ 2 [Add] ホスト ポリシー アイコンをクリックします。

ステップ 3 [Add Host Policy] ウィンドウで、次のフィールドのパラメータを指定します。

- Policy Name：フロー ポリシーに一意のポリシー名を指定します。
- Host：ポリシーを適用するホストを指定します。 値は、ドロップダウン リストから選択できます。
- Multicast IP：フロー ポリシーにマルチキャスト IP アドレスを指定します。
- Acting As：ホスト ポリシーが [Sender] または [Receiver] いずれの役割を果たすかを指定します。必要な値はドロップダウン リストから選択できます。
- Allow/Deny：ラジオ ボタンから [Allow] または [Deny] のいずれかをクリックし、ポリシーはトラフィック フローの許可または拒否のいずれを行う必要があるか選択します。

ステップ 4 [Save] をクリックしてホスト ポリシーを設定します。

ホスト ポリシーの編集

ホスト ポリシーを追加するには、次の手順を実行します。

ステップ 1 メニュー バーから、[Media Controller] > [Policies] > [Host Policies] の順に選択します。

ステップ 2 編集が必要なホスト ポリシー名の隣のチェックボックスをオンにします。

ステップ 3 [Edit] ホスト ポリシー アイコンをクリックします。

ステップ 4 [Edit Host Policy] ウィンドウで、ポリシーはトラフィックに対して [Allow] または [Deny] いずれの動作を行うか指定する編集をします。

（注） ホスト ポリシーに加えた変更は、ただちに適用されます。ポリシーがいずれかのデバイスにすでに適用されている場合、その変更は、既存のフローに影響する可能性があります。

ステップ 5 [Save] をクリックして新しい設定を保存します。

ホスト ポリシーの削除

ホスト ポリシーを削除するには、次の手順を実行します。

（注） 削除できるのは、ユーザ定義のホスト ポリシーだけです。

ステップ 1 メニュー バーから、[Media Controller] > [Policies] > [Host Policies] の順に選択します。

ステップ 2 削除が必要なホスト ポリシー名の隣のチェックボックスをオンにします。
削除対象のホスト ポリシーは、複数選択できます。

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

ステップ 4 削除の通知で [OK] をクリックし、ホスト ポリシーを削除します。[Policy Policies] ページに戻るには、[Cancel] をクリックします。

（注） ホスト ポリシーを削除すると、そのポリシーが適用されていたリーフにポリシーの適用が行われます。

ホスト ポリシー削除成功のメッセージがページの下部に表示されます。

ホスト ポリシーのインポート

ホスト ポリシーをインポートするには、次の手順を実行します。

ステップ 1 メニュー バーから、[Media Controller] > [Policies] > [Host Policies] の順に選択します。

ステップ 2 [Import] ホスト 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、ホスト 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 [Open] をクリックします。
ホスト ポリシー設定は、Cisco DCNM Web クライアントの [Media Controller] > [Hosts] > [Host Policies] にインポートされ、表示されます。

ホスト ポリシーのエクスポート

ホスト ポリシーをエクスポートするには、次の手順を実行します。

ステップ 1 メニュー バーから、[Media Controller] > [Policies] > [Host Policies] の順に選択します。

ステップ 2 [Export] ホスト ポリシー 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 自分のディレクトリ上で、ホスト ポリシー詳細ファイルを保存する場所を選択します。

ステップ 4 [OK] をクリックします。
ホスト ポリシー ファイルは、ローカル ディレクトリにエクスポートされます。ファイル名の後ろには、ファイルがエクスポートされた日付が付きます。エクスポートされるファイルの形式は、*.csv* です。

フロー ポリシー

フロー ポリシーの設定は、[Cisco Web Client] > [Media Controller] > [Policies] > [Flow Policies] で行えます。

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 *13* : フロー ポリシーの操作

フィールド	説明
Add	新規フロー ポリシーを追加できます。

フィールド	説明
Edit	選択されたフロー ポリシー パラメータの表示または編集ができます。
Delete	ユーザ定義のフローポリシーを削除できます。
Import	自分のディレクトリからフローポリシーをインポートできます。
Export	ローカル ディレクトリにフロー ポリシーをエクスポートできます。

表 *14*：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
Policy Name	フロー ポリシー名を指定します。 デフォルトでは、デフォルトのホストポリシーの [Operation] は [permit] に設定されています。
Multicast IP	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。
Bandwidth	トラフィックに割り当てられている帯域幅を指定します。
QoS/DSCP	スイッチ定義の QoS ポリシーを指定します。
Last Updated	ホストポリシーが最後に更新された日付と時刻を指定します。 形式は、曜日 *MMM DD YYYY HH:MM:SS* タイムゾーンです。

（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。
- 新しいポリシーは追加または編集済みで、そのフロー ポリシーと一致するフローが期限切れとなって再形成される場合。

この項の構成は、次のとおりです。

フロー ポリシーの追加

フロー ポリシーを追加するには、次の手順を実行します。

ステップ 1 メニュー バーから、[Media Controller] > [Policies] > [Flow Policies] の順に選択します。

ステップ 2 [Add] フロー ポリシー アイコンをクリックします。

ステップ 3 [Add Flow Policy] ウィンドウで、次のフィールドのパラメータを指定します。

- Policy Name：フロー ポリシーに一意のポリシー名を指定します。
- Multicast IP：フロー ポリシーにマルチキャスト IP アドレスを指定します。
- Bandwidth：フロー ポリシーに割り当てる帯域幅を指定します。ラジオ ボタンから、[Gbps] または [Mbps] のいずれかを選択します。

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 [Save] をクリックしてフロー ポリシーを設定します。

フロー ポリシーの編集

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. メニュー バーから、[Media Controller] > [Policies] > [Flow Policies] の順に選択します。
2. 編集が必要なフロー ポリシー名の隣のチェックボックスをオンにします。
3. [Edit] フロー ポリシー アイコンをクリックします。
4. [Edit Flow Policy] ウィンドウで、[Multicast IP] フィールド、[Bandwidth] フィールド、および [QoS/DSCP] フィールドを編集します。
5. [Save] をクリックして新しい設定を保存します。

手順の詳細

ステップ 1 メニュー バーから、[Media Controller] > [Policies] > [Flow Policies] の順に選択します。
ステップ 2 編集が必要なフロー ポリシー名の隣のチェックボックスをオンにします。
ステップ 3 [Edit] フロー ポリシー アイコンをクリックします。
ステップ 4 [Edit Flow Policy] ウィンドウで、[Multicast IP] フィールド、[Bandwidth] フィールド、および [QoS/DSCP] フィールドを編集します。
ステップ 5 [Save] をクリックして新しい設定を保存します。

フロー ポリシーの削除

フロー ポリシーを削除するには、次の手順を実行します。

ステップ 1 メニュー バーから、[Media Controller] > [Policies] > [Flow Policies] の順に選択します。
ステップ 2 削除が必要なフロー ポリシー名の隣のチェックボックスをオンにします。
削除対象のフロー ポリシーは、複数選択できます。
ステップ 3 [Delete] フロー ポリシー アイコンをクリックします。
フロー ポリシーが削除されます。

フロー ポリシーのインポート

フロー ポリシーをインポートするには、次の手順を実行します。

手順の概要

1. メニュー バーから、[Media Controller] > [Policies] > [Flow Policies] の順に選択します。
2. [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. [Open] をクリックします。

手順の詳細

ステップ 1 メニュー バーから、[Media Controller] > [Policies] > [Flow Policies] の順に選択します。

ステップ 2 [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 [Open] をクリックします。
フロー ポリシー設定は、Cisco DCNM Web クライアントの [Media Controller] > [Hosts] > [Flow Policies] にインポートされ、表示されます。

フロー ポリシーのエクスポート

ホスト ポリシーをエクスポートするには、次の手順を実行します。

ステップ 1 メニュー バーから、[Media Controller] > [Policies] > [Flow Policies] の順に選択します。

ステップ 2 [Export] フロー ポリシー 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 自分のディレクトリ上で、フロー ポリシー詳細ファイルを保存する場所を選択します。

ステップ 4 [OK] をクリックします。
フロー ポリシー ファイルは、ローカル ディレクトリにエクスポートされます。ファイル名の後ろには、ファイルがエクスポートされた日付が付きます。エクスポートされるファイルの形式は、`.csv` です。

フローの状態

Cisco DCNM では、フローの状態を図や統計情報で表示することができます。フローの状態は、[Cisco Web Client] > [Media Controller] > [Flow Status] で確認できます。

（注） フローの状態の収集頻度とキャッシュ サイズは、[Web Client] > [Administration] > [DCNM Server] > [Server Properties] ページで、それぞれ cisco.pmn-stats-interval コマンドおよび cisco.pmn-stats-cache-size コマンドを使用して確認できます。

次の表で、[Flow Status] タブに表示されるフィールドを説明します。

表 *15* : *[Flow Status]* タブ

フィールド	説明
Multicast IP	フローのマルチキャスト IP アドレスを指定します。 （注） マルチキャスト IP アドレスの隣のウェーブ リンクをクリックすると、フローの統計情報が図で表示されます。
Flow Alias	フロー エイリアスの名前を指定します。
Sender	送信者 ID を指定します。
Receiver	
Bandwidth	トラフィックに割り当てられている帯域幅を指定します。
QoS/DSCP	スイッチ定義の QoS ポリシーを指定します。
Flow Link State	（注） [READY] リンク状態をクリックすると、送信者と受信者のネットワーク図が表示されます。 表示される点線は、トラフィックが流れる方向を示します。
Policy ID	マルチキャスト IP に適用されているポリシー ID を指定します。
Receiver Start Time	受信者がデータの受信を開始した時刻を表示します。

次の表で、[Sender Only] タブに表示されるフィールドを説明します。

表 *16* : *[Sender Only]* タブ

フィールド	説明
Multicast IP	フローのマルチキャスト IP アドレスを指定します。
Flow Alias	フロー エイリアスの名前を指定します。
Name	送信者 ID を指定します。

フィールド	説明
Sender Leaf IP	マルチキャスト フローを開始する送信者の IP アドレスを指定します。
Sender Leaf Name	送信者リーフの名前を指定します。
Sender Ingress Interface	送信者の入力インターフェイスの名前を指定します。
Policy ID	マルチキャスト IP に適用されているポリシー ID を指定します。
Bandwidth	トラフィックに割り当てられている帯域幅を指定します。
State	フロー リンクの状態を指定します。

次の表で、[Receiver Only] タブに表示されるフィールドを説明します。

表 *17*：*[Receiver Only]* タブ

フィールド	説明
Multicast IP	フローのマルチキャスト IP アドレスを指定します。
Flow Alias	フロー エイリアスの名前を指定します。
Name	送信者 ID を指定します。
Receiver Leaf IP	マルチキャスト フローを受信する受信者の IP アドレスを指定します。
Receiver Interface	送信者インターフェイスの名前を指定します。
Receiver Leaf Name	受信者リーフの名前を指定します。
Policy ID	マルチキャスト IP に適用されているポリシー ID を指定します。
Bandwidth	トラフィックに割り当てられている帯域幅を指定します。
Number of Receivers	トラフィックに割り当てられている受信者の数を指定します。

フィールド	説明
State	フロー リンクの状態を指定します。

統計情報表示エリアの [Show] ドロップダウン リストをクリックすると、統計情報がさまざまな形式で表示されます。

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 DCNM では、フローの統計値は DCNM サーバ の内部メモリに保持されます。したがって、DCNM の再起動または HA 切り替えの後は、以前に収集された値はフロー統計に表示されなくなります。ただし、サーバの再起動または HA 切り替えの後に収集されたフロー統計情報は表示できます。

DCNM で検出されたスイッチ間のアップリンクより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、スイッチ間のアップリンクが DCNM によって検出されると解決します。

Event

Cisco DCNM では、ホストとフローの間のさまざまなイベントを表示および消去することができます。イベントの記録は、[Cisco Web Client] > [Media Controller] > [Events] で行われます。

[PMN Events] テーブルは、リアルタイムで更新されます。

PMN イベントの最大保存数とクリーンアップ頻度は、[Web Client] > [Administration] > [DCNM Server] > [Server Properties] ページの [pmn.rows.limit] フィールドと [pmn.delete.interval] フィールドで、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
Purge	古い、または不要なイベントをクリックし、削除します。 次のラジオ ボタンのいずれかをクリックし、削除のオプションを選択します。 • Max # of Records：削除する必要のあるレコードの最大数を入力します。 • #ofDays：イベントを削除する必要がある日数を入力します。 • Delete all data from the previous date：日付を指定し、その日より前のデータをすべて削除します。 [Purge] をクリックし、PMN イベントの情報を削除または保持します。
Category	イベントのカテゴリを指定します。
Severity	イベントの重大度を指定します。
Description	イベントの説明を指定します。 サンプルとして、説明は次のように表示されます。 `Creating flow for FlowRequest:The flowRequest is for hostId:<<IP_Address>> hostInterface:<<Host_Int_ID>> mcastIp:<<Multicast IP>> Is sender role:false originating from switch:<<Host IP Address>>`
Impacted Flows	このイベントの影響を受けるフローを指定します。
Last Update Time	イベントが最後に変更された日付と時刻を指定します。 形式は、曜日 *MMM DD YYYY HH:MM:SS* タイムゾーンです。
Export	ローカルディレクトリパスにイベントをダウンロードできます。 ファイル名の後ろには、ファイルがエクスポートされた日付が付きます。エクスポートされるファイルの形式は、`.xls` です。

索 引

C

controller ip 20, 22
controller-credentials username 21, 22

F

feature nbm 20, 22, 23
feature nxapi 20, 22
feature ptp 32

I

ip address 28, 29, 30
ip group 24
ip group-range 24
ip igmp immediate-leave 30, 31
ip pim passive 28, 29, 30, 31
ip pim sparse-mode 28, 29, 30
ip router ospf 28, 29, 30

M

master ipv4 35, 36

N

nbm flow bandwidth 24
nbm mode controller 20, 22
nbm mode flow 24
no shutdown 28, 29, 30, 31

P

policy 24
ptp 33
ptp announce interval 33
ptp announce timeout 33
ptp delay-request minimum interval 34
ptp offload 33
ptp source 32
ptp sync interval 34
ptp transport ipv4 ucast master 35, 36
ptp ucast-source 35, 36
ptp vlan 35

S

show nbm controller 21, 22, 25
show nbm flows 25
show nbm flows bandwidth 23, 24, 25
show nbm flows statistics 25
show ptp brief 35, 36
show ptp counters interface ethernet 36
show ptp port interface 35
show running-config nbm 26
slave ipv4 35, 36