コア ACI ファブリック サービスのプロビジョニング

この章は、次の内容で構成されています。

リンク レベル ポリシー

アクセス ポリシーの一種であるリンク レベル ポリシーを設定できます。リンク レベル ポリシーには、自動ネゴシエーション、ポート速度、リンク デバウンスなどの物理層（レイヤ 1）インターフェイス設定が含まれます。

電磁場干渉に対する再トレーニング

5.2(4) 以降のリリースには、電磁干渉（EMI）再トレーニング機能があり、電磁干渉からのリンク上のノイズのフィルタリングを行い、リンク フラップを回避するようにリンクを再トレーニングできます。データセンター環境に大量の EMI ノイズが存在する場合は、EMI 再トレーニングを有効にしてください。

リンク レベル ポリシーを構成するときに、EMI 再トレーニング プロパティの有効化を選択することで、EMI再トレーニングを有効にすることができます。この機能は、銅ケーブルを使用

する Cisco N9K-C93108TC-EX および N9K-C93108TC-FX リーフ スイッチでのみサポートされます。

GUI を使用したリンク レベル ポリシーの設定

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[インターフェイス（Interface）]** > **[リンク レベル（Link Level）]**を選択します。

ステップ 3 **[リンク レベル（Link Level）]** を右クリックし、**[リンク レベル ポリシー（Create Link Level Policy）]** を選択します。

ステップ 4 **[リンク レベル ポリシーの作成（Create Link Level Policy）]** ダイアログで、必要な設定に応じてフィールドに入力します。

フィールドの詳細については、ツールチップとオンライン ヘルプを参照してください。

ステップ 5 [送信（Submit）] をクリックします。

ポート起動遅延

リリース 4.2（5）から、リンク レベル ポリシーを構成する場合は、ポートの起動時に判定フィードバック イコライザ（DFE）の調整が遅延する時間をミリ秒単位で指定する **[ポート起動遅延（ミリ秒）（Port bring-up delay (milliseconds)）]** パラメータを設定します。遅延は、一部のサードパーティ製アダプタを使用する場合に、リンクの起動中に CRC エラーを回避するために使用されます。遅延は必要な場合にのみ設定してください。ほとんどの場合、遅延を設定する必要はありません。

（注） ファブリック エクステンダ（FEX）ポートでは、**ポートの起動遅延（ミリ秒）**パラメータは適用されません。

リンク フラップ ポリシー

リンク フラップは、スイッチ上の物理インターフェイスが一定期間にわたって継続的にアップおよびダウンする状況です。原因は通常、不良、サポート対象外、または非標準のケーブルまたは Small Form-Factor Pluggable（SFP）に関連しているか、または他のリンク同期の問題に関連しており、原因は断続的または永続的です。

リンク フラップ ポリシーは、リンク フラッピング エラーのためにスイッチ ポートを無効にするタイミングを指定します。リンク フラップ ポリシーでは、スイッチのポートが指定した時間内にフラップできる最大回数を指定します。ポートが指定された時間内に指定された回数以上フラップした場合、ポートは「error-disable」状態になります。Cisco Application Policy Infrastructure Controller（APIC）を使用してポートで手動フラップを実行し、ポートを無効または有効にするまで、ポートはこの状態のままです。

（注） リンク フラップ ポリシーは、ファブリック エクステンダ（FEX）ホスト インターフェイス（HIF）ポート、および製品 ID に -EX、-FX、-FX2、-GX が指定されていないリーフ スイッチ モデルでは適用されません。

GUI を使用したリンク フラップ ポリシーの設定

次の手順では、GUI を使用してリンク フラップ ポリシーを設定します。これを任意のリーフまたはスパイン ノード インターフェイス ポリシーに接続して、ノードのアクセス ポートにリンク フラップ ポリシーを展開できます。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）] > [アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）] > [インターフェイス（Interface）] > [リンク フラップ（Link Flap）]**を選択します。

ステップ 3 **[リンク フラップ（Link Flap）]** を右クリックし、**[リンク フラップ ポリシーの作成（Create Link Flap Policy）]** を選択します。

ステップ 4 **[リンク レベル ポリシーの作成（Create Link Level Policy）]** ダイアログで、必要な設定に応じてフィールドに入力します。

フィールドの詳細については、ツールチップとオンライン ヘルプを参照してください。

ステップ 5 [送信（Submit）] をクリックします。

時刻同期と NTP

シスコ アプリケーション セントリック インフラストラクチャ（ACI）ファブリックにおいて、時刻の同期は、モニタリング、運用、トラブルシューティングなどの多数のタスクが依存している重要な機能です。クロック同期は、トラフィック フローの適切な分析にとって重要であり、複数のファブリック ノード間でデバッグとフォールトのタイム スタンプを関連付けるためにも重要です。

1 つ以上のデバイスでオフセットが生じると、多くの一般的な運用問題を適切に診断して解決する機能がブロックされる可能性があります。また、クロック同期によって、アプリケーションのヘルススコアが依存している ACI の内蔵アトミック カウンタ機能をフル活用できます。時刻同期が存在しない場合や不適切に設定されている場合でも、エラーやヘルススコアの低下が引き起こされるわけではありません。これらの機能を適切に使用できるように、ファブリックやアプリケーションを完全に展開する前に、時刻同期を設定する必要があります。デバイスのクロックを同期させる最も一般的な方法は、ネットワーク タイム プロトコル（NTP）を使用することです。

NTP を設定する前に、どの管理 IP アドレス スキームを ACI ファブリックに配置するかを検討してください。すべての ACI ノードと Application Policy Infrastructure Controller（APIC）の管理を設定するために、インバンド管理とアウトオブバンド管理の 2 つのオプションがあります。ファブリックに対して選択した管理オプションに応じて、NTP の設定が異なります。時刻同期の展開に関するもう 1 つの考慮事項は、時刻源の場所です。プライベート内部時刻または外部パブリック時刻の使用を決定する際は、時刻源の信頼性について慎重に検討する必要があります。

インバンドの管理 NTP

（注） インバンド管理アクセスについては、本書の「管理アクセスの追加」という項を参照してください。

- インバンド管理 NTP：ACI ファブリックをインバンド管理とともに展開する場合は、ACI のインバンド管理ネットワーク内から NTP サーバへの到達可能性を検討します。ACI ファブリック内で使用されるインバンド IP アドレッシングには、ファブリックの外部から到達できません。インバンド管理されているファブリックの外部の NTP サーバを使用するには、その通信を可能にするポリシーを作成します。。

NTP over IPv6

NTP over IPv6 アドレスは、ホスト名とピア アドレスでサポートされます。gai.conf も、IPv4 アドレスのプロバイダーまたはピアの IPv6 アドレスが優先されるように設定できます。ユーザは、IP アドレス（インストールまたは優先順位よって IPv4、IPv6、または両方）を提供することによって解決できるホスト名を設定できます。

GUI を使用した NTP の設定

（注） 使用する DNS サーバがインバンドまたはアウトオブバンド接続で到達可能に設定されている場合、ホスト名ベースの NTP サーバのホスト名解決に失敗するリスクがあります。ホスト名を使用する場合は、DNS プロバイダと接続する DNS サービス ポリシーが設定されていることを確認します。また、DNS プロファイル ポリシーの設定時に選択した管理 EPG のインバンドまたはアウトオブバンド VRF インスタンスに適切な DNS ラベルが設定されていることを確認します。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[ファブリック ポリシー（Fabric Policies）]**の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポッド ポリシー（Pod Policies）]** > **[ポリシー（Policies）]**の順に選択します。

ステップ 3 **[作業（Work）]** ペインで、**[アクション（Actions）]**> > **[日時ポリシーの作成（Create Date and Time Policy）]** の順に選択します。

ステップ 4 [Create Date and Time Policy] ダイアログボックスで、次の操作を実行します。

a) 環境内のさまざまな NTP 設定を区別するポリシーの名前を入力します。

b) をクリックして **有効になっている** の **認証状態** フィールドおよび展開、 **NTP クライアントの認証キー** テーブルが表示され、重要な情報を入力します。**Update** と **Next** をクリックします。

c) [+] 記号をクリックし、使用する NTP サーバ情報（プロバイダー）を指定します。

d) [Create Providers] ダイアログボックスで、次のフィールドを含めて、すべての関連情報を入力します。[Name]、[Description]、[Minimum Polling Intervals]、[Maximum Polling Intervals]。

- 複数のプロバイダーを作成する場合は、最も信頼できる NTP 時刻源の [Preferred] チェックボックスをオンにします。
- ファブリックのすべてのノードがアウトオブバンド管理によって NTP サーバに到達できる場合は、[Management EPG] ドロップダウン リストで、[Out-of-Band] を選択します。インバンド管理を導入した場合は、インバンド管理 NTP の詳細を参照してください。[OK] をクリックします。

作成するプロバイダーごとに、この手順を繰り返します。

ステップ 5 **[ナビゲーション（Navigation）]** ペインで、**[ポッド ポリシー（Pod Policies）]** > **[ポリシー グループ（Policy Groups）]**を選択します。

ステップ 6 **[作業（Work）]** ペインで、**[アクション（Actions）]**> **[ポッド ポリシー グループの作成（Create Pod Policy Group）]**を選択します。

ステップ 7 [Create Pod Policy Group] ダイアログボックスで、次の操作を実行します。

a) ポリシー グループの名前を入力します。
b) [Date Time Policy] フィールドのドロップダウン リストから、前に作成した NTP ポリシーを選択します。[Submit] をクリックします。
ポッド ポリシー グループが作成されます。または、デフォルトのポッド ポリシー グループを使用することもできます。

ステップ 8 **[ナビゲーション（Navigation）]** ペインで、**[ポッド ポリシー（Pod Policies）]** > **[プロファイル（Profiles）]**を選択します。

ステップ 9 [Work] ペインで、目的のポッド セレクタ名をダブルクリックします。

ステップ 10 [Properties] 領域の [Fabric Policy Group] ドロップダウン リストから、作成したポッド ポリシー グループを選択します。[送信（Submit）] をクリックします。

REST API を使用した NTP の設定

（注） 使用する DNS サーバがインバンドまたはアウトオブバンド接続で到達可能に設定されている場合、ホスト名ベースの NTP サーバのホスト名解決に失敗するリスクがあります。ホスト名を使用する場合は、DNS プロバイダと接続する DNS サービス ポリシーが設定されていることを確認します。また、DNS プロファイル ポリシーの設定時に選択した管理 EPG のインバンドまたはアウトオブバンド VRF インスタンスに適切な DNS ラベルが設定されていることを確認します。

手順

ステップ 1 NTP を設定します。

例：

```
POST url: https://APIC-IP/api/node/mo/uni/fabric/time-test.xml

<imdata totalCount="1">
    <datetimePol adminSt="enabled" authSt="disabled" descr=""
dn="uni/fabric/time-CiscoNTPPol" name="CiscoNTPPol" ownerKey="" ownerTag="">
        <datetimeNtpProv descr="" keyId="0" maxPoll="6" minPoll="4" name="10.10.10.11"
preferred="yes">
            <datetimeRsNtpProvToEpg tDn="uni/tn-mgmt/mgmtp-default/inb-default"/>
        </datetimeNtpProv>
    </datetimePol>
</imdata>
```

ステップ 2 デフォルトの日付と時刻のポリシーをポッド ポリシー グループに追加します。

例：

```
POST url: https://APIC-IP/api/node/mo/uni/fabric/funcprof/podpgrp-calo1/rsTimePol.xml

POST payload: <imdata totalCount="1">
<fabricRsTimePol tnDatetimePolName="CiscoNTPPol">
```

```
</fabricRsTimePol>
</imdata>
```

ステップ 3 ポッド ポリシー グループをデフォルトのポッド プロファイルに追加します。

例：

```
POST url:
https://APIC-IP/api/node/mo/uni/fabric/podprof-default/pods-default-typ-ALL/rspodPGrp.xml

payload: <imdata totalCount="1">
<fabricRsPodPGrp tDn="uni/fabric/funcprof/podpgrp-calo1" status="created">
</fabricRsPodPGrp>
</imdata>
```

GUI を使用した NTP の動作の確認

手順

ステップ 1 メニュー バーで、**[FABRIC]** > **[Fabric Policies]** を選択します。

ステップ 2 [Navigation] ペインで、**[Pod Policies]** > **[Policies]** > **[Date and Time]** > ***[ntp_policy]*** > ***[server_name]*** の順に選択します。

ntp_policy は前に作成したポリシーです。[Host Name] フィールドまたは [IP address] フィールドでは IPv6 アドレスがサポートされます。入力したホスト名に IPv6 アドレスが設定されている場合、IPv6 アドレスが IPv4 アドレスより優先されるように実装する必要があります。

ステップ 3 [Work] ペインで、サーバの詳細を確認します。

NTPサーバ

NTP サーバ機能は、クライアントのスイッチも NTPサーバとして動作して、下流のクライアントに NTP の時間情報を提供できるようにします。NTP サーバを有効にすると、スイッチ上の NTP デーモンは、NTP クライアントからのすべてのユニキャスト (IPv4 または IPv6) リクエストに対し、が時間情報によって応答します。NTP サーバの実装は、NTP RFCv3 に準拠しています。NTP RFC に従い、サーバはクライアントに関連する状態情報は維持しません。

- NTP サーバは、NTP クライアント リクエストを処理するスイッチのインバンド/アウトオブバンド管理 IP アドレスを有効にします。
- NTP サーバは、両方の管理 VRF で着信 NTP 要求に応答し、同じ VRF を使用して応答します。
- NTP サーバはIPv4 と IPv6 の両方をポートします。
- スイッチは、IPv4 クライアントとして同期して IPv6 サーバとして動作すること、およびその逆が可能です。

- スイッチは、アウトオブバンド管理 VRF 経由で NTP クライアントとして同期し、インバンド管理 VRF 経由でサーバとして動作すること、およびその逆が可能です。
- 追加コントラクトまたは IP テーブルの設定は必要ありません。
- スイッチは上流のサーバと同期すると、サーバとして時間情報をストラタム番号とともに送信します。この番号はシステムのピアのストラタム番号から 1 増えたものになります。
- スイッチ クロックが非統制 (アップストリーム サーバに同期されていない) の場合、サーバはストラタム 16 で時間情報を送信します。クライアントはこのサーバには同期できません。

デフォルトでは、NTP サーバ 機能は無効になっています。これはポリシーの設定によって明示的に有効にする必要があります。

（注） クライアントは、リーフ スイッチのインバンド、アウトオブ バンドの IP アドレスを NTP サーバ IP アドレスとして使用できます。クライアントはまた、NTPサーバ IP の一部である EPG のブリッジ ドメイン SVI も、NTP サーバ IP アドレスとして使用できます。

ファブリックのスイッチは、同じファブリックの他のスイッチに同期するべきではありません。ファブリック スイッチは常に、外部の NTP サーバに同期するべきです。

GUI を使用した NTP サーバの有効化

このセクションでは、APIC GUI で NTP を設定して NTPサーバを有効にする方法について説明します。

手順

ステップ 1 メニュー バーで、**FABRIC** > **Fabric Policies** を選択します。

ステップ 2 **ナビゲーション** ウィンドウで、**Pod Policies** > **Policies** を選択します。

Date and Time オプションが **Navigation** ウィンドウに表示されます。

ステップ 3 **Navigation** ウィンドウで、、**Date and Time** を右クリックして **Create Date and Time Policy** を選択します。

Create Date and Time Policy ダイアログが **Work** ウィンドウに表示されます。

ステップ 4 [Create Date and Time Policy] ダイアログボックスで、次の操作を実行します。

a) 環境内のさまざまな NTP 設定を区別するポリシーの名前を入力します。

b) **Server State** オプションで、**enabled** をクリックします。

Server State によって、スイッチを NTP サーバとして動作し、下流のクライアントに NTP 時間情報を提供できるようにします。

（注） サーバ機能をサポートする場合、サーバは常にピア設定にすることを推奨します。これにより、サーバはクライアントに対し、一貫した時間を提供できるようになります。

Server State を有効にすると、次のことが可能になります:

- NTP サーバは、上流のサーバに同期するスイッチに対し、時刻情報とともにストラタム番号を送信します。この番号はシステムのピアのストラタム番号から 1 つ増えたものになります。
- スイッチのクロックが上流サーバに同期していない場合、サーバは時刻情報とストラタム 16 を送信します。クライアントはこのサーバに同期することはできません。

（注） サーバ機能をサポートする場合、サーバは常にピア設定にすることを推奨します。ピア設定では、クライアントに対し一貫した時間を提供できます。

c) **Master Mode** オプションで、**enabled** をクリックします。

Master Mode を使用すれば、指定された NTP サーバが、下流のクライアントに対し、設定されたストラタム番号とともに、調整されていないローカルクロック時刻を提供することが可能になります。たとえば、NTP サーバとして動作しているリーフ スイッチは、クライアントとして動作しているリーフスイッチに対し、調整されていないローカルクロック時刻を提供できます。

（注）
- **Master Mode** が適用できるのは、サーバのクロックが調整されていない場合のみです。
- デフォルトのマスター モードの **Stratum Value** は 8 です。

d) **Stratum Value** フィールドには、NTP クライアントが同期した時刻を取得するときのストラタム番号を指定します。範囲は 1 ～ 14 です。
e) **Next** をクリックします。
f) [+] 記号をクリックし、使用する NTP サーバ情報（プロバイダー）を指定します。
g) [Create Providers] ダイアログボックスで、次のフィールドを含めて、すべての関連情報を入力します。[Name]、[Description]、[Minimum Polling Intervals]、[Maximum Polling Intervals]。
   - 複数のプロバイダーを作成する場合は、最も信頼できる NTP 時刻源の [Preferred] チェックボックスをオンにします。
   - ファブリックのすべてのノードがアウトオブバンド管理によって NTP サーバに到達できる場合は、[Management EPG] ドロップダウン リストで、[Out-of-Band] を選択します。インバンド管理を導入した場合は、インバンド管理 NTP の詳細を参照してください。[OK] をクリックします。

作成するプロバイダーごとに、この手順を繰り返します。

ステップ 5 **Navigation** ウィンドウで、**Pod Policies** を選択し、**Policy Groups** を右クリックします。

Create Pod Policy Group ダイアログが表示されます。

ステップ 6 [Work] ペインで、**[Actions]** > **[Create Pod Policy Group]** の順に選択します。

ステップ 7 [Create Pod Policy Group] ダイアログボックスで、次の操作を実行します。

a) ポリシー グループの名前を入力します。

b) [Date Time Policy] フィールドのドロップダウン リストから、前に作成した NTP ポリシーを選択します。[Submit] をクリックします。
ポッド ポリシー グループが作成されます。または、デフォルトのポッド ポリシー グループを使用することもできます。

ステップ 8 [Navigation] ペインで、**[Pod Policies]** > **[Profiles]** の順に選択します。

ステップ 9 [Work] ペインで、目的のポッド セレクタ名をダブルクリックします。

ステップ 10 [Properties] 領域の [Fabric Policy Group] ドロップダウン リストから、作成したポッド ポリシー グループを選択します。

ステップ 11 [送信（Submit）] をクリックします。

GUI を使用した日時形式の設定

ここでは、Cisco APIC GUI を使用して日時形式を設定する方法を示します。

手順

ステップ 1 メニューバーで、**[システム（System）]**>>**[システム設定（System Settings）]** を選択します。

ステップ 2 ナビゲーションペインで **[日付と時間（Date and Time）]** をクリックします。

ステップ 3 [作業（Work）] ペインで、次のオプションから選択します。

- **[表示形式（Display Format）]**：**[local]** をクリックして日時を現地時間で表示するか、**[utc]** をクリックして日時を UTC で表示します。デフォルトは **[local]** です。
- **[タイムゾーン（Time Zone）]**：ドロップダウン矢印をクリックして、ドメインのタイムゾーンを選択します。デフォルトは **[協定世界時（Coordinated Universal Time）]** です。
- **[オフセット状態（Offset State）]**：**[有効（enable）]** または **[無効（disable）]** をクリックします。有効にすると、ローカル時刻と基準時刻の差が表示されます。デフォルトは **[有効（enable）]** です。

DHCP リレー ポリシーの設定

DHCP リレー ポリシーは、DHCP クライアントとサーバが異なるサブネット上にある場合に使用できます。クライアントが配置された vShield ドメイン プロファイルとともに ESX ハイパーバイザ上にある場合は、DHCP リレー ポリシー設定を使用することが必須です。

（注）

- インフラまたは共通テナントで作成された DHCP リレー ポリシーは、ブリッジ ドメインで DHCP リレーを設定するときに他のテナントで使用できません。テナント間 DHCP リレー通信の場合は、グローバル DHCP リレー ポリシーの作成 （60 ページ） の説明に従ってグローバル DHCP リレー ポリシーを作成します。
- DHCP リレー IP アドレスは、常にプライマリ SVI IP アドレスに設定されます。

vShield コントローラが Virtual Extensible Local Area Network（VXLAN）を展開すると、ハイパーバイザ ホストはカーネル（vmkN、仮想トンネル エンドポイント（VTEP））インターフェイスを作成します。これらのインターフェイスは、DHCP を使用するインフラストラクチャ テナントで IP アドレスを必要とします。したがって、APIC が DHCP サーバとして動作しこれらの IP アドレスを提供できるように、DHCP リレー ポリシーを設定する必要があります。

ACI fabric は DHCP リレーとして動作するときに、DHCP オプション 82（DHCP Relay Agent Information Option）を、クライアントの代わりに中継する DHCP 要求に挿入します。応答（DHCP オファー）がオプション 82 なしで DHCP サーバから返された場合、その応答はファブリックによってサイレントにドロップされます。したがって、ACI fabric が DHCP リレーとして動作するときは、ACI fabric に接続されたノードを計算するために IP アドレスを提供している DHCP サーバはオプション 82 をサポートする必要があります。

Cisco APIC リリース 5.2(4) 以降、DHCPv6 オプション 79 を含むように DHCP リレー エージェントとして設定されたブリッジ ドメインを設定できるようになりました。オプション 79 が有効になっている場合、ブリッジ ドメインがリレー エージェントとして設定されているリーフ スイッチには、DHCPv6 リレー パケットのオプション 79 を介してクライアントのリンク層アドレスが含まれます。

オプション 79 を選択すると、DHCP パケットのペイロードにクライアントの MAC アドレス (クライアント リンク層アドレス) が含まれるようになります。オプション 79 には、デバイスの実際のリンク層アドレスが含まれています。リレー メッセージは、クライアントから送信される実際の DHCP パケットのイーサネット送信元 MAC アドレスを使用し、イーサネット ソースを示す 00:01 のプレフィックスを付けてから、これらの 8 バイト（クライアント MAC アドレス）をオプション 79 にコピーします。

DHCPv6 のクライアント リンク層アドレス オプションの詳細については、*RFC 6939* を参照してください。

オプション 79 を使用する利点

デュアルスタック シナリオ（IPv6 と IPv4 をサポート）では、DHCPv4 および DHCPv6 メッセージを同じクライアント インターフェイスに関連付ける必要がある場合、オプション 79 は、

RFC 標準に準拠して、DHCPv6 リレー パケットにクライアント MAC アドレスを含めて送信します。

DHCP サーバー設定フィールドについて

（注） 以下は、このセクションで使用されるいくつかの用語の定義です。

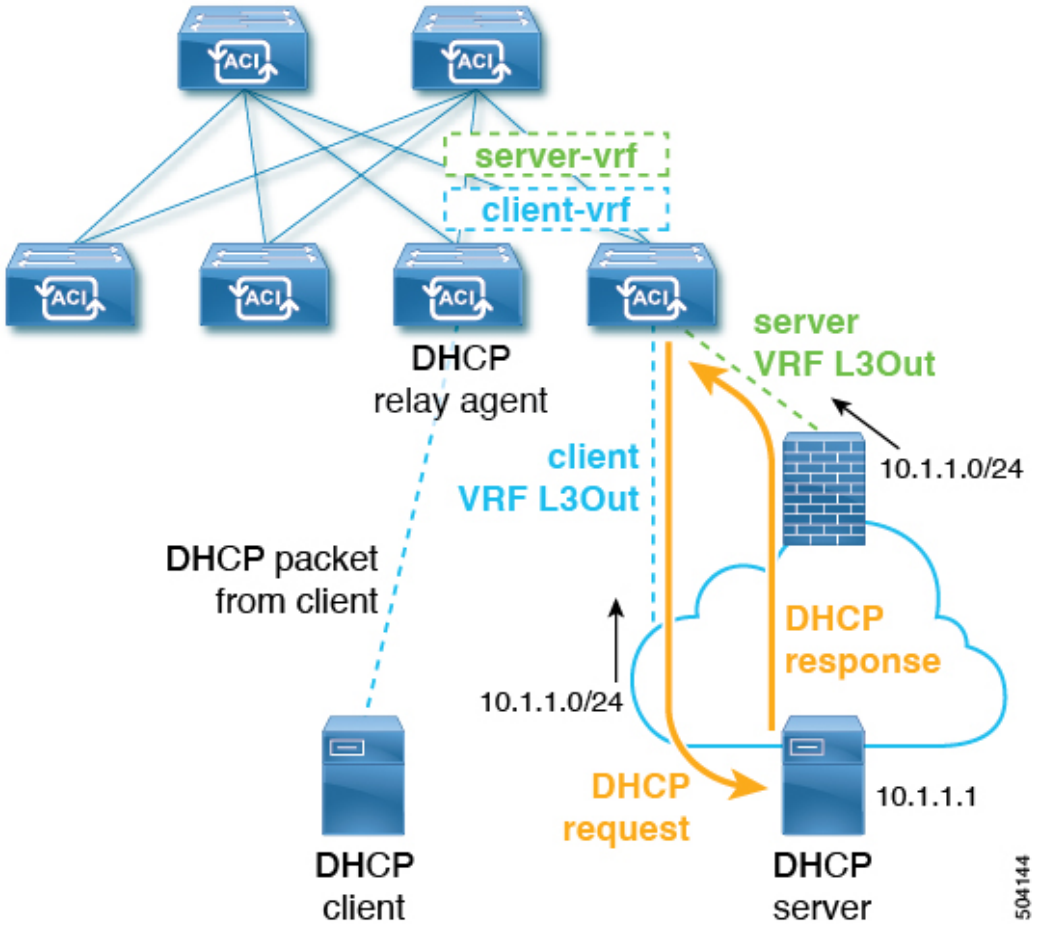
- **クライアント VRF**：DHCP 要求を開始するホストが配置されている VRF。
- **サーバー VRF**：DHCP サーバーが配置されている VRF、または DHCP サーバーに到達するためのパスを提供する VRF (たとえば、L3Out 経由で)。
- **クライアント EPG**：DHCP 要求を開始するホストが配置されている EPG。
- **サーバー EPG**：DHCP サーバーが接続されている EPG (または、DHCP サーバーが ACI ファブリックの外部にある場合、は外部 EPG)。

ACIリリース 5.2(4) では、DHCP リレー プロバイダーの設定時の `use-vrf` オプションのサポートが追加されています。この機能は、DHCP プロバイダー EPG（たとえば、DHCP サーバーが接続されている EPG）または、DHCP サーバーに到達するために使用されるレイヤー 3 外部ネットワークが、DHCP 要求を開始するホストが存在するブリッジ ドメイン（DHCP ポリシーを DHCP リレー ラベルとして参照しているブリッジ ドメイン）とは異なる VRF にある場合に使用されます。この機能は、NX-OS で使用可能な DHCP リレー `use-vrf` オプションに相当します。`use-vrf` オプションが DHCP リレー プロバイダーに対して有効になっている場合、DHCP クライアントが配置されているリーフ スイッチは、DHCP クライアントの VRF の代わりに、設定された DHCP プロバイダー EPG （または、DHCP サーバーに接続できるように設定された L3Out）の VRF を経由して、DHCP リレー パケットをルーティングします。

ACI リリース 5.2(4) より前のリリースでは、DHCP クライアントが存在する VRF とは異なる VRF の EPG またはレイヤ 3 外部ネットワークで DHCP リレー プロバイダー (サーバー) を指定できます。この VRF 間リレー ポリシーは、VRF 間コントラクトに依存しており、また DHCP サーバーへの到達可能性がある VRF（**サーバー VRF** とも呼ばれる）から DHCP クライアントが存在する VRF（**クライアント VRF** とも呼ばれる） への DHCP サーバー ネットワークのルート リークにも依存しています。DHCP リレー パケットはクライアント VRF からルーティングされ、VRF 間ルート リークを使用して、サーバー VRF から DHCP サーバーに到達します。一部のシナリオでは、DHCP サーバー ネットワークがクライアント VRF からも到達できる場合（たとえば、DHCP サーバー ネットワークにも到達できるクライアント VRF にローカル L3Out がある場合）、DHCP リレー パケットがサーバー VRF をバイパスすることがあります。DHCP リレー ポリシー プロバイダーが、クライアント VRF の 1 つとは異なるレイヤー 3 外部ネットワークを使用するように構成されている場合、DHCP リレー パケットのソース IP アドレスは、サーバー VRF（**プロバイダー L3Out** とも呼ばれる）の L3Out から選択されます。 。これらの DHCP リレー パケットが、サーバー VRF の L3Out ではなくクライアント VRF の L3Out からルーティングされる場合にも（クライアント VRF の L3Out が DHCP サーバーへのルートも持っている場合に生じる可能性があります）、DHCP サーバーの応答はサーバー VRF の L3Out に送り返されます。 DHCP リレー パケットの IP アドレスがサーバー VRF の L3Out の IP アドレ

スに設定されているためです。これにより、DHCP リレー パケットの非対称転送が発生し、ファイアウォールなどのステートフル デバイスによってドロップされる可能性があります。

次の図は、このシナリオの例を示しています。



このシナリオ例では、外部 DHCP サーバ ネットワークは、クライアントとサーバーの両方の VRF を介して ACI ファブリックで到達可能です。DHCP リレー パケットは、クライアント VRF からルーティングされ、クライアント VRF L3Out 経由で送信されます。DHCP リレー パケットの送信元 IP アドレスは、DHCP リレー ポリシーに従って、サーバーの VRF L3Out から選択されます。サーバーからの DHCP リレー応答は DHCP サーバー L3Out にルーティングされるため、非対称フローになります。

この問題を解決するため、リリース 5.2(4) 以降では、**[サーバー VRF を使用（Use Server VRF）]** というオプションが、**[DHCP サーバー設定（DHCP Server Preference）]** フィールドで使用できるようになりました。**[サーバー VRF を使用（Use Server VRF）]** オプションを有効にすると、DHCP リレー パケットは常にサーバー VRF からルーティングされます。このオプションは、VRF 間コントラクトとルート リークの要件も削除します。

[DHCP サーバー設定（DHCP Server Preference）] フィールドで選択したオプションに基づいて、リーフ スイッチは、DHCP リレー パケットをクライアント VRF またはサーバー VRF のどちらからルーティングするかを決定します。

- **[なし（None）]**: これはデフォルトのオプションで、リリース 5.2(4) より前の動作を反映しています。**[なし（None）]** オプションを選択すると、スイッチは常にクライアント VRF からの DHCP リレー パケットをルーティングします。VRF 間 DHCP リレーに使用する場合、サーバー VRF ネットワークをクライアント VRF にリークするには、共有サービス コントラクトが必要です。
- **[サーバー VRF を使用（Use Server VRF）]**: このオプションは、リリース 5.2(4) で導入された新しい動作を反映しています。**[サーバー VRF を使用（Use Server VRF）]** オプションを選択すると、スイッチは、DHCP クライアントが存在する EPG と DHCP サーバーが存在する EPG（またはDHCP サーバーが到達可能な L3Out のレイヤー 3 外部）の間にコントラクトがあるかどうかには関わりなく、サーバー VRF からの DHCP リレー パケットをルーティングします。

  VRF 間設定の場合、**[サーバー VRF を使用（Use Server VRF）]** オプション（**[DHCP サーバー プリファレンス（DHCP Server Preference）]** フィールド）を選択すると、ルート ルックアップのため、サーバー サブネット ルートは、クライアント リーフ スイッチのサーバ - VRF 内でプログラムされます。クライアント リーフ スイッチの DHCP プロセスは、それ以後、DHCP リレー パケットをサーバー VRF 経由で送信します。このため、サーバー VRF は、クライアント ブリッジ ドメインが展開されているすべてのリーフ スイッチに少なくとも 1 つの IP アドレスを使用して展開する必要があります。

GUI を使用した APIC インフラストラクチャに対する DHCP サーバ ポリシーの設定

この手順では、エンドポイント グループ（EPG）の DHCP リレー ポリシーを展開します。

次の注意事項および制約事項を確認します。

- アプリケーション エンドポイント グループで使用されるポートおよびカプセル化は、物理または VM マネージャ（VMM）ドメインに属している必要があります。ドメインにそれらの関連付けが確立されていない場合、APIC では EPG の展開を続行しますが障害が発生します。
- Cisco APIC は、IPv4 と IPv6 の両方のテナント サブネットで DHCP リレーをサポートします。DHCP サーバ アドレスには IPv4 または IPv6 を使用できます。DHCPv6 リレーは、ファブリック インターフェイスで IPv6 が有効になっており、1 つ以上の DHCPv6 リレー サーバが設定されている場合にのみ、発生します。
- シスコ APIC では、プライマリ IP アドレス プールに対してのみ DHCP リレーをサポートしています。
- 次の注意事項と制約事項は、リリース 5.2(4) で導入された **[DHCP サーバー プリファレンス（DHCP Server Preference）]** フィールドに適用されます。
  - L3Out 用に DHCP リレーが設定されている場合（たとえば、DHCP サーバーが L3Out の背後にあり、DHCP リレー ポリシーが **[サーバー VRF を使用（Use Server VRF）]** オプションに設定されている場合（**[DHCP サーバー プリファレンス（DHCP Server Preference）]** フィールドにおいて））、EPG/サーバー VRF にインターフェイスがま

だ存在しなければ、クライアント ブリッジ ドメインが展開されているリーフ スイッチへ EPG/ブリッジ ドメイン/ブリッジ ドメイン サブネットを展開する必要があります。

- EPG の背後にある DHCP サーバーに対して、DHCP リレー ポリシーが **[サーバー VRF を使用（Use Server VRF）]** オプションに設定されている場合（**[DHCP サーバー プリファレンス（DHCP Server Preference）]** フィールド）、IPv4 および IPv6 ルートの両方と、サーバ ブリッジ ドメイン SVI がクライアント リーフ スイッチに作成されます。
- **[サーバー VRF を使用（Use Server VRF）]** オプションは、サイト間 DHCP トラフィックではサポートされていません。

- オプション 79 には、以下の制限が適用されます。
  - オプション 79 は DHCPv6 でのみサポートされています。
  - オプション 79 はインフラ テナントではサポートされていません。

始める前に

レイヤ 2 またはレイヤ 3 管理接続が設定されていることを確認します。

手順

ステップ 1 メニュー バーで、**[テナント（Tenant）]** > *[テナント名（tenant_name）]* を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインの **[テナント（Tenant）]** *[テナント名（tenant_name）]* の下で、**[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[DHCP]**を展開します。

ステップ 3 [Relay Policies] を右クリックし、[Create DHCP Relay Policy] をクリックします。

ステップ 4 [Create DHCP Relay Policy] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、DHCP リレー プロファイル名（DhcpRelayP）を入力します。

この名前では最大 64 文字までの英数字を使用できます。

b) （任意） [説明（Description）] フィールドに、DHCP リレー ポリシーの説明を入力します。

説明には最大 128 文字までの英数字を使用できます。

c) [Providers] を展開します。

[DHCP プロバイダーの作成（Create DHCP Provider）] ダイアログボックスが表示されます。

d) [Create DHCP Provider] ダイアログボックスの [EPG Type] フィールドで、DHCP サーバがどこで接続されているかによって適切なオプション ボタンをクリックします。

選択する EPG タイプのオプションは、EPG タイプによって異なります。

- EPG タイプとして **[アプリケーション EPG（Application EPG）]** を選択すると、次のオプションが **[アプリケーション EPG（Application EPG）]** 領域に表示されます。
  - **[テナント（Tenant）]** フィールドで、ドロップダウン リストから、テナントを選択します。（infra）
  - [Application Profile] フィールドで、ドロップダウン リストから、アプリケーションを選択します。（access）
  - [EPG] フィールドで、ドロップダウン リストから、EPG を選択します。（デフォルト）
- EPG タイプとして **[L2 外部ネットワーク（L2 External Network）]** を選択すると、**[L2 外部ネットワーク領域（L2 External Network）]** に次のオプションが表示されます。
  - **[テナント（Tenant）]** フィールドで、ドロップダウン リストから、テナントを選択します。
  - **[L2 Out]** フィールドで、ドロップダウン リストから [L2 Out] を選択します。
  - **[External Network（外部ネットワーク）]** フィールドで、ドロップダウン リストから外部ネットワークを選択します。
- EPG タイプとして **[L3 外部ネットワーク（L3 External Network）]** を選択すると、**[L3 外部ネットワーク（L3 External Network）]**領域に次のオプションが表示されます。
  - **[テナント（Tenant）]** フィールドで、ドロップダウン リストから、テナントを選択します。
  - **[L3 Out]** フィールドで、ドロップダウン リストから [L3 Out] を選択します。
  - **[External Network（外部ネットワーク）]** フィールドで、ドロップダウン リストから外部ネットワークを選択します。
- EPG タイプとして **[DN]** を選択した場合は、ターゲット エンドポイント グループの識別名を入力します。

e) [DHCP Server Address] フィールドに、インフラ DHCP サーバの IP アドレスを入力します。

（注） インフラ DHCP IP アドレスは、インフラ IP アドレス APIC1 です。vShield コントローラ設定のために展開する場合は、デフォルトの IP アドレス 10.0.0.1 を入力する必要があります。

f) **[DHCP サーバー プレファレンス（DHCP Server Preference）]**フィールドで、このプロバイダーの管理設定値を選択します。

[DHCP サーバー プレファレンス（DHCP Server Preference）] フィールドは、リリース 5.2(4) 以降で使用できます。リーフ スイッチは、このフィールドの値を基に、クライアント VRF またはサーバー VRF のどちらから DHCP リレー パケットをルーティングするかを決定します。詳細については、DHCP サーバー設定フィールドについて （12 ページ）を参照してください。

- **[なし（None）]** : これはデフォルトのオプションで、リリース 5.2(4) より前の動作を反映しています。**[なし（None）]** オプションを選択すると、スイッチは常にクライアント VRF からの DHCP リレー パケットをルーティングします。VRF 間 DHCP リレーに使用する場合、サーバー VRF ネットワークをクライアント VRF にリークするには、共有サービス コントラクトが必要です。
- **[サーバー VRF を使用（Use Server VRF）]** : このオプションは、リリース 5.2(4) で導入された新しい動作を反映しています。**[サーバー VRF を使用（Use Server VRF）]** オプションを選択すると、スイッチは、DHCP クライアントが存在する EPG と DHCP サーバーが存在する EPG（または DHCP サーバーが到達可能な L3Out のレイヤー 3 外部）の間にコントラクトがあるかどうかには関わりなく、サーバー VRF からの DHCP リレー パケットをルーティングします。

  VRF 間設定の場合、**[サーバー VRF を使用（Use Server VRF）]** オプション（**[DHCP サーバー プリファレンス（DHCP Server Preference）]** フィールド）を選択すると、ルート ルックアップのため、サーバー サブネット ルートは、クライアント リーフ スイッチのサーバ - VRF 内でプログラムされます。クライアント リーフ スイッチの DHCP プロセスは、それ以後、DHCP リレー パケットをサーバー VRF 経由で送信します。このため、サーバー VRF は、クライアント ブリッジ ドメインが展開されているすべてのリーフ スイッチに少なくとも 1 つの IP アドレスを使用して展開する必要があります。

g) [OK] をクリックします。

[**DHCP リレー ポリシーの作成（Create DHCP Relay Policy）]** ウィンドウに戻ります。

h) [Submit] をクリックします。

DHCP リレー ポリシーが作成されます。

ステップ 5

ステップ 6 [Navigation] ペインで、**[Networking]** > **[Bridge Domains]** > **[default]** > **[DHCP Relay Labels]** を展開します。

ステップ 7 [DHCP Relay Labels] を右クリックし、[Create DHCP Relay Label] をクリックします。

ステップ 8 [Create DHCP Relay Label] ダイアログボックスで、次の操作を実行します。

a) [Scope] フィールドで、テナントのオプション ボタンをクリックします。
このアクションにより、[Name] フィールドのドロップダウン リストに、以前に作成した DHCP リレー ポリシーが表示されます。

b) [Name] フィールドのドロップダウン リストから、作成済みの DHCP ポリシーの名前（DhcpRelayP）を選択するか、[Create DHCP Relay Policy] を選択して新しいリレー ポリシーを作成します。

c) [DHCP Option Policy] で、既存のオプション ポリシーを選択するか、[Create DHCP Option Policy] を選択して新しいオプション ポリシーを作成します。

オプション 79 を呼び出すには、**ID** として 79 を使用して以前に作成した DHCP オプション ポリシーを選択します。

新しいオプション ポリシーを作成する場合は、**[DHCP オプションポリシー作成（Create DHCP Option Policy）]** ウィンドウの **[オプション（Options）]** ペインで、**ID** として 79 を入力してください。

d) [Submit] をクリックします。

DHCP サーバがブリッジ ドメインに関連付けられます。

ステップ 9 [Navigation] ペインで、**[Networking]** > **[Bridge Domains]** > **[default]** > **[DHCP Relay Labels]** を展開し、作成された DHCP サーバを表示します。

REST API を使用してオプション 79 を設定する

REST API を使用して DHCP オプション ポリシーのオプション 79 を設定するには：

```
POST URL: https://apic-ip-address/api/mo/uni.xml

<dhcpOptionPol dn="uni/tn-dhcp_client/dhcpoptpol-dhcp_option_policy"
name="dhcp_option_policy" status="">
<dhcpOption data="" id="79" name="option_79"/>
</dhcpOptionPol>
```

NX-OS スタイル CLI を使用した APIC インフラストラクチャの DHCP サーバー ポリシーの設定

- アプリケーション エンドポイント グループで使用されるポートおよびカプセル化は、物理または VM マネージャ（VMM）ドメインに属している必要があります。ドメインにそれらの関連付けが確立されていない場合、APIC では EPG の展開を続行しますが障害が発生します。
- Cisco APIC は、IPv4 と IPv6 の両方のテナント サブネットで DHCP リレーをサポートします。DHCP サーバ アドレスには IPv4 または IPv6 を使用できます。DHCPv6 リレーは、ファブリック インターフェイスで IPv6 が有効になっており、1 つ以上の DHCPv6 リレー サーバが設定されている場合にのみ、発生します。

始める前に

DHCP サーバ アドレスに到達するためにレイヤ 2 またはレイヤ 3 接続が設定されていることを確認します。

手順

APIC インフラストラクチャ トラフィックの DHCP サーバ ポリシー設定を設定します。

例：

エンドポイント グループの DHCP リレー ポリシー

```
apic1(config)# tenant infra
apic1(config-tenant)# template dhcp relay policy DhcpRelayP
apic1(config-tenant-template-dhcp-relay)# ip address 10.0.0.1 tenant infra application access epg default
apic1(config-tenant-template-dhcp-relay)# exit
apic1(config-tenant)# interface bridge-domain default
apic1(config-tenant-interface)# dhcp relay policy tenant DhcpRelayP
apic1(config-tenant-interface)# exit
```

例：

レイヤ 3 Outside の DHCP リレー ポリシー

```
ifav28-ifc2(config)# tenant dhcpTn
ifav28-ifc2(config-tenant)# template dhcp relay policy DhcpRelayPol
ifav28-ifc2(config-tenant-template-dhcp-relay)# ip address 11.1.1.11 tenant dhcpTn application ap epg serverEpg
ifav28-ifc2(config-tenant-template-dhcp-relay)# exit
ifav28-ifc2(config-tenant)# exit
ifav28-ifc2(config)# leaf 2001
ifav28-ifc2(config-leaf)# interface ethernet 1/4
ifav28-ifc2(config-leaf-if)# no switchport
ifav28-ifc2(config-leaf-if)# vrf member tenant dhcpTn vrf v1
ifav28-ifc2(config-leaf-if)# dhcp relay policy tenant DhcpRelayPol
ifav28-ifc2(config-leaf-if)# exit
```

GUI を使用した APIC インフラストラクチャ用 DHCP サーバ ポリシーの設定

- このタスクは、vShield ドメイン プロファイルを作成するユーザの前提条件です。
- アプリケーション エンドポイント グループで使用されるポートおよびカプセル化は、物理または VM マネージャ（VMM）ドメインに属している必要があります。ドメインにそれらの関連付けが確立されていない場合、APIC では EPG の展開を続行しますが障害が発生します。
- Cisco APIC は、IPv4 と IPv6 の両方のテナント サブネットで DHCP リレーをサポートします。DHCP サーバ アドレスには IPv4 または IPv6 を使用できます。DHCPv6 リレーは、ファブリック インターフェイスで IPv6 が有効になっており、1 つ以上の DHCPv6 リレー サーバが設定されている場合にのみ、発生します。

始める前に

レイヤ 2 またはレイヤ 3 管理接続が設定されていることを確認します。

手順

インフラストラクチャ テナントの DHCP サーバ ポリシーとして APIC を設定します。

（注） このリレー ポリシーは、接続エンティティ プロファイルの設定を使用した接続されたハイパーバイザであるすべてのリーフ ポートにプッシュされます。接続エンティティ プロファイルによる設定の詳細については、VMM ドメイン プロファイルの作成に関連する例を参照してください。

例：

EPG の DHCP リレー ポリシー

```
<!-- api/policymgr/mo/.xml -->
<polUni>

POST https://apic-ip-address/api/mo/uni.xml


  <fvTenant name="infra">

    <dhcpRelayP name="DhcpRelayP"  owner="tenant">
      <dhcpRsProv tDn="uni/tn-infra/ap-access/epg-default" addr="10.0.0.1" />
    </dhcpRelayP>

    <fvBD name="default">
      <dhcpLbl name="DhcpRelayP" owner="tenant"/>
    </fvBD>

  </fvTenant>
</polUni>
```

例：

レイヤ 3 Outside の DHCP リレー ポリシー

（注） **l3extLIfP** で適切な名前とオーナーを使用して DHCP リレー ラベルを指定する必要があります。

```
<polUni>
  <fvTenant name="dhcpTn">
    <l3extOut name="Out1" >
      <l3extLNodeP name="NodeP" >
        <l3extLIfP name="Intf1">
           <dhcpLbl name="DhcpRelayPol" owner="tenant" />
       </l3extLIfP>
     </l3extLNodeP>
   </l3extOut>
 </fvTenant>
<polUni>

POST https://apic-ip-address/api/mo/uni.xml
```

例：

DHCP サーバー プリファレンスを [サーバー VRF を使用] オプションに設定する

```
<!-- api/policymgr/mo/.xml -->
<polUni>

POST https://apic-ip-address/api/mo/uni.xml

<dhcpRelayP descr="" dn="uni/tn-dhcp_client/relayp-dhcp_relay_pol" status="">
    <dhcpRsProv addr="100.1.1.1/24" pref="use-server-vrf"
tDn="uni/tn-dhcp_server/ap-ap_server/epg-epg_server"/>
</dhcpRelayP>
```

例：

DHCP サーバー プリファレンスを [なし] オプションに設定する

```
<!-- api/policymgr/mo/.xml -->
```

```
<polUni>

POST https://apic-ip-address/api/mo/uni.xml

<dhcpRelayP descr="" dn="uni/tn-dhcp_client/relayp-dhcp_relay_pol" status="">
    <dhcpRsProv addr="100.1.1.1/24" pref=""
tDn="uni/tn-dhcp_server/ap-ap_server/epg-epg_server"/>
</dhcpRelayP>
```

DNS サービス ポリシーの設定

DNS ポリシーは、ホスト名で外部サーバ（AAA、RADIUS、vCenter、サービスなど）に接続するために必要です。DNS サービス ポリシーは共有ポリシーであるため、このサービスを使用するすべてのテナントと VRF を特定の DNS プロファイル ラベルで設定する必要があります。ACI ファブリックの DNS ポリシーを設定するには、次のタスクを完了する必要があります。

- 管理 EPG が DNS ポリシー用に設定されていることを確認してください。設定されていない場合、このポリシーはスイッチで有効になりません。

（注） 管理 EPG では、デフォルトの DNS ポリシーのみがサポートされます。

- DNS プロバイダーと DNS ドメインに関する情報が含まれる DNS プロファイル（デフォルト）を作成します。
- DNS プロファイル（デフォルトまたは別の DNS プロファイル）の名前を必要なテナントで DNS ラベルに関連付けます。

テナントごと、VRF ごとの DNS プロファイル設定を設定することができます。適切な DNS ラベルを使用して、追加の DNS プロファイルを作成して、特定のテナントの特定の VRF に適用できます。たとえば、名前が acme の DNS プロファイルを作成する場合、テナント設定で acme の DNS ラベルを適切な **[Networking]** > **[VRF]** ポリシー設定に追加できます。

インバンド DNS サービス ポリシーによる外部宛先の設定

次のように、サービスに対して外部宛先を設定します。

ソース	インバンド管理	アウトオブバンド管理	外部サーバの場所
APIC	IP アドレスまたは完全修飾ドメイン名（FQDN）	IP アドレスまたは FQDN	Anywhere

ソース	インバンド管理	アウトオブバンド管理	外部サーバの場所
リーフ スイッチ	IP アドレス	IP アドレスまたは FQDN （注） DNS ポリシーは、DNS サーバの到達可能性に対するアウトオブバンド管理 EPG を指定する必要があります。	Anywhere
スパイン スイッチ	IP アドレス	IP アドレスまたは FQDN （注） DNS ポリシーは、DNS サーバの到達可能性に対するアウトオブバンド管理 EPG を指定する必要があります。	リーフスイッチに直接接続されます

次に示すのは、外部サーバのリストです。

- Call Home SMTP サーバ
- Syslog サーバ
- SNMP トラップの宛先
- 統計情報のエクスポートの宛先
- エクスポートの設定の宛先
- Techsupport のエクスポートの宛先
- コア エクスポートの宛先

推奨されるガイドラインは次のとおりです。

- 外部サーバは、リーフ アクセス ポートに接続する必要があります。
- 管理ポートの追加の配線を避けるために、リーフ スイッチにはインバンド接続を使用します。
- スパイン スイッチにはアウトオブバンド管理接続を使用します。スパイン スイッチとリーフ スイッチが外部サーバの同じセットに到達できるように、スパイン スイッチのこのアウトオブバンドネットワークをインバンド管理の仮想ルーティングおよび転送（VRF）機能があるリーフ ポートの 1 つに接続します。
- 外部サーバには IP アドレスを使用します。

デュアル スタック IPv4 および IPv6 DNS サーバ

DNS サーバには、A レコード (IPv4) または AAAA レコード (IPv6) のプライマリ DNS レコードがあります。A および AAAA レコードは、ドメイン名を特定の IP アドレス (IPv4 または IPv6) と関連付けます。

ACI ファブリックは、IPv4 で実行する信頼できるパブリック DNS サーバを使用するように設定できます。これらのサーバは、A レコード (IPv4) または AAAA レコード (IPv6) で解決および応答できます。

純粋な IPv6 環境では、システム管理者は IPv6 DNS サーバを使用する必要があります。IPv6 DNS サーバは、/etc/resolv.conf に追加することによって有効化されます。

より一般的な環境では、デュアルスタック IPv4 および IPv6 DNS サーバを使用します。デュアルスタックの場合、IPv4 と IPv6 の両方が /etc/resolv.conf にリストされます。ただし、デュアルスタック環境で、単純に IPv6 DNS サーバをリストに追加すると、DNS 解決の大きな遅延を引き起こす可能性があります。これは、デフォルトで IPv6 プロトコルが優先されるため、IPv4 DNS サーバに接続できないためです (/etc/resolv.conf で最初にリストされている場合) 。この解決法は、IPv4 DNS サーバの前に IPv6 DNS サーバをリストすることです。また、IPv4 と IPv6 両方のルックアップで同一ソケットを使用できるようにするために、「options single-request-reopen」を追加します。

IPv6 DNS サーバが最初にリストされているデュアルスタック IPv4 および IPv6 DNS サーバの resolv.conf の例を次に示します。「single-request-reopen」オプションにも注意してください。

```
options single-request-reopen
nameserver 2001:4860:4680::8888
nameserver 2001:4860:4680::8844
nameserver 8.8.8.8
nameserver 8.8.4.4
```

デュアル スタック IPv4 および IPv6 環境

ACI ファブリックの管理ネットワークが IPv4 と IPv6 の両方をサポートする場合、Linux システム アプリケーション（glibc）では、getaddrinfo() が IPv6 を最初に返すため、IPv6 ネットワークをデフォルトで使用します。

ただし、特定の条件下では IPv4 アドレスが IPv6 アドレスよりも推奨されることがあります。Linux IPv6 スタックには、IPv6 にマッピングされた IPv4 アドレス（::ffff/96）を使用して、IPv6 アドレスとしてマッピングされた IPv4 アドレスを有効にする機能があります。これは、IPv6 対応アプリケーションが IPv4 と IPv6 両方を受け入れまたは接続するためにシングル ソケットのみ使用できるようにします。これは /etc/gai.conf の getaddrinfo() の glibc IPv6 選択項目によって制御されます。

/etc/hosts を使用する場合は glibc が複数のアドレスを返すようにするために、/etc/hosts ファイルに「multi on」を追加する必要があります。追加しないと、最初に一致したものだけを返す場合があります。

アプリケーションが IPv4 と IPv6 の両方が存在するかどうかを認識していない場合、異なるアドレス ファミリを使用するフォールバック試行が実行されないことがあります。このようなアプリケーションでは、フォールバックの実装が必要な場合があります。

DNS プロファイルの IPv4 または IPv6 の優先順位のポリシー

DNS プロファイルは、IPv4 と IPv6 のバージョン優先順位の選択をサポートします。ユーザ インターフェイスを使用して、優先順位を有効にすることができます。IPv4 がデフォルトです。

次の例は、Postman REST API を使用したポリシーベースの設定を示します。

```
<?xml version="1.0" encoding="UTF-8”?>
<!– api/node/mo/uni/fabric/dnsp-default.xml –>
<dnsProfile dn="uni/fabric/dnsp-default" IPVerPreference="IPv6" childAction="" descr=""
 >
</dnsProfile>
```

gai.conf の設定は、宛先アドレス選択を制御します。ファイルには、ラベル テーブル、優先順位テーブル、IPv4 範囲テーブルが含まれます。IPv4 または IPv6 をもう一方よりも優先付けする変更は、優先順位テーブルのエントリに含める必要があります。Linux システムで多数のフレーバーに使用されている標準ファイルの内容例を下に示します。ファイルの precedence ラベルの一行でデフォルト設定を上書きします。

次の例は、IPv4 を IPv6 よりも優先させるための gai.conf です。

```
# Generated by APIC
label ::1/128       0
label ::/0          1
label 2002::/16     2
label ::/96         3
label ::ffff:0:0/96 4
precedence  ::1/128       50
precedence ::/0           40
precedence 2002::/16      30
precedence ::/96          20
# For APICs prefering IPv4 connections, change the value to 100.
precedence ::ffff:0:0/96  10
```

GUI を使用した DNS プロバイダーと接続するための DNS サービス ポリシーの設定

始める前に

レイヤ 2 またはレイヤ 3 管理接続が設定されていることを確認します。

手順

ステップ 1 メニュー バーで、**[FABRIC]** > **[Fabric Policies]** を選択します。[Navigation] ペインで、**[Global Policies]** > **[DNS Profiles]** を展開し、デフォルトの DNS プロファイルをクリックします。

ステップ 2 [Work] ペインの [Management EPG] フィールドで、ドロップダウン リストから、適切な管理 EPG （デフォルト（Out-of-Band））を選択します。

ステップ 3 [DNS Providers] を展開し、次の操作を実行します。

a) [Address] フィールドに、プロバイダー アドレスを入力します。

b) [Preferred] カラムで、優先するプロバイダーとしてこのアドレスが必要な場合は、チェックボックスをオンにします。

優先するプロバイダーは 1 つだけ指定できます。

c) [Update] をクリックします。

d) （任意）セカンダリ DNS プロバイダーを追加するには、[DNS Providers] を展開し、[Address] フィールドで、プロバイダー アドレスを入力します。[Update] をクリックします。

ステップ 4 [DNS Domains] を展開し、次の操作を実行します。

a) [Name**]** フィールドに、ドメイン名（cisco.com）を入力します。

b) [Default] カラムで、チェックボックスをオンにしてこのドメインをデフォルト ドメインにします。

デフォルトとして指定できるドメイン名は 1 つだけです。

c) [Update] をクリックします。

d) （任意）セカンダリ DNS ドメインを追加するには、[DNS Domains] を展開します。[Address] フィールドに、セカンダリ ドメイン名を入力します。**Update** をクリックします。

ステップ 5 [送信（Submit）] をクリックします。
DNS サーバが設定されます。

ステップ 6 メニュー バーで、**[TENANTS]** > **[mgmt]** をクリックします。

ステップ 7 [Navigation] ペインで、**[Networking]** > **[VRF]** > **[oob]** の順に展開し、[oob] をクリックします。

ステップ 8 [Work] ペインの [Properties] 下で、[DNS labels] フィールドに、適切な DNS ラベル（デフォルト）を入力します。[Submit] をクリックします。
DNS プロファイル ラベルがテナントおよび VRF で設定されました。

カスタム証明書の設定

カスタム証明書の設定のガイドライン

- Cisco Application Policy Infrastructure Controller（APIC）で証明書署名要求（CSR）を生成するために使用される秘密キーのエクスポートはサポートされていません。証明書の CSR を生成するために使用された秘密キーを共有することにより、「Subject Alternative Name（SAN）」フィールドのワイルドカード（「* cisco.com」など）を介して複数のサーバで同じ証明書を使用する場合は、秘密キーを Cisco Application Centric Infrastructure（ACI）ファブリックの外部に配置し、Cisco ACI ファブリックにインポートします。
- 証明書署名要求（CSR）を生成する前に、公開中間証明書とルート CA 証明書をダウンロードしてインストールする必要があります。ルート CA 証明書は技術的には CSR を生成するために必要ではありませんが、シスコでは、対象とする CA 機関と CSR への署名に使用される実物の間の不一致を防ぐために、CSR を生成する前にルート CA 証明書が必要です。Cisco APIC は、送信された証明書が設定された CA によって署名されていることを確認します。
- 更新された証明書の生成に同じ公開キーと秘密キーを使用するには、次のガイドラインを満たす必要があります。
  - 元の CSR にはキー リング内の秘密キーとペアになる公開キーが含まれているため、元の CSR を維持する必要があります。
  - Cisco APIC で公開キーと秘密キーを再使用する場合は、元の証明書に使用されたものと同じ CSR を更新された証明書に再送信する必要があります。
  - 更新された証明書に同じ公開キーと秘密キーを使用する場合は、元のキー リングを削除しないでください。キー リングを削除すると、CSR で使用されている関連秘密キーが自動的に削除されます。
- Cisco ACI マルチサイト、VCPlugin、VRA、および SCVMM は、証明書ベースの認証ではサポートされません。
- Cisco APIC クラスタごとに 1つのSSL証明書のみが許可されます。
- 以降のリリースからリリース 4.0(1) にダウングレードする前に、証明書ベースの認証を無効にする必要があります。
- 証明書ベースの認証セッションを終了するには、ログアウトして CAC カードを削除する必要があります。
- Cisco APIC に設定されたカスタム証明書は、リーフ スイッチとスパイン スイッチに展開されます。ファブリック ノードに接続するために使用される URL または DN が **[サブジェクト（Subject）]** または **[サブジェクト代替名（Subject Alternative Name）]** フィールド内にある場合、ファブリック ノードは証明書でカバーされます。

• Cisco APIC GUI は、最大サイズが 4k バイトの証明書を受け入れることができます。

GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定

注意：ダウンタイムの可能性があるため、メンテナンス時間中にのみこのタスクを実行してください。ダウンタイムは外部ユーザーまたはシステムからの Cisco Application Policy Infrastructure Controller（APIC）APIC クラスタおよびスイッチへのアクセスには影響しますが、Cisco APIC とスイッチの接続には影響しませスイッチ上の NGINX プロセスも影響を受けますが、外部接続のみでファブリックのデータ プレーンには影響ありません。Cisco APIC、設定、管理、トラブルシューティングなどへのアクセスは影響を受けることになります。Cisco APIC および スイッチで実行されている NGINX Web サーバは、この操作中に再起動されます。

始める前に

適切な認証局を作成できるように、信頼できる証明書を取得する機関を決定します。

手順

ステップ 1 メニュー バーで、**[Admin]** > **[AAA]** の順に選択します。

ステップ 2 [Navigation] ペインで、[Security] を選択します。

ステップ 3 **作業**ペインで、**[認証局（Certificate Authorities）]** > **[アクション（Actions）]** > **[認証局の作成（Create Certificate Authority）]** の順に選択します。

ステップ 4 [**認証局の作成（Create Certificate Authority**）] 画面で、[**Name（名前**）] フィールドに、認証局の名前を入力します。

ステップ 5 （オプション）認証局の [**説明（Description**）] を入力します。

ステップ 6 **[証明書チェーン（Certificate Chain）]** フィールドで、Cisco APIC の証明書署名要求（CSR）に署名する認証局の中間証明書とルート証明書をコピーします。

証明書は、Base64 エンコード X.509（CER）形式である必要があります。中間証明書はルート CA 証明書の前に配置されます。次の例のようになります。

```
-----BEGIN CERTIFICATE-----
<Intermediate Certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA Certificate>
-----END CERTIFICATE-----
```

ステップ 7 [保存（Save）] をクリックします。

ステップ 8 **作業**ペインで、**[キーリング（Key Rings）]** > **[アクション（Actions）]** > **[キーリングの作成（Create Key Ring）]** の順に選択します。

キー リングを使用すると、秘密キー（外部デバイスからインポートされるか、APIC で内部的に生成される）、秘密キーによって生成される CSR、および CSR によって署名された証明書を管理できます。

ステップ 9 [Create Key Ring] ダイアログボックスで、[Name] フィールドに、名前を入力します。

ステップ 10 （オプション）キーリングの **[説明（Description）]** を入力します。

ステップ 11 **[認証局（Certificate Authority）]** フィールドで、**[認証局の選択（Select Certificate Authority）]** をクリックし、以前に作成した認証局を選択するか、**[認証局の作成（Create Certificate Authority）]** を選択します。

ステップ 12 **[秘密キー（Private Key）]** フィールドで必要なラジオボタンをクリックします。オプションは、[新しいキーの生成（Generate New Key）]、[既存のキーのインポート（Import Existing Key）] です。

ステップ 13 秘密キーを入力します。このオプションは、**秘密キー**の [既存のキーのインポート（Import Existing Key）] オプションを選択した場合にのみ表示されます。

キーリングから Cisco APIC を使用して CSR を生成する場合は、コンテンツを追加しないでください。

署名付き証明書と秘密キーを入力していない場合は、**[作業（Work）]** ペインの **[キー リング（Key Rings）]** 領域で、作成されたキー リングの **[管理状態（Admin State）]** に **[開始（Started）]** と表示され、CSR が生成されるのを待ちます。手順 17 に進みます。

署名付き証明書と秘密キーの両方を入力した場合は、**[キーリング（Key Rings）]** 領域に、作成されたキー リングの **[管理状態（Admin State）]** が **[完了（Completed）]** と表示されます。手順 21 に進みます。

（注） キー リングは削除しないでください。キー リングを削除すると、CSR で使用されている関連秘密キーが自動的に削除されます。

ステップ 14 キー リングで Cisco APIC を使用して CSR を生成する場合は、**[証明書（Certificate）]** フィールドにコンテンツを追加しないでください。または、Cisco APIC 外の秘密キーおよび CSR を生成して前の手順で CA によって署名されたものがある場合は、署名された証明書の内容を追加します。

ステップ 15 **[モジュラス（Modulus）]** フィールドで、ドロップダウンリストから目的のキーの強さを選択します。このオプションは、**秘密キー**に [新しいキーの生成（Generate New Key）] オプションを選択した場合にのみ表示されます。

ステップ 16 **[保存（Save）]** (**[キーリングの作成（Create Key Ring）]** 画面) をクリックします。

ステップ 17 **作業**ペインで、**[キーリング（Key Rings）]** > ***[キーリング名]***を選択します（または、必要なキーリングの行をダブルクリックします）。

新しい画面に選択したキーリングが表示されます。

ステップ 18 **[証明書要求（Certificate Request）]** ペインで、**[証明書要求の作成（Create Certificate Request）]** をクリックします。

[証明書要求（Certificate Request）] ウィンドウが表示されます。

a) **[サブジェクト（Subject）]** フィールドに、CSR の共通名（CN）を入力します。

ワイルドカードを使用して Cisco APIC の完全修飾ドメイン名（FQDN）を入力できますが、最新の証明書では、通常、識別可能な証明書の名前を入力し、**[代替サブジェクト名（Alternate Subject Name）]** フィールドにすべての Cisco APIC の FQDN を入力することを

推奨します（多くの最新のブラウザはSANフィールドにFQDNを想定しているため、*SAN*（サブジェクト代替名）とも呼ばれます。

b) **[代替サブジェクト名（Alternate Subject Name）]** フィールドに、「DNS：apic1.example.com、DNS：apic2.example.com、DNS：apic3.example.com」や「DNS：* example.com」など、すべての Cisco APIC の FQDN を入力します。 。

c) **[地域（Locality）]** フィールドに、組織の市または町を入力します。

d) **[州（State）]** フィールドに、組織が所在する州を入力します。

e) **[国（Country）]** フィールドに、組織の所在地の国を表す 2 文字の ISO コードを入力します。

f) **[組織名（Organization Name）]** を入力し、**[組織単位名（ Organization Unit Name）]** に単位を入力します。

g) 組織の連絡担当者の **[電子メール（Email）]** アドレスを入力します。

h) **[パスワード（Password）]** に入力し、**[パスワードの確認（Confirm Password）]** フィールドにもう一度入力します。

i) [OK] をクリックします。

ステップ 19 [証明書要求の設定] ペインに、上で入力した情報が表示されます（手順 18）。

ステップ 20 **作業**ペインで、**[キーリング（Key Rings）]** > ***[キーリング名]***を選択します（または、必要なキーリングの行をダブルクリックします）。

新しい画面に選択したキーリングが表示されます。証明書の詳細が表示されます。

（注） CSR がキー リングで示されている認証局によって署名されていない場合、または証明書に MS-DOS 形式の行末が含まれている場合は、エラー メッセージが表示され、証明書は承認されません。MS-DOS 形式の行末を削除します。

キーが確認されて [Work] ペインの [Admin State] が [Completed] に変わり、HTTP ポリシーを使用できるようになります。

ステップ 21 メニュー バーで、**[Fabric]** > **[Fabric Policies]** の順に選択します。

ステップ 22 [Navigation] ペインで、**[Pod Policies]** > **[Policies]** > **[Management Access]** > **[default]** の順に選択します。

ステップ 23 **[作業（Work）]** ペインの **[管理者キーリング（Admin Key Ring）]** ドロップダウン リストで、目的のキー リングを選択します。

ステップ 24 （オプション）証明書ベースの認証では、[Client Certificate TP] ドロップダウン リストで、以前に作成したローカル ユーザ ポリシーを選択し、[Client Certificate Authentication state] の [Enabled] をクリックします。

ステップ 25 [Submit] をクリックします。
すべての Web サーバが再起動されます。証明書がアクティブになり、デフォルト以外のキーリングが HTTPS アクセスに関連付けられています。

次のタスク

証明書の失効日には注意しておき、期限切れになる前に対応する必要があります。更新された証明書に対して同じキーペアを維持するには、CSR を維持する必要があります。これは、CSR にはキーリング内の秘密キーとペアになる公開キーが含まれているためです。証明書が期限切れになる前に、同じ CSR を再送信する必要があります。キーリングを削除すると、Cisco APIC に内部的に保存されている秘密キーも削除されるため、新しいキーリングの削除または作成は行わないでください。

ファブリック全体のシステム設定のプロビジョニング

APIC インバンドまたはアウトオブバンド接続設定(preferences)の設定

このトピックでは、APIC サーバ認証サーバまたは ACI ファブリックに外部 SNMP サーバなどのデバイスの管理アクセスのインバンドおよびアウトオブバンド接続の間で切り替える方法について説明します。有効化 **インバンド** ACI ファブリックのリーフ スイッチからの外部デバイスに APIC サーバ間のインバンド管理接続を実行します。有効化 **ooband** ACI ファブリックに外部接続の外部デバイスに APIC サーバ間のアウトオブバンド管理接続を実行します。

始める前に

インバウンドおよびアウトバウンド管理ネットワークを構成します。詳細については、「管理」(『*Cisco APIC* 基本設定ガイド、リリース *3.x*』) を参照してください。

手順

ステップ 1 メニューバーで、 **System** > **System Settings** の順にクリックします。
ステップ 2 ナビゲーション バーで、をクリックして **APIC 接続設定 (preferences)** 。
ステップ 3 ポリシーを有効にするにはクリックして **インバンド** または **ooband** 。
ステップ 4 [送信（Submit）] をクリックします。

クォータ管理ポリシーの設定

Application Policy Infrastructure Controller (APIC) リリース 2.3(1) 移行から、テナント管理者が設定できるオブジェクトの数に制限が設けられました。これにより、管理者は、テナントを超えてグローバルに追加される管理対象オブジェクトの数を制限できるようになりました。

この機能は、テナントまたはテナントのグループが、リーフごと、またはファブリックごとの ACI の最大数を超えないようにする点で、または利用可能なリソースの大部分を不当に消費して、同じファブリックの他のテナントに影響を及ぼすことがないようにする点で役立ちます。

手順

ステップ 1 メニュー バーで、**System** > **System Settings** をクリックします。

ステップ 2 **Quota** を右クリックして、**Create Quota Configuration** を選択します。

ステップ 3 **Class** フィールドで、クォータによる制限を掛けるオブジェクトのタイプを選択します。

ステップ 4 **Container Dn** フィールドに、クラスを説明する識別名 (DN) を入力します。

ステップ 5 **Exceed Action** フィールドで、**Fail Transaction Action** または **Raise Fault Action** を選択します。

ステップ 6 **Max Number** フィールドで、作成できる管理対象オブジェクトの最大数を入力します。これを超えると、超過アクションが適用されることになります。

ステップ 7 [送信（Submit）] をクリックします。

適用 BD 例外リストの作成

このトピックでは、適用対象のブリッジ ドメインには従わない、サブネットのグローバルな例外リストの作成方法について説明します。適用 BD の機能を設定している場合、対象のエンドポイント グループ (EPG) が ping を送信できるのは、関連付けられたブリッジ ドメイン内のサブネット ゲートウェイだけです。

例外 IP アドレスは、すべての VRF のすべての BD ゲートウェイに ping を送信できます。

L3Out 用に設定されたループバック インターフェイスでは、対象のループバック インターフェイスに合わせて設定された IP アドレスへの到達可能性は適用されません。

EBGP ピアとなる IP アドレスが、L3Out インターフェイスのサブネットとは異なるサブネットに存在している場合には、許容例外サブネットにピア サブネットを追加する必要があります。そうしないと、送信元 IP アドレスが L3Out インターフェイスのサブネットとは異なるサブネットに存在するため、eBGP トラフィックがブロックされます。

始める前に

適用対象のブリッジ ドメイン (BD) を作成します。

手順

ステップ 1 メニュー バーで、**System** > **System Settings** を選択します。

ステップ 2 **BD Enforced Exception List** をクリックします。

ステップ 3 **Exception List** の [+] をクリックします。

ステップ 4 任意のサブネット ゲートウェイに ping を送信できるサブネットの IP アドレスとネットワーク マスクを追加します。

ステップ 5 これを繰り返して、適用ブリッジ ドメインの例外となるサブネットを追加します。

ステップ 6 [送信（Submit）] をクリックします。

BGP ルータ リフレクタ ポリシーとルート リフレクタ ノード エンドポイントの作成

このトピックでは、ACI ファブリック ルート リフレクタを作成する方法について説明します。リフレクタは、ファブリック内で外部ルートを配布するために、マルチ プロトコル BGP (MP-BGP) を使用します。ACI ファブリックでルート リフレクタをイネーブルにするには、ファブリックの管理者がルート リフレクタになるスパイン スイッチを選択して、自律システム（AS）番号を提供する必要があります。ルート リフレクタが ACI ファブリックで有効になれば、管理者は、外部ネットワークへの接続を設定できます。

始める前に

必須項目：

- ACI ファブリックに外部ルータを接続するには、ファブリック インフラストラクチャの管理者がボーダー ゲートウェイ プロトコル（BGP）のルート リフレクタとしてスパイン ノードを設定するひつようがあります。
- 冗長性のために、複数のスパインがルータ リフレクタ ノードとして設定されます（1 台のプライマリ リフレクタと 1 台のセカンダリ リフレクタ）。

手順

ステップ 1 BGP ルート リフレクタ ポリシーを作成するには、次の手順を実行します:

a) メニュー バーで、**System** > **System Settings** をックリックします。
b) **BGP Route Reflector** をクリックします。
c) 入力自律システム番号を入力します。
d) **Route Reflector Nodes** で [+] をクリックします。
e) スパイン ルート リフレクタ ノードの ID エンドポイントを入力し、**Submit** をクリックします。

ステップ 2 外部ルート リフレクタ ノードのエンドポイントを作成するには、次の手順に従います:

a) **External Route Reflector Nodes** で [+] をクリックします。
b) 外部ルート リフレクタ ノードのエンドポイントとして機能するスパインを選択します。
c) これがマルチサイトによって管理されるサイトである場合には、インターサイト スパイン ルート リフレクタも指定できます。
d) [送信（Submit）] をクリックします。

ファブリック全体のコントロール プレーンの MTU ポリシーを設定する

このトピックでは、ファブリック全体のコントロール プレーン (CP) の MTU ポリシーを作成する方法について説明します。これは、ファブリックのノード (APIC とスイッチ) から送信されたコントロール プレーン パケットのグローバル MTU サイズを設定します。

マルチポッド トポロジでは、ファブリック外部ポートの MTU 設定は、CP MTU の値セット以上である必要があります。そうしないと、ファブリックの外部ポートがCPMTUパケットをドロップする可能性があります。

（注） MTU を IPN から継承する L3Out インターフェイス プロファイルを設定するには 9150 にします。IPN 全体で使用される MTU を 2916 に設定する必要がある場合には、L3Out インターフェイス プロファイル内で明示的に設定する必要があります (**Tenants** > ***tenant-name*** > **Networking** > **External Routed Networks** > **Create Routed Outside** > **Nodes and Interface Protocol Profiles** > **Create Node Profile** > **Create Interface Profile** で設定します)。

IPN または CP MTU を変更する場合、Cisco では CP MTU 値を変更し、次にリモート ポッドのスパイン上のMTU値を変更することをお勧めします。これで、MTUの不一致によりポッド間の接続が失われるリスクが減少します。

手順

ステップ 1 メニュー バーで、**System** > **System Settings** をックリックします。
ステップ 2 **Control Plane MTU** をクリックします。
ステップ 3 ファブリック ポートの MTU を入力します。
ステップ 4 [送信（Submit）] をクリックします。

エンドポイント ループ保護の設定

エンドポイントのループ保護ポリシーでは、頻繁な MAC の移動を処理することによる、ループ検出の方法を指定します。EP ループ保護を設定するには、次の手順を実行します:

手順

ステップ 1 メニュー バーで、**System** > **System Settings** を選択します。
ステップ 2 をクリックして **エンドポイント コントロール** 。
ステップ 3 **Ep Loop Protection** タブをクリックします。

ステップ 4 ポリシーを有効にするには、**Enabled** をクリックします (**Administrative State** フィールドにあります)。

ステップ 5 オプション。ループを検出の間隔を設定します。これはループを検出するための時間を指定します。指定できる範囲は 30～ 300 秒です。デフォルトの設定は 60 秒です。

ステップ 6 ループ検出乗算係数を設定します。これは、ループ検出間隔内で単一の EP がポート間を移動した回数です。範囲は 1 ～ 255 です。デフォルトは 4 です。

ステップ 7 ループを検出したときに実行するアクションを選択します。

アクションとしては、次のものがあります:

- **BD Learn Disable**
- **Port Disable**

デフォルトは **Port Disable** です。

ステップ 8 [送信（Submit）] をクリックします。

不正エンドポイント制御ポリシー

不正なエンドポイントの制御ポリシーについて

不正なエンドポイントは、リーフ スイッチを頻繁に攻撃し、異なるリーフ スイッチ ポートにパケットを繰り返し挿入し、802.1Q タグを変更する（エンドポイントの移動をエミュレートする）ことで、学習されたクラスと EPG ポートを変更します。誤設定により頻繁に IP アドレスと MAC アドレスが変更 (移動する) されることになります。

ファブリックの急速な移動などで、大きなネットワークの不安定状態、高い CPU 使用率、まれなケースでは、大量かつ長期のメッセージおよびトランザクション サービス (MTS) バッファ消費のため、エンドポイント マッパー (EPM) および EPM クライアント (EPMC) がクラッシュすることになります。また、このような頻繁な移動により、EPM および EPMC ログが非常にすばやくロールオーバーされ、無関係なエンドポイントのデバッグを妨害する可能性があります。

不正なエンドポイントの制御機能は脆弱性にすばやく対処します。

- 急速に移動する MAC および IP エンドポイントの特定。
- エンドポイントを一時的に静的にして、エンドポイントを隔離することによって移動を停止します。
- 3.2(6) リリースより前：**不正 EP 検出間隔**のエンドポイントを静的に維持し、不正エンドポイントとの間のトラフィックをドロップします。この時間が経過すると、不正な MAC アドレスまたは IP アドレスが削除されます。
- 3.2(6) リリース以降：**不正な EP 検出間隔**のエンドポイントを静的に維持（この機能はトラフィックをドロップしなくなりました）。この時間が経過すると、不正な MAC アドレスまたは IP アドレスが削除されます。

- ホスト トラッキング パケットを生成して、影響を受ける MAC または IP アドレスをシステムが再学習できるようにします。
- 修正アクションを有効にするための障害の発生。

不正なエンドポイント制御ポリシーはグローバルに設定されており、他のループ防止方法とは異なり、個々のエンドポイント レベルの機能です (IP および MAC アドレス) 。ローカルまたはリモートの移動を区別していません。いかなる種類のインターフェイスの変更も、エンドポイントを隔離する必要があるかどうかを決定する際に移動と見なされます。

不正なエンドポイント制御機能は、デフォルトで無効になっています。

不正エンドポイント制御ポリシーの制限事項

不正エンドポイント制御ポリシーを使用する際には、次の制限が適用されます:

- 不正エンドポイント制御ポリシーのパラメータを変更しても、既存の不正エンドポイントには影響しません。
- 不正エンドポイントが有効になっていても、ループ検出とブリッジ ドメイン移動頻度は有効になりません。
- 不正エンドポイント機能を無効にすると、すべての不正エンドポイントがクリアされます。
- エンドポイント マッパー (EPM) の値は、不正エンドポイントのパラメータに制限を課します。この範囲外のパラメータ値を設定すると、Cisco APIC 適切でないパラメータごとにエラーが発生します。
- 不正エンドポイント検出のサポートは、リモート リーフ ノードに接続されているエンドポイントではなく、ファブリックに接続されているエンドポイントに限定されます。
- 不正なエンドポイント機能は、Cisco ACI マルチサイト 展開の各サイト内で使用でき、サイト内でエンドポイントを移動させるサーバの設定ミスに役立ちます。不正エンドポイント機能は、エンドポイントがサイト間を移動する可能性があるシナリオ向けには設計されていません。
- Cisco APIC リリース 4.1 にアップグレードする前に、不正エンドポイント制御を無効にする必要があります。

GUI を使用した不正エンドポイント制御ポリシーの設定

Cisco Application Policy Infrastructure Controller（Cisco APIC）GUI を使用して、不正なエンドポイントを検出して削除するようにファブリックの**不正 EP 制御**ポリシーを設定できます。このトピックには、アドホックのリーフスイッチで不正なエンドポイントをクリアする手順も含まれています。

手順

ステップ 1 メニュー バーで、**System** > **System Settings** を選択します。

ステップ 2 ナビゲーション ウィンドウで、**[エンドポイント制御（Endpoint Controls）]** を選択します。

ステップ 3 [ナビゲーション（Navigation）] ペインで、**[不正な EP 制御（Rogue EP Control）]** タブを選択します。

ステップ 4 **[Administrative State]** を **[Enabled]** に設定します。

ステップ 5 **[不正な EP 検出間隔（Rogue EP Detection Interval）]**、**[不正な EP 検出倍数係数（Rogue EP Detection Multiplication Factor）]**、および **[保持間隔（秒）（Hold Interval (sec)）]** を目的の値に設定します。

- **不正な EP 検出間隔**：不正エンドポイントの検出間隔を設定します。これは、不正エンドポイントを検出する時間を指定します。有効な値は 0 ～ 65535 秒です。デフォルトは 60 です。
- **不正な EP 検出倍数係数**：エンドポイントが不正かどうかを判断するための不正エンドポイント検出の乗数を設定します。エンドポイントがこの数よりも多く移動すると、エンドポイント検出間隔内で、エンドポイントは不正と宣言されます。有効値は 2 ～ 10 です。デフォルト値は 6 です。
- **保持間隔（秒）**：エンドポイントが不正であると宣言されてからの間隔（秒単位）。学習が防止され、不正なエンドポイントとの間のトラフィックがドロップされます。このインターバルが経過すると、エンドポイントは削除されます。5.2(3) リリースより前では、有効な値は 1800 ー 3600 秒です。5.2(3) リリースより前では、有効な値は 1800 ー 3600 秒です。デフォルト値は 1800 です。

ステップ 6 （任意）リーフ スイッチの不正なエンドポイントをクリアするには、次の手順を実行します。

a) Cisco APICメニュー バーで、**[Fabric]** > **[Inventory]** の順にクリックします。
b) ナビゲーションバーで、[Pod] を展開し、不正なエンドポイントをクリアするリーフ スイッチをクリックします。
c) リーフ スイッチ サマリが作業ウィンドウに表示されたら、ナビゲーション バーのリーフ スイッチ名を右クリックし、**[Clear Rogue Endpoints]** を選択します。
d) **[はい（Yes）]** をクリックします。

NX-OS スタイル CLI を使用している不正エンドポイント制御ポリシーの設定

NX-OS スタイルの CLI を使用して、不正なエンドポイントを検出および削除するように、ファブリックの不正エンドポイント制御ポリシーを設定できます。

手順

ステップ 1 グローバル コンフィギュレーション モードに入ります。

例：

```
apic1# configure
```

ステップ 2 グローバルな不正エンドポイント制御ポリシーを有効にします。

例：

```
apic1(config)# endpoint rogue-detect enable
```

ステップ 3 ホールド間隔を設定します。

保持間隔は、エンドポイントが不正であると宣言されてからエンドポイントが静的に保たれ、学習が防止され、エンドポイントとの間のトラフィックがドロップされた後の期間（秒）です。このインターバルが経過すると、エンドポイントは削除されます。リリース 5.2(2) 以前では、有効な値は 1800 ～ 3600 秒です。リリース 5.2(3) 以降では、有効な値は 300 ～ 3600 秒です。デフォルト値は 1800 です。

例：

```
apic1(config)# endpoint rogue-detect hold-interval 1800
```

ステップ 4 検出間隔を設定します。

検出間隔は、不正エンドポイント制御がエンドポイントの移動数をカウントしている間の期間（秒）です。この間隔の中のカウントが検出乗算係数で指定された値を超える場合、エンドポイントは不正であると宣言されます。有効な値は 0 ～ 65535 秒です。デフォルトは 60 です。

例：

```
apic1(config)# endpoint rogue-detect interval 60
```

ステップ 5 検出倍率を設定します。

エンドポイントが、検出間隔で指定された期間中に検出倍率で指定された値よりも多く移動した場合、エンドポイントは不正であると宣言されます。有効値は 2 ～ 10 です。デフォルト値は 6 です。

例：

```
apic1# endpoint rogue-detect factor 6
```

REST API を使用した不正エンドポイント制御ポリシーの設定

REST API を使用して、不正エンドポイントを検出および削除するようにファブリックの不正エンドポイント制御ポリシーを設定できます。

手順

ステップ 1 不正エンドポイント制御ポリシーを設定するには、次の例のような XML を使用してポストを送信します。

例：

```
<polUni>
    <infraInfra>
        <epControlP name="default" adminSt="enabled"  holdIntvl="1800"
rogueEpDetectIntvl="60" rogueEpDetectMult="6"/>
    </infraInfra>
</polUni>
```

- `adminSt`：不正エンドポイント制御の管理状態。不正エンドポイント制御を有効にするには、`[指定（enable）]` を指定します。
- `holdIntvl`：不正エンドポイントの保持間隔。保持間隔は、エンドポイントが不正であると宣言されてからエンドポイントが静的に保たれ、学習が防止され、エンドポイントとの間のトラフィックがドロップされた後の期間（秒）です。このインターバルが経過すると、エンドポイントは削除されます。リリース 5.2(2) 以前では、有効な値は 1800 ～ 3600 秒です。リリース 5.2(3) 以降では、有効な値は 300 ～ 3600 秒です。デフォルト値は 1800 です。
- `rogueEpDetectIntvl`：不正エンドポイント検出間隔。検出間隔は、不正エンドポイント制御がエンドポイントの移動数をカウントしている間の期間（秒）です。この間隔の中のカウントが検出乗算係数で指定された値を超える場合、エンドポイントは不正であると宣言されます。有効な値は 0 ～ 65535 秒です。デフォルトは 60 です。
- `rogueEpDetectMult`：不正エンドポイント検出の乗算係数エンドポイントが、検出間隔で指定された期間中に検出倍率で指定された値よりも多く移動した場合、エンドポイントは不正であると宣言されます。有効値は 2 ～ 10 です。デフォルト値は 6 です。

ステップ 2 この機能の動作を元に戻すと、次の例のように XML を使用してポストを送信することで、不正なエンドポイントとの間のトラフィックを再度ドロップできます。

例：

```
<infraImplicitSetPol rogueModeAction="quarantine-fault-and-drop" infraDn="uni/infra"/>
```

不正/ COOP 例外リストについて

不正/ COOP 例外リストを使用すると、エンドポイントが不正としてマークされる前に、不正エンドポイント制御によるエンドポイント移動の許容度を高くするエンドポイントの MAC アドレスを指定できます。不正/ COOP 例外リストのエンドポイントは、10 分以内に 3000 回以上移動した場合にのみ不正としてマークされます。エンドポイントが不正としてマークされた後、学習を防ぐためにエンドポイントは静的なままになります。不正エンドポイントは 30 秒後に削除されます。

不正/ COOP 例外リストのガイドラインと制限事項

不正/COOP 例外リストを使用するとき、次の注意事項と制限事項が適用されます。

- MAC アドレス例外リスト機能は、レイヤ 2 ブリッジ ドメイン（IP ルーティングが有効になっていないブリッジ ドメイン）で動作します。これは、レイヤ 3 ブリッジ ドメイン（IP ルーティングが有効になっているブリッジ ドメイン）では、MAC アドレスとともに移動

する IP アドレスがあった場合、最初に IP アドレスが放浪しているとしてマークされ、その後 IP アドレスと MAC アドレスの両方が検疫対象とされるためです。

- レイヤ 3 ブリッジ ドメインの場合、放浪エンドポイント制御から除外する特定の IP アドレスについては、サブネットごとのデータプレーン IP アドレス学習を無効にします。

  サブネットごとのデータプレーン IP アドレス学習機能については、*Cisco APIC Layer 3* ネットワーキング設定ガイドを参照してください。

- このリストに追加されている MAC アドレスの種類を完全に理解している必要があります。このリスト内の MAC アドレスが、ファブリック全体での過剰な移動に寄与しないようにすることは、ユーザーの責任です。
- 例外リストには、ファブリック全体で最大 100 個の MAC アドレスを追加できます。
- リーフ スイッチの例外リストの免除は、放浪エンドポイント制御が有効になっている場合にのみ適用されます。放浪エンドポイント制御が無効になっている場合、MAC アドレス例外リストは、COOP ダンプニングでのみ使用されます。
- 不正/ COOP 例外リストには、ブリッジ ドメインの MAC アドレスのみを含めることができ、VRF インスタンスの IP アドレスは含めることができません。ただし、IP アドレスのみの移動では、IP アドレスが通常の不正エンドポイント制御基準を満たす場合でも、IP アドレスが不正としてマークされる可能性があります。
- データ パストラフィックに基づいて IP アドレスの不正検出およびマーキングをマスクするには、ブリッジ ドメイン サブネット学習無効を使用します。ブリッジ ドメイン サブネット ラーニング無効化は、移動するたびに Cisco ACI が IP アドレスの場所を学習しなくなります。

GUI を使用したブリッジ ドメイン作成時の不正/ COOP 例外リストの設定

次の手順では、ブリッジ ドメインの作成時に不正/ COOP 例外リストを設定します。

始める前に

- ブリッジ ドメインを作成するテナントが必要です。
- 不正エンドポイント制御を有効にする必要があります。不正エンドポイント制御を有効にする手順については、GUI を使用した不正エンドポイント制御ポリシーの設定 （35 ページ） を参照してください。

手順

ステップ 1 目的のテナントで、ブリッジドメインを作成します。メニューバーで、**[テナント（Tenants）]**> ***[tenant_name]***を選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、**[ネットワーキング（Networking）]** > **[ブリッジ ドメイン（Bridge Domains）]** の順に選択します。

ステップ 3 **Bridge Domains** を右クリックして、**Create Bridge Domain** を選択します。

ステップ 4 **[ブリッジ ドメインの作成（Create Bridge Domain）]** ダイアログで、**[ステップ 1（STEP 1）]** の **[メイン（MAIN）]** および **[ステップ 2（STEP 2）]** の **[L3 設定（L3 Configurations）]** に必要なフィールドに入力します。

ステップ 5 **[STEP 3（ステップ 3）]** の **[アドバンスト/トラブルシューティング（Advanced / Troubleshooting）]** で、**[不正/COOP 例外リスト（Rogue / Coop Exception List）]** の **[+]** をクリックし、リストに追加するエンドポイントの MAC アドレスを入力して、**[更新（Update）]** をクリックします。

MAC アドレスの形式は `AA:BB:CC:DD:EE:FF` です。

a) リストに追加するエンドポイントごとにこのステップを繰り返します。

ステップ 6 必要に応じて、**[ステップ 3（STEP 3）]** > **[アドバンスト/トラブルシューティング（Advanced/Troubleshooting）]** の残りのフィールドに入力します。

ステップ 7 [Finish] をクリックします。

GUI を使用した既存のブリッジ ドメインの不正/ COOP 例外リストの設定

次の手順では、既存のブリッジ ドメインの不正/ COOP 例外リストを設定します。

始める前に

- ブリッジ ドメインを持つテナントが必要です。
- 不正エンドポイント制御を有効にする必要があります。不正エンドポイント制御を有効にする手順については、GUI を使用した不正エンドポイント制御ポリシーの設定 （35 ページ） を参照してください。

手順

ステップ 1 目的のテナントで、ブリッジドメインを作成します。メニューバーで、**[テナント（Tenants）]**> ***[tenant_name]***を選択します。

ステップ 2 [ナビゲーション（Navigation）] ウィドウで、**[ネットワーキング（Networking）]** > **[ブリッジ ドメイン（Bridge Domains）]** > ***[bridge_domain_name]***. を選択します。

ステップ 3 [作業（Work）] ペインで、**[ポリシー（Policy）]** > **[アドバンスト/トラブルシューティング（Advanced/Troubleshooting）]** を選択します。

ステップ 4 **[不正/COOP 例外リスト（Rogue / Coop Exception List）]** で **[+]** をクリックし、リストに追加するエンドポイントの MAC アドレスを入力して、**[更新（Update）]** をクリックします。

MAC アドレスの形式は `AA:BB:CC:DD:EE:FF` です。

a) リストに追加するエンドポイントごとにこのステップを繰り返します。

ステップ 5 [送信（Submit）] をクリックします。

REST API を使用して既存のブリッジ ドメインの不正/COOP 例外リストを設定する

次の REST API ポストは、既存のブリッジ ドメインの不正/ COOP 例外リストに MAC アドレスを追加します。

```
https://apic1.myDomain.com/api/node/mo/uni/tn-tenant1.xml
<fvBD name="bd1">
    <fvRogueExceptionMac annotation="" descr="" mac="00:16:04:00:00:1"/>
</fvBD>
```

最大 IP アドレス フロー制御について

3.2(6) リリースでは、最大IPアドレスフロー制御機能が追加されています。これは、エンドポイントの動作不良を識別し、MAC アドレスに関連付けられている学習 IP アドレスの数に基づいて不正としてフラグを立てます。Cisco Application Centric Infrastructure（ACI）ファブリックは、MAC アドレスで最大 4,096 個の IP アドレスをサポートします。リーフ スイッチが MAC アドレスに関連付けられた 4,096 を超える IP アドレスを学習した場合、MAC アドレスとすべての IP アドレスが不正として分類されます。

最大 IP アドレス フロー制御機能がエンドポイントを不正として識別した後、エンドポイントは隔離され、APIC で障害が発生し、このエンドポイントで新しい IP アドレスの学習は行われません。隔離期間は 1 時間です。標準の不正機能が有効になっている場合、隔離期間は標準の不正設定で設定された期間と同じです。

不正なエンドポイント制御ポリシー機能（移動による不正）は有効または無効に設定できますが、最大 IP アドレス フロー制御機能では明示的な設定を有効にする必要はありません。

この機能が導入される前は、設定可能な期間内に設定された回数だけロケーションを移動し続けた場合、ACI ファブリックはエンドポイントを不正と識別していました。この機能を使用すると、ACI ファブリックは、移動の数に基づいて、または MAC アドレスで 4,096 を超える IP アドレスを学習した場合に、エンドポイントを不正として識別できます。

COOP の設定

COOP について

Council of Oracle Protocol（COOP）は、スパイン スイッチ プロキシにマッピング情報（場所と ID）を通信するために使用されます。リーフ スイッチ（「citizen」）は、ゼロ メッセージ キュー（ZMQ）を使用して、エンドポイント アドレス情報をスパイン スイッチ（「oracle」）に転送します。スパイン ノードで実行している COOP によって、すべてのスパイン ノードが一貫性のあるエンドポイント アドレスとロケーション情報のコピーを維持することができ、さらに、ロケーション マッピング データベースに対するエンドポイント ID の分散ハッシュ テーブル（DHT）レポジトリを維持することができます。

COOP エンドポイントのダンプニング

悪意のある動作または誤った動作によって不要なエンドポイント更新が発生すると、COOPプロセスが過負荷になり、有効なエンドポイント更新の処理が妨げられる可能性があります。リーフ スイッチの不正エンドポイント検出機能により、多数の誤った更新がスパイン スイッチに到達するのを防ぐことができます。不正なエンドポイントの検出が不十分な場合、COOPプロセスはエンドポイントのダンプニングを呼び出します。COOPの負荷を軽減するために、スパイン スイッチはすべてのリーフ スイッチに、指定された期間、不正な動作をしているエンドポイントからの更新を無視するように要求します。これが発生すると、エンドポイントのダンプニング状態は「フリーズ」になり、障害が生成されます。

（注） COOP エンドポイント ダンプニングは、Cisco Application Policy Infrastructure Controller（APIC）リリース 4.2(3) で導入され、デフォルトで有効になっています。

検出基準は、次の表に示すように、エンドポイント関連イベントのタイプに基づくペナルティ値の計算に基づきます。

イベント（Event）	ペナルティ値	注
新しい IP アドレスを確認する	0	新しい IP アドレスが学習されます。
追加の IP アドレスを確認する	2	追加の IP アドレスは、既存のエンドポイントの MAC アドレスで学習されます。
IP アドレスの削除	50	リモート エンドポイントの IP アドレスは、IP アドレスが学習されると削除されます。
削除された IP アドレスを確認する	50	IP アドレスが削除された後のリモート エンドポイントの IP アドレスを確認します。
IP アドレスの削除	400	IP アドレスが学習されたら、ローカル エンドポイントの IP アドレスを削除します。
削除された IP アドレスを確認する	400	IP アドレスが削除された後のローカル エンドポイント IP アドレスを確認します。
エンドポイントの移動	200	エンドポイントが別のインターフェイスに移動します。
IP アドレスの移動	200	IP アドレスが別の MAC アドレスに移動する。 このイベントでは、BGP へのルート更新が 2 回発生するため、ペナルティは高くなります。
URIB プログラミング	50	エンドポイントのスパイン スイッチ トンネル インターフェイスのステータス変更（アップ/ダウン）。

ペナルティ値は IP アドレスごとに計算され、5 分ごとに 50% ずつ減少します。たとえば、エンドポイントのペナルティ値が 4000 で、エンドポイントの IP アドレスの数が 2 の場合、IP アドレスあたりのペナルティ値は 4000/2 = 2000 です。IP アドレスあたりのペナルティ値がクリティカルしきい値（4000）を超えると、エンドポイントの状態が **[標準（Normal）]** から **[クリティカル（Critical）]** に変更されます。エンドポイントが 5 分を超えて **[クリティカル（Critical）]** 状態になっている場合、または IP アドレスあたりのペナルティ値がフリーズしきい値（10000）を超えている場合、エンドポイントの状態は**フリーズ**（ダンプニング）になり、エンドポイントの更新は無視されます。IPアドレスあたりのペナルティ値が再利用しきい値（2500）を下回ると、エンドポイントの状態は **Normal**（非ダンプニング）になります。ペナルティ値を 75%（10000 * 0.5 * 0.5 = 2500）減らすには、10 分経過する必要があります。しきい値はユーザが設定することはできません。

COOP 認証

COOPデータパス通信は、セキュアな接続を介した転送を優先します。悪意のあるトラフィック インジェクションから COOP メッセージを保護するために、Cisco APIC およびスイッチは COOP プロトコル認証をサポートしています。

COOP プロトコルは、次の 2 つの ZMQ 認証モードをサポートしています。

- **厳密モード**： COOP では、MD5 認証 ZMQ 接続のみ許可します。
- **互換性モード**：COOP ではメッセージの転送に MD5 認証接続と非認証 ZMQ 接続の両方を許可します。

COOP 認証の詳細については、『*Cisco APIC* セキュリティ設定ガイド』を参照してください。

GUI を使用した COOP 減衰エンドポイントの表示

スパイン ノードのすべての減衰エンドポイントを表示するには、この Cisco Application Policy Infrastructure Controller（APIC）GUI 手順を使用します。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）] > [インベントリ（Inventory）]** をクリックします。

ステップ 2 [ナビゲーション（Navigation）] ペインで、パッドとスパイン ノードを展開します。

ステップ 3 **[プロトコル（Protocols）] > [COOP]** および **[COOP]** インスタンスを展開します。

ステップ 4 **[エンドポイント データベース（Endpoint Database）]** をクリックして、エンドポイントを表示します。

[減衰状態（Dampened State）] カラムを調べて、減衰したエンドポイントを見つけます。次の状態があります。

- **Normal**：エンドポイントの更新は正常です。
- **Critical**：エンドポイントをフリーズ状態に移行できる十分な更新を受信しました。エンドポイントが 5 分以上 **Critical** 状態のままになると、状態は **Freeze** に変わります。

- **Freeze**：このエンドポイントからの更新は、頻繁に不要な更新が行われているため、現在無視されています。障害が生成されました。

スイッチ CLI を使用した COOP 減衰エンドポイントの表示

スパインまたはリーフ ノードのすべての減衰エンドポイントを表示するには、このスイッチ CLI 手順を使用します。

スパインまたはリーフ スイッチ CLI にログインし、次のコマンドを入力します。

```
show coop internal info repo ep dampening
```

GUI を使用した COOP 減衰エンドポイントのクリア

スパインまたはリーフ ノードのすべての減衰エンドポイントをクリアおよび回復するには、この Cisco Application Policy Infrastructure Controller（APIC）GUI 手順を使用します。この操作は、すべてのスパイン スイッチおよびエンドポイントの送信元リーフ スイッチで実行する必要があります。減衰されたエンドポイントがリーフ スイッチのエンドポイント テーブルにまだある場合、エンドポイントはスパイン スイッチ COOP データベースにパブリッシュされます。そうでない場合、減衰したエンドポイントは、2 分後にスパイン スイッチ COOP データベースから削除されます。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）] > [インベントリ（Inventory）]** をクリックします。

ステップ 2 [ナビゲーション（Navigation）] ペインで、パッドとスパインまたはリーフ ノードを展開します。

ステップ 3 ノードを右クリックし、**[減衰エンドポイントの消去（Clear Dampened Endpoints）]** を選択します。

ステップ 4 **[はい（Yes）]** をクリックして、アクションを確認します。

スイッチ CLI を使用した COOP 減衰エンドポイントのクリア

スパインまたはリーフ ノードの減衰エンドポイントをクリアして回復するには、次の手順を使用します。この手順では、ダンプニング状態が **Freeze** である単一のエンドポイントを回復します。この操作は、すべてのスパイン スイッチおよびエンドポイントの送信元リーフ スイッチで実行する必要があります。

スパインまたはリーフ スイッチ CLI にログインし、次のコマンドを入力します。

```
clear coop internal info repo ep dampening key <bd> <mac>
```

RESTAPI を使用した COOP エンドポイント ダンプニングの無効化

この手順では、APIC REST API を使用して COOP EP ダンプニングを無効または有効にする方法を示します。

COOPエンドポイントのダンプニングはデフォルトで有効になっていますが、場合によっては無効にする必要があります。たとえば、1つの MAC アドレスに対して多数の IP 更新が予想され、それらの更新を無視するとネットワークが中断される場合があります。

次の API を使用し、`disableEpDampening = "true"` を設定して COOP エンドポイント ダンプニングを無効にします。

```
<!-- api/policymgr/mo/.xml -->

<polUni>
    <infraInfra>
        <infraSetPol disableEpDampening="true"></infraSetPol>
    </infraInfra>
</polUni>
```

ファブリック内のすべてのノードは COOP エンドポイント ダンプニングを無効にし、ダンプニング状態が「フリーズ」である既存のエンドポイントを回復します。

APIC GUI を使用した COOP 認証の設定

手順

ステップ 1 メニュー バーで、**[System]** > **[System Settings]** の順に選択します。

ステップ 2 **[ナビゲーション]** ペインで **[COOP グループ]** をクリックします。

ステップ 3 **[作業]** ペインの **[タイプ]** フィールドにある **[ポリシー プロパティ]** 領域で、**[互換性のあるタイプ]** および **[ストリクト タイプ]** オプションから希望のタイプを選択します。

ステップ 4 [Submit] をクリックします。
これにより、COOP 認証ポリシー設定を完了します。

Cisco NX OS スタイル CLI を使用した COOP 認証の設定

手順

ストリクト モード オプションを使用して、COOP 認証ポリシーを設定します。

例：

```
apic1# configure
apic1(config)# coop-fabric
apic1(config-coop-fabric)# authentication type ?
compatible  Compatible type
```

```
strict      Strict type
apic101-apic1(config-coop-fabric)# authentication type strict
```

REST API を使用した COOP 認証の設定

手順

COOP 認証ポリシーを設定します。

例では、ストリクト モードが選択されます。

例：

```
https://172.23.53.xx/api/node/mo/uni/fabric/pol-default.xml

<coopPol type="strict">
</coopPol>
```

エンドポイント リッスン ポリシー

エンドポイント リッスン ポリシーについて

エンドポイント リッスン ポリシーを設定して、ポリシーが適用されていない Cisco Application Centric Infrastructure（ACI）のリーフ スイッチに匿名エンドポイントから送信されるタグなしトラフィックを検出できます。デフォルトでは、ポートにポリシーが展開されていない場合、すべてのエンドポイント トラフィックがそのポートでドロップされます。エンドポイント リッスン ポリシーを設定すると、このポリシーは、適用されている既存のポリシーがないすべてのリーフ スイッチ ポートに展開されます。エンドポイント リッスン ポリシーでは、Cisco ACI でこれらのポートに着信するタグなしトラフィックを検出できます。これにより、Cisco ACI で匿名エンドポイントの MAC アドレスまたは IP アドレスがわかります。これにより、Cisco ACI 管理者はこれらのエンドポイントを配置する EPG を決定できます。Cisco Application Policy Infrastructure Controller（APIC）GUI は、検出されたすべての匿名エンドポイントを**グローバル エンド ポイント**設定画面に表示します。

（注） エンドポイント リッスン ポリシーはベータ機能です。この機能が意図したとおりに動作する保証はありません。自己責任で使用してください。

GUI を使用したエンドポイント リッスン ポリシーの設定

この手順では、エンドポイント リッスン ポリシーを設定します。このポリシーは、匿名エンドポイントから、適用されたポリシーがない Cisco Application Centric Infrastructure（ACI）リーフ スイッチに送信されるタグなしトラフィックを検出します。

（注） エンドポイント リッスン ポリシーはベータ機能です。この機能が意図したとおりに動作する保証はありません。自己責任で使用してください。

手順

ステップ 1 メニュー バーで、**[システム（System）] > [システム設定（System Settings）]** の順に選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、**[グローバル エンドポイント（Global Endpoints）]** を選択します。

ステップ 3 [作業（Work）] ペインで、**[エンドポイント リッスン ポリシー（End Point Listen Policy）]** チェックボックスをオンにします。

ステップ 4 **[エンドポイント リッスン エンキャップ（End Point Listen Encap）]** ドロップダウン リストで、**[VLAN]** を選択します。

ステップ 5 **[エンドポイント リッスン エンキャップ（End Point Listen Encap）]** テキスト フィールドに、VLAN ID を入力します。有効な値は 1 ～ 4094 です。これは予約済みの VLAN カプセル化である必要があり、どの EPG でも使用できません。

ステップ 6 [送信（Submit）] をクリックします。

IP エージングの設定

このトピックでは、IP エージング ポリシーを有効にする方法について説明します。有効な場合、IP エージング ポリシーは、エンドポイント上の未使用の Ip 5 します。

管理状態が有効になっているときに、IP エージング ポリシーは、エンドポイントの ip アドレスを追跡する (IPv4) の ARP 要求と (IPv6) のネイバー要請を送信します。応答が指定されていない場合、ポリシーは、未使用の IPs 5 します。

手順

ステップ 1 メニュー バーで、**System** > **System Settings** を選択します。

ステップ 2 をクリックして **エンドポイント コントロール** 。

ステップ 3 **Ip Aging** タブをクリックします。

ステップ 4 ポリシーを有効にするにはクリックして **Enabled** で、 **Administrative State** フィールド。

次のタスク

、、エンドポイント上の ip アドレスを追跡するために使用されるタイマーを指定する必要があるエンド ポイント保持ポリシーを作成します。移動 **テナント** > **テナント名** > > **ポリシー** > **プロトコル** > **エンド ポイント保持** 。

リモート エンドポイントの学習を無効にする

このトピックでは、有効化または IP エンド ポイント ラーニングを無効にする方法について説明します。

このポリシーの適用範囲は、ファブリック全体です。を設定した後、ポリシーは起動に各リーフ スイッチにプッシュされます。

Cisco Nexus 9000 シリーズのスイッチで 93128 を含むファブリックでは、このポリシーを有効にする必要がありますが正常に APIC リリース 2.2(2x) にアップグレードされた以降のすべてのノードが表示された後の N9K M12PQ アップリンク モジュール、TX、9396 PX または 9396 TX がスイッチします。

次の設定の変更のいずれか後に、、手動で以前に学習された IP エンドポイントをフラッシュする必要があります。

- リモート IP エンドポイント ラーニングが無効になっています
- 入力ポリシーの適用、VRF が設定されています。
- VRF に少なくとも 1 つのレイヤ 3 インターフェイスが存在します

以前に学習された IP エンドポイントを手動でフラッシュ、VPC ピアの両方で、次のコマンドを入力します: `vsh-c"システム内部 epm エンドポイントの vrf をクリア<vrf-name>リモート「 </vrf-name>`
。

IP エンドポイントの学習を有効または無効にするには、次の手順を実行します:

手順

ステップ 1 メニュー バーで、**[System]** > **[System Settings]** の順にクリックします。
ステップ 2 **[Fabric Wide Setting]** をクリックします。
ステップ 3 チェック ボックスをクリックして **リモート EP 学習の無効化** 。
ステップ 4 [送信（Submit）] をクリックします。

サブネット チェックのグローバルな適用

このトピックでは、サブネット チェックを有効また無効にする方法について説明します。有効にすると、ある VRF で設定されたサブネットの外、つまり他のすべての VRF では、IP 学習が無効になります。

このポリシーの適用範囲は、ファブリック全体です。を設定した後、ポリシーは起動に各リーフ スイッチにプッシュされます。

手順

ステップ 1 メニュー バーで、**[System]** > **[System Settings]** の順にクリックします。
ステップ 2 **[Fabric Wide Setting]** をクリックします。
ステップ 3 **Enforce Subnet Check** チェック ボックスをオンにします。
ステップ 4 [送信（Submit）] をクリックします。

GIPo の再割り当て

このトピックでは、非ストレッチ ブリッジ ドメインの GIPos の再割り当てを有効にして、ストレッチ ブリッジ ドメイン用のスペースを確保する方法について説明します。

Cisco ACI Multi-Site の導入により、GIPo 割り当て方式を変更して次の利点を提供する必要がありました。

1. 同じ GIPo を持つブリッジ ドメインの数を最小限に抑えます。
2. Cisco ACI Multi-Site 拡張ブリッジ ドメインに割り当てられた GIPos は、非拡張ブリッジ ドメインに割り当てられた GIPos と重複しません。

この割り当てを実現するために、Cisco ACI では、ストレッチされたブリッジ ドメインとストレッチされていないブリッジ ドメインの量に基づいてサイズが異なる複数のプールが導入されました。

Cisco ACI の新規インストールの場合、Cisco APIC は #1 と #2 の両方が実行されることを保証します。2.3(1) よりも前のリリースからの Cisco ACI のアップグレード中は、既存の GIPo が非ストレッチ ブリッジ ドメインにすでに使用されている可能性があるため、ファブリックの中断を避けるために古いスキーマが維持されます。その結果、Cisco ACI は #2 が完了したことを保証できません。

Cisco APIC のファブリック全体の設定ポリシーで **[GIPo の再割り当て（Reallocate GIPo）]** ノブを有効にすると、Cisco APIC は GIPos を再割り当てし、新しい割り当て方式を使用します。ノブの有効化は 1 回限りの操作です。その後、GIPos はオーバーラップしません。このノブは、2.3(1) より前のリリースから 3.0(1) 以降のリリースにアップグレードする場合にのみ、Cisco ACI Multi-Site Orchestrator の導入に関連します。

このポリシーの適用範囲は、ファブリック全体です。を設定した後、ポリシーは起動に各リーフ スイッチにプッシュされます。

手順

ステップ 1 メニューバーで、**[システム（System）]**> >**[システム設定（System Settings）]** を選択します。
ステップ 2 [Fabric Wide Setting] をクリックします。
ステップ 3 [Reallocate Gipo] のチェック ボックスをオンにします。
ステップ 4 [送信（Submit）] をクリックします。

ドメインの検証のグローバルな適用

このトピックでは、ドメインの検証を適用する方法について説明します。有効な場合、静的なパスを追加すると、EPGに関連付けられたドメインがないかどうか判断するために、検証チェックが実行されます。

このポリシーの適用範囲は、ファブリック全体です。を設定した後、ポリシーは起動に各リーフ スイッチにプッシュされます。

手順

ステップ 1 メニュー バーで、**[System]** > **[System Settings]** の順にクリックします。
ステップ 2 **[Fabric Wide Setting]** をクリックします。
ステップ 3 **Enforce Domain Validation** チェック ボックスをオンにします。
ステップ 4 [送信（Submit）] をクリックします。

OpFlex クライアント認証を有効にする

このトピックでは、GOLF および Linux 用の OpFlex クライアント認証を有効にする方法について説明します。

クライアントの ID がネットワークによって保証されない環境で GOLF または Linux Opflex クライアントをデプロイするには、クライアント証明書に基づいてクライアントの ID を動的に検証できます。

（注） 証明書の適用を有効にすると、クライアント認証をサポートしていない GOLF または Linux Opflex クライアントとの接続が無効になります。

このポリシーの適用範囲は、ファブリック全体です。を設定した後、ポリシーは起動に各リーフ スイッチにプッシュされます。

手順

ステップ 1 メニュー バーで、**[System]** > **[System Settings]** の順にクリックします。

ステップ 2 **[Fabric Wide Setting]** をクリックします。

ステップ 3 **OpFlex Client Authentication** のチェック ボックスをクリックして、GOLF および Linux Opflex クライアントのクライアント証明書認証を有効または無効にします。

ステップ 4 [送信（Submit）] をクリックします。

ファブリック ロード バランシング

ACI ファブリックでは、利用可能なアップリンク リンク間のトラフィックを平衡化するためのロード バランシング オプションがいくつか提供されます。ここでは、リーフからスパインへのスイッチ トラフィックのロード バランシングについて説明します。

スタティック ハッシュ ロードバランシングは、各フローが 5 タプルのハッシュに基づいてアップリンクに割り当てられるネットワークで使用される従来のロードバランシング機構です。このロードバランシングにより、使用可能なリンクにほぼ均等な流量が分配されます。通常、流量が多いと、流量の均等な分配により帯域幅も均等に分配されます。ただし、いくつかのフローが残りよりも多いと、スタティック ロード バランシングにより完全に最適ではない結果がもたらされる場合があります。

ACI ファブリック ダイナミック ロード バランシング（DLB）は、輻輳レベルに従ってトラフィック割り当てを調整します。DLB では、使用可能なパス間の輻輳が測定され、輻輳状態が最も少ないパスにフローが配置されるので、データが最適またはほぼ最適に配置されます。

DLB は、フローまたはフローレットの粒度を使用して使用可能なアップリンクにトラフィックを配置するように設定できます。フローレットは、時間の大きなギャップによって適切に区切られるフローからのパケットのバーストです。パケットの 2 つのバースト間のアイドル間隔が使用可能なパス間の遅延の最大差より大きい場合、2 番目のバースト（またはフローレット）を 1 つ目とは異なるパスに沿ってパケットのリオーダーなしで送信できます。このアイドル間隔は、フローレット タイマーと呼ばれるタイマーによって測定されます。フローレットにより、パケット リオーダーを引き起こすことなくロードバランシングに対する粒度の高いフローの代替が提供されます。

DLB 動作モードは積極的または保守的です。これらのモードは、フローレット タイマーに使用するタイムアウト値に関係します。アグレッシブ モードのフローレット タイムアウトは比較的小さい値です。この非常に精密なロード バランシングはトラフィックの分配に最適ですが、パケット リオーダーが発生する場合があります。ただし、アプリケーションのパフォーマンスに対する包括的なメリットは、保守的なモードと同等かそれよりも優れています。保守的なモードのフローレット タイムアウトは、パケットが並び替えられないことを保証する大きな値です。新しいフローレットの機会の頻度が少ないので、トレードオフは精度が低いロードバランシングです。DLB は常に最も最適なロード バランシングを提供できるわけではありませんが、スタティック ハッシュ ロード バランシングより劣るということはありません。

（注） すべての Nexus 9000 シリーズ スイッチには DLB のハードウェア サポートがありますが、DLB 機能は、第 2 世代プラットフォーム（EX、FX、および FX2 サフィックスを持つスイッチ）の現在のソフトウェア リリースでは有効になっていません。

ACI ファブリックは、リンクがオフラインまたはオンラインになったことで使用可能なリンク数が変化すると、トラフィックを調整します。ファブリックは、リンクの新しいセットでトラフィックを再分配します。

スタティックまたはダイナミックのロードバランシングのすべてのモードでは、トラフィックは、Equal Cost Multipath (ECMP) の基準を満たすアップリンクまたはパス上でのみ送信され、これらのパスはルーティングの観点から同等で最もコストがかかりません。

ロードバランシング技術ではありませんが、Dynamic Packet Prioritization（DPP）は、スイッチで DLB と同じメカニズムをいくつか使用します。DPP の設定は DLB 専用です。DPP は、長いフローよりも短いフローを優先します。短いフローは約 15 パケット未満です。短いフローは長いフローよりも遅延の影響を受けやすいため、DPP はアプリケーション全体のパフォーマンスを向上させることができます。

すべての DPP 優先トラフィックには、カスタム QoS 設定にもかかわらず CoS 3 がマークされています。

これらのパケットが同じリーフに入力および出力されると、CoS 値が保持され、フレームが CoS3 マーキングを使用してファブリックから送信されます。

GPRS トンネリング プロトコル（GTP）は、主にワイヤレス ネットワークでデータを配信するために使用されます。Cisco Nexus スイッチは Telcom データセンター内の場所です。パケットがデータセンターの Cisco Nexus 9000 スイッチを介して送信される場合、トラフィックは GTP ヘッダーに基づいてロード バランシングされる必要があります。ファブリックがリンク バンドルを介して外部ルータに接続されている場合、トラフィックはすべてのバンドル メンバー（たとえば、レイヤ 2 ポート チャネル、レイヤ 3 ECMP リンク、レイヤ 3 ポート チャネル、およびポート チャネル上の L3Out）に均等に分散される必要があります。）。GTP トラフィックのロード バランシングは、ファブリック内でも実行されます。

GTP ロード バランシングを実現するために、Cisco Nexus 9000 シリーズ スイッチは 5 タプルのロード バランシング メカニズムを使用します。ロードバランシング メカニズムでは、パケットの送信元 IP、宛先 IP、プロトコル、レイヤ 4 リソース、および宛先ポート（トラフィックが TCP または UDP の場合）フィールドが考慮されます。GTP トラフィックの場合は、これらのフィールドへの一意の値の数が限られていると、トンネルでのトラフィック ロードの均等分散が制限されます。

ロード バランシングにおける GTP トラフィックの極性化を回避するために、GTP ヘッダーのトンネル エンドポイント ID（TEID）が UDP ポート番号の代わりに使用されます。TEID がトンネルごとに異なるため、トラフィックをバンドルの複数のリンク間で均等にロードバランシングすることができます。

GTP ロード バランシングは、GTPU パケットに存在する 32 ビット TEID 値で送信元および宛先ポート情報を上書きします。

GTP トンネルのロード バランシング機能により、次のサポートが追加されます。

- 物理インターフェイスでの IPv4/IPv6 トランスポート ヘッダーによる GTP
- UDP ポート 2152 を使用した GTPU

ACI ファブリックのデフォルト設定では、従来の静的なハッシュが使用されます。スタティックなハッシュ機能により、アップリンク間のトラフィックがリーフ スイッチからスパイン スイッチに分配されます。リンクがダウンまたは起動すると、すべてのリンクのトラフィックが新しいアップリンク数に基づいて再分配されます。

リーフ/スパイン スイッチ ダイナミック ロード バランシング アルゴリズム

次の表に、リーフ/スパイン スイッチ ダイナミック ロード バランシングで使用されるデフォルトの設定不可能なアルゴリズムを示します。

表 *1 : ACI* リーフ/スパイン スイッチ ダイナミック ロード バランシング

Traffic Type	データ ポイントのハッシュ
リーフ/スパイン IP ユニキャスト	• 送信元 MAC アドレス • 宛先 MAC アドレス • 送信元 IP アドレス • 宛先 IP アドレス • プロトコル タイプ • 送信元レイヤ 4 ポート • 宛先レイヤ 4 ポート • セグメント ID（VXLAN VNID）または VLAN ID
リーフ/スパイン レイヤ 2	• 送信元 MAC アドレス • 宛先 MAC アドレス • セグメント ID（VXLAN VNID）または VLAN ID

Cisco APIC GUI を使用したロード バランサ ポリシーの作成

このトピックでは、デフォルトのロードバランサーポリシーを構成する方法について説明します。

ロード バランシング ポリシー オプションは、利用可能なアップリンク ポート間でトラフィックのバランスをとります。スタティック ハッシュ ロード バランシングは、各フローが 5 タプルのハッシュに基づいてアップリンクに割り当てられるネットワークで使用される従来のロー

ド バランシング機構です。このロード バランシングにより、使用可能なリンクにほぼ均等な流量が分配されます。通常、流量が多いと、流量の均等な分配により帯域幅も均等に分配されます。ただし、いくつかのフローが残りよりも多いと、スタティック ロード バランシングにより完全に最適ではない結果がもたらされる場合があります。

手順

ステップ 1 メニュー バーで、**[System]** > **[System Settings]** の順にクリックします。

ステップ 2 **[Load Balancer]** をクリックします。

ステップ 3 **[Dynamic Load Balancing Mode]** を選択します。

ダイナミック ロード バランシング (DLB) モードは、輻輳レベルに応じてトラフィックの割り当てを調整します。DLB では、使用可能なパス間の輻輳が測定され、輻輳状態が最も少ないパスにフローが配置されるので、データが最適またはほぼ最適に配置されます。DLB は、フローまたはフローレットの粒度を使用して使用可能なアップリンクにトラフィックを配置するように設定できます。フローレットは、間隔で区切られたフローからのパケットのバーストです。モードは **[Aggressive]**, **[Conservative]**, または **[Off]** (デフォルト)。

ステップ 4 **[オン（On）]** または **[オフ（Off）]**（デフォルト）を選択して、**ダイナミック パケットの優先順位付け**を有効または無効にします。

Dynamic Packet Prioritization (DPP) は、長いフローよりも短いフローを優先します。短いフローは約 15 です。短いフローは、長いフローより遅延に敏感です。DPP により、アプリケーション全体のパフォーマンスが向上します。

ステップ 5 [Load Balancing Mode] を選択します。モードは、**Link Failure** または **Traditional** (デフォルト) です。

ロードバランサーの管理状態。スタティックまたはダイナミックのロードバランシングのすべてのモードでは、トラフィックは、Equal Cost Multipath (ECMP) の基準を満たすアップリンクまたはパス上でのみ送信され、これらのパスはルーティングの観点から同等で最もコストがかかりません。

ステップ 6 [送信（Submit）] をクリックします。

CLI を使用したロード バランサ ポリシーの作成

CLI を使用したダイナミック ロード バランサ ポリシーの作成

ダイナミックアグレッシブ と **ダイナミック保守** の 2 つのダイナミック ロード バランサ モードがあります。**ダイナミックアグレッシブ** モードでは、より短い flowlet タイムアウト間隔が有効になり、**ダイナミック保守**モードでは、より長い flowlet タイムアウト間隔が有効になります。これらのコマンドの詳細については、『*Cisco APIC NX-OS* スタイル *CLI* コマンド資料』を参照してください。

このセクションでは、CLI を使用してダイナミック ロード バランサ ポリシーを設定する方法を示します。

手順

ステップ 1 アグレッシブ モードのダイナミック ロード バランシングを有効にするには、次の手順を実行します。

```
apic1# conf t
apic1# (config)# system dynamic-load-balance mode dynamic-aggressive
```

ステップ 2 保守モードのダイナミック ロード バランシングを有効にするには、次の手順を実行します。

```
apic1# conf t
apic1# (config)# system dynamic-load-balance mode dynamic-conservative
```

CLI を使用したダイナミック パケット優先順位付けポリシーの作成

ここでは、CLI を使用してダイナミック パケットの優先順位付けを有効にする方法を示します。このコマンドの詳細については、『*Cisco APIC NX-OS* スタイル *CLI* コマンド資料』を参照してください。

手順

ダイナミック パケット優位性を有効にします。

```
apic1# conf t
apic1# (config)# system dynamic-load-balance mode packet-prioritization
```

CLI を使用した GTP ロード バランサ ポリシーの作成

このセクションでは、CLI を使用して GTP ロード バランサ ポリシーを作成する方法を示します。このコマンドの詳細については、『*Cisco APIC NX-OS* スタイル *CLI* コマンド資料』を参照してください。

手順

ダイナミック パケット優位性を有効にします。

```
apic1# conf t
apic1# (config)# ip load-sharing address source_destination gtpu
```

REST API を使用したロード バランサ ポリシーの作成

このセクションでは、DLB、DPP、および GTP ロード バランサ ポリシーを有効にする方法を示します。使用可能なすべてのプロパティ値のリストについては、『*Cisco APIC* 管理情報モデル資料』を参照してください。

手順

DLB、DPP、およびGTP ロードバランサポリシーを有効にするには、次の手順を実行します。

```
https://apic-ip-address/api/mo/uni.xml
<polUni>
<fabricInst>
 <lbpPol name="default" hashGtp="yes" pri="on" dlbMode="aggressive">
 </lbpPol>
</fabricInst>
</polUni>
```

時間精度ポリシーの有効化

このトピックでは、ネットワーク上の分散ノードの時間同期プロトコルである Precision Time Protocol (PTP) を有効にする方法について説明します。そのハードウェアのタイムスタンプ機能は、ネットワーク タイム プロトコル（NTP）などの他の時刻同期プロトコルより高い精度を実現します。

PTP は、システムのリアルタイム PTP クロックが相互に同期する方法を指定する分散プロトコルです。これらのクロックは、グランドマスタークロック（階層の最上部にあるクロック）を持つマスター/メンバー同期階層に編成され、システム全体の時間基準を決定します。同期は、タイミング情報を使用して階層のマスターの時刻にクロックを調整するメンバーと、PTP タイミング メッセージを交換することによって実現されます。PTP は、PTP ドメインと呼ばれる論理範囲内で動作します。

手順

ステップ 1 メニュー バーで、**System** > **System Settings** を選択します。

ステップ 2 **Precision Time Protocol** をクリックします。

ステップ 3 **Enabled** または **Disabled** を選択します。

PTP を無効にするように選択した場合は、NTP の時間がファブリックを同期するために使用されます。PTP を有効にすると、サイト全体を同期するためのマスターとしてあるスパインが自動的に選択されます。

ステップ 4 [送信（Submit）] をクリックします。

グローバル システム GIPo ポリシーの有効化

このトピックでは、インフラ テナント GIPo をシステム GIPo として使用する方法について説明します。

ACI マルチポッドを導入するには、239.255.255.240 のシステム グローバル IP アウトサイド (GIPo) を、インターポッド ネットワーク (IPN) 上で、PIM BIDIR の範囲として設定する必要があります。この、IPN デバイス上での 239.255.255.240 PIM BIDIR 範囲の設定は、インフラ GIPo をシステム GIPo として使用することによって回避できます。

始める前に

リーフ スイッチおよびスパイン スイッチを含む、ACI ファブリックのすべてのスイッチを、最新の APIC リリースにアップグレードします。

手順

ステップ 1 メニューバーで、 **System** > **System Settings** の順にクリックします。

ステップ 2 **Enabled** または **Disabled** (デフォルト) を、**Use Infra GIPo as System GIPo** で選択します。

ステップ 3 [送信（Submit）] をクリックします。

ファブリック ポート トラッキング ポリシーの設定

アップリンク障害検出は、ファブリック アクセス ファブリック ポート トラッキング ポリシーで有効にできます。ポート トラッキング ポリシーは、リーフ スイッチとスパイン スイッチ間のリンクの状態を監視します。有効なポート トラッキング ポリシーがトリガーされると、リーフ スイッチは、EPG によって導入されたスイッチ上のすべてのアクセス インターフェイスをダウンさせます。ファブリック ポートトラッキングの詳細については、 *Cisco APIC Layer 2 Networking Configuration Guide*を参照してください。

手順

ステップ 1 メニューバーで、**[システム（System）]**>>**[システム設定（System Settings）]** を選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、**[ポート トラッキング（Port Tracking）]** を選択します。

ステップ 3 **Port tracking state** を **on** に設定して、ポート トラッキングを有効にします。

ステップ 4 （任意） **[毎日の復元タイマー（Daily restore timer）]** の値を変更します。

ステップ 5 **ポート トラッキング パラメータをトリガーするアクティブなスパイン リンク**の数を設定します。

ステップ 6 [送信（Submit）] をクリックします。

グローバル ファブリック アクセス ポリシーのプロビジョニング

グローバル接続可能アクセス エンティティ プロファイルの作成

接続可能エンティティ プロファイル（AEP）は、同様のインフラストラクチャ ポリシー要件を持つ外部エンティティのグループを表します。インフラストラクチャ ポリシーは、Cisco Discovery Protocol（CDP）、Link Layer Discovery Protocol（LLDP）、Link Aggregation Control Protocol（LACP）などのさまざまなプロトコル オプションを設定する物理インターフェイス ポリシーで構成されます。

AEP は、リーフ スイッチで VLAN プールを展開するのに必要です。カプセル化ブロック（および関連 VLAN）は、リーフ スイッチで再利用可能です。AEP は、VLAN プールの範囲を物理インフラストラクチャに暗黙的に提供します。

次の AEP の要件と依存関係は、さまざまな設定シナリオ（ネットワーク接続、VMMドメイン、マルチポッド設定など）でも考慮する必要があります。

- AEP は許容される VLAN の範囲を定義しますが、それらのプロビジョニングは行いません。EPG がポートに展開されていない限り、トラフィックは流れません。AEP で VLAN プールを定義しないと、EPGがプロビジョニングされてもVLANはリーフ ポートでイネーブルになりません。
- リーフ ポートで静的にバインディングしているEPGイベントに基づいて、またはVMware vCenter や Microsoft Azure Service Center Virtual Machine Manager（SCVMM）などの外部コントローラからのVMイベントに基づいて、特定のVLANがリーフ ポート上でプロビジョニングされるかイネーブルになります。
- 添付されているエンティティプロファイルに関連付けられているすべてのポートに関連付けられているアプリケーションEpgを導入するアプリケーションEpgに直接と関連付けることができますプロファイルのエンティティが添付されています。AEPでは、アタッチ可能なエンティティプロファイルに関連付けられているセレクタの一部であるすべてのインターフェイスで導入されている EPG (infraRsFuncToEpg) との関係が含まれている設定可能な一般的な機能 (infraGeneric) があります。

Virtual Machine Manager（VMM）ドメインは、AEP のインターフェイス ポリシー グループから物理インターフェイス ポリシーを自動的に取得します。

始める前に

接続されているエンティティプロファイルに関連付けられるテナント、VRF、アプリケーション プロファイルおよび EPG を作成します。

手順

ステップ 1 メニュー バーで、**Fabric** > **External Access Policies** をクリックします。

ステップ 2 ナビゲーション バーで、**Policies** と **Global** を展開します。

ステップ 3 **[接続可能なアクセス エンティティ プロファイル]** を右クリックして、**[接続可能なアクセス エンティティ プロファイルの作成]** を選択します。

ステップ 4 ポリシーの名前を入力します。

ステップ 5 **[ドメイン]** テーブル上の [+] アイコンをクリックします。

ステップ 6 物理ドメイン、以前に作成した物理、レイヤ 2、レイヤ 3、ファイバ チャネル ドメインを入力するか、新規作成します。

ステップ 7 ドメインのカプセル化を入力して、**[更新]** をクリックします。

ステップ 8 **[EPG 展開]** テーブルの [+] アイコンをクリックします。

ステップ 9 テナント、アプリケーション プロファイル、EPG カプセル化（vlan-1 など）、プライマリ カプセル化（プライマリ カプセル化番号）、インターフェイス モードを入力します（トランク、802.1P またはアクセス（タグなし）。

ステップ 10 **Update** をクリックします。

ステップ 11 [Next] をクリックします。

ステップ 12 接続可能なエンティティ プロファイルに関連付けるインターフェイスを選択します。

ステップ 13 [Finish] をクリックします。

QoS クラスのグローバル ポリシーを設定します。

グローバル QoS クラス ポリシーを使用できます。

- CoS を保持する、CoS 値を保証するために、優先度レベル 802.1 P のパケット数を入力し、ACI ファブリックを通過するが保持されます。802.1 P CoS の保持は単一のポッドおよび multipod トポロジでサポートされます。Multipod トポロジは、CoS の保持を使用できますポッド 1 を入力して、ポッド 2 外からの 802.1 P トラフィックの優先順位の QoS の設定を保持したいですが、CoS の保持を行わない/interpod の DSCP 設定のネットワーク (IPN) トラフィックポッド間。CoS を保持するために multipod トラフィックが通信中、IPN の DSCP 設定を使用して、DSCP ポリシー/(で設定されている **テナント** > **インフラ** > > **ポリシー** > **プロトコル** > **DSCP クラス-cos L3 トラフィックのポリシーの変換**)
- 次のように、デフォルトの QoS クラス レベルのプロパティをリセットします **MTU** 、**キュー制限** 、または **スケジューリング アルゴリズム** 。

手順

ステップ 1 メニュー バーで、**Fabric** > **External Access Policies** をクリックします。

ステップ 2 ナビゲーション バーで、**Policies** と **Global** を展開します。

ステップ 3 **QOS Class** をクリックします。

ステップ 4 CoS 802.1 P の有効化にして、をクリックして、 **保持 COS** チェック ボックス。

ステップ 5 QoS クラスのデフォルト設定を変更するには、それをダブルクリックします。新しい設定を入力し、**Submit** をクリックします。

グローバル DHCP リレー ポリシーの作成

グローバル DHCP リレー ポリシーは、ファブリックの DHCP サーバを識別します。

手順

ステップ 1 メニュー バーで、**Fabric** > **External Access Policies** をクリックします。

ステップ 2 ナビゲーション バーで、**Policies** と **Global** を展開します。

ステップ 3 **DHCP Relay** を右クリックし、**Create DHCP Relay Policy** を選択します。

ステップ 4 [Create DHCP Relay Policy] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、DHCP リレー プロファイル名（DhcpRelayP）を入力します。

この名前では最大 64 文字までの英数字を使用できます。

b) （任意） [説明（Description）] フィールドに、DHCP リレー ポリシーの説明を入力します。

説明には最大 128 文字までの英数字を使用できます。

c) [Providers] を展開します。

[DHCP プロバイダーの作成（Create DHCP Provider）] ダイアログボックスが表示されます。

d) [Create DHCP Provider] ダイアログボックスの [EPG Type] フィールドで、DHCP サーバがどこで接続されているかによって適切なオプション ボタンをクリックします。

選択する EPG タイプのオプションは、EPG タイプによって異なります。

- EPG タイプとして **[アプリケーション EPG（Application EPG）]** を選択すると、次のオプションが **[アプリケーション EPG（Application EPG）]** 領域に表示されます。
  - **[テナント（Tenant）]** フィールドで、ドロップダウン リストから、テナントを選択します。（infra）
  - [Application Profile] フィールドで、ドロップダウン リストから、アプリケーションを選択します。（access）
  - [EPG] フィールドで、ドロップダウン リストから、EPG を選択します。（デフォルト）

- EPG タイプとして **[L2 外部ネットワーク（L2 External Network）]** を選択すると、**[L2 外部ネットワーク領域（L2 External Network）]** に次のオプションが表示されます。
  - **[テナント（Tenant）]** フィールドで、ドロップダウン リストから、テナントを選択します。
  - **[L2 Out]** フィールドで、ドロップダウン リストから [L2 Out] を選択します。
  - **[External Network（外部ネットワーク）]** フィールドで、ドロップダウン リストから外部ネットワークを選択します。
- EPG タイプとして **[L3 外部ネットワーク（L3 External Network）]** を選択すると、**[L3 外部ネットワーク（L3 External Network）]**領域に次のオプションが表示されます。
  - **[テナント（Tenant）]** フィールドで、ドロップダウン リストから、テナントを選択します。
  - **[L3 Out]** フィールドで、ドロップダウン リストから [L3 Out] を選択します。
  - **[External Network（外部ネットワーク）]** フィールドで、ドロップダウン リストから外部ネットワークを選択します。
- EPG タイプとして **[DN]** を選択した場合は、ターゲット エンドポイント グループの識別名を入力します。

e) [DHCP Server Address] フィールドに、インフラ DHCP サーバの IP アドレスを入力します。

（注） インフラ DHCP IP アドレスは、インフラ IP アドレス APIC1 です。vShield コントローラ設定のために展開する場合は、デフォルトの IP アドレス 10.0.0.1 を入力する必要があります。

f) **[DHCP サーバー プレファレンス（DHCP Server Preference）]**フィールドで、このプロバイダーの管理設定値を選択します。

[DHCP サーバー プレファレンス（DHCP Server Preference）] フィールドは、リリース 5.2(4) 以降で使用できます。リーフ スイッチは、このフィールドの値を基に、クライアント VRF またはサーバー VRF のどちらから DHCP リレー パケットをルーティングするかを決定します。詳細については、DHCP サーバー設定フィールドについて （12 ページ） を参照してください。

- **[なし（None）]** : これはデフォルトのオプションで、リリース 5.2(4) より前の動作を反映しています。**[なし（None）]** オプションを選択すると、スイッチは常にクライアント VRF からの DHCP リレー パケットをルーティングします。VRF 間 DHCP リレーに使用する場合、サーバー VRF ネットワークをクライアント VRF にリークするには、共有サービス コントラクトが必要です。
- **[サーバー VRF を使用（Use Server VRF）]** : このオプションは、リリース 5.2(4) で導入された新しい動作を反映しています。**[サーバー VRF を使用（Use Server VRF）]** オプションを選択すると、スイッチは、DHCP クライアントが存在する EPG と DHCP サーバーが存在する EPG（またはDHCP サーバーが到達可能な L3Out のレイヤー 3 外

部）の間にコントラクトがあるかどうかには関わりなく、サーバーVRFからのDHCPリレー パケットをルーティングします。

VRF 間設定の場合、**[サーバー VRF を使用（Use Server VRF）]** オプション（**[DHCP サーバー プリファレンス（DHCP Server Preference）]** フィールド）を選択すると、ルート ルックアップのため、サーバー サブネット ルートは、クライアント リーフ スイッチのサーバ - VRF 内でプログラムされます。クライアント リーフ スイッチの DHCP プロセスは、それ以後、DHCP リレー パケットをサーバー VRF 経由で送信します。このため、サーバー VRF は、クライアント ブリッジ ドメインが展開されているすべてのリーフ スイッチに少なくとも 1 つの IP アドレスを使用して展開する必要があります。

g) [OK] をクリックします。

[**DHCP リレー ポリシーの作成（Create DHCP Relay Policy）]** ウィンドウに戻ります。

h) [Submit] をクリックします。

DHCP リレー ポリシーが作成されます。

グローバル MCP インスタンス ポリシーの有効化にします。

グローバル Mis-Cabling プロトコル (MCP) インスタンス ポリシーを有効にします。現在の実装では、システムで MCP の 1 つだけのインスタンスが実行されます。

手順

ステップ 1 メニュー バーで、**Fabric** > **External Access Policies** をクリックします。

ステップ 2 ナビゲーション バーで、**Policies** と **Global** を展開します。

ステップ 3 をクリックして **MCP インスタンス ポリシーのデフォルト** 。

ステップ 4 **Admin State** を **Enabled** に変更します。

ステップ 5 必要に応じて、ファブリックの他のプロパティを設定します。

ステップ 6 [送信（Submit）] をクリックします。

次のタスク

作成エラーには、回復ポリシーが無効になっています

エラーディセーブル回復ポリシーは、1 つ以上の事前定義されたエラー状態が無効になっていたポートを再度有効にするポリシーを指定します。

手順

ステップ 1 メニュー バーで、**Fabric** > **External Access Policies** をクリックします。
ステップ 2 ナビゲーション バーで、**Policies** と **Global** を展開します。
ステップ 3 をクリックして **エラーには、回復ポリシーが無効になっている** .
ステップ 4 回復ポリシーを有効にするイベントをダブルクリックします。
ステップ 5 チェック ボックスをクリックし、をクリックして **更新** 。
ステップ 6 オプション。その他のイベントについて、ステップ 4 と 5 を繰り返します。
ステップ 7 オプション。リセット、 **エラー復旧間隔 (秒) の無効化** 。
ステップ 8 [送信（Submit）] をクリックします。

ポート単位ポリシー

ポート単位ポリシーについて

ポート単位ポリシーは、Cisco Application Policy Infrastructure Controller（APIC）GUI を使用してリーフ スイッチのインターフェイスを設定するために使用する暗黙的なポリシーです。ポート単位ポリシーは、標準のポリシーベース モデルと比較して単純化されています。これは、Cisco APIC を使用する方法を学習し続けています。この簡素化のため、既存のポリシーに新しいポートを追加することはできません。代わりに、インターフェイスごとにポリシーの新しいチャンクのみを作成できます。

ポート単位のポリシーペインでは、バックグラウンドで NX-OS CLI を使用して、暗黙的および明示的なオブジェクトを作成します。たとえば、新しいポート チャネルを作成すると、明示的なポート チャネルポリシー グループと暗黙的なオーバーライドが作成されます。明示的なポリシー グループへの変更は、暗黙的なポリシー グループが削除されるまでポートに適用されません。CLI と GUI を組み合わせて使用しないことを推奨します。再利用可能なポリシー設定の高度な使用例に移行する場合は、ポート ポリシー ウィザードを使用して Cisco Application Centric Infrastructure（ACI）ポリシー モデルについて学習し、同じウィザードからポートを設定解除します。

ポート単位のポリシーは、次の GUI の場所からのみ作成できます。

[ファブリック（Fabric）] > **[インベントリ（Inventory）]** > ***[Pod-#]*** > ***[leaf-switch-name]*** > **[インターフェイス タブ（Interface）] タブ**

（注） **[インターフェイス（Interface）]** タブは、作業ペインの **[インターフェイス（Interface）]** タブを参照します。これは、ナビゲーション ペインの **[インターフェイス（Interfaces）]** フォルダではありません。

GUI を使用したポート ポリシーごとの設定

この手順では、Cisco Application Policy Infrastructure Controller（APIC）GUI を使用して、ポート ポリシーごとのポリシーを作成します。

手順

ステップ 1 メニュー バーで、**[Fabric]** > **[Inventory]** を選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、***pod-#*** > ***leaf-switch-name*** を選択します。

ステップ 3 [作業（Work）] ペインで、**[インターフェイス（Interface）]** タブを選択します。

ステップ 4 **[モード（Mode）]** ドロップダウン リストで、**[設定（Configuration）]** を選択します。

ステップ 5 インターフェイス番号を 1 つ以上クリックして、それらのインターフェイスを選択します。

[作業（Work）]ペインのタブのすぐ下にあるボタンが、選択したインターフェイスに設定できるコンポーネントでアクティブになります。

ステップ 6 設定するコンポーネントのいずれかのボタンをクリックします。

[作業（Work）] ペインにはそのコンポーネントのプロパティが表示されます。

ステップ 7 コンポーネントのプロパティを必要に応じて設定します。

ステップ 8 **[送信（Submit）]** をクリックします。`

ステップ 9 選択したインターフェイスの追加コンポーネントを設定するか、別のインターフェイスを選択してコンポーネントを設定します。

GUI を使用したポート ポリシーごとの確認

この手順では、Cisco Application Policy Infrastructure Controller（APIC）GUI を使用してポート単位ポリシーを検証する方法について説明します。

始める前に

非表示ポリシーを表示するには、Cisco APIC を設定する必要があります。デフォルトでは、ポート単位のポリシーは Cisco APIC に表示されません。

手順

ステップ 1 メニュー バーで、**[Fabric]** > **[Inventory]** を選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、***pod-#*** > ***leaf-switch-name*** を選択します。

ステップ 3 [作業（Work）] ペインで、**[インターフェイス（Interface）]** タブを選択します。

ステップ 4 **[モード（Mode）]** ドロップダウン リストで、**[設定（Configuration）]** を選択します。

ステップ 5 インターフェイス数を選択する場合は、そのインターフェイス名をクリックします。

[作業（Work）]ペインのタブのすぐ下にあるボタンが、選択したインターフェイスに設定できるコンポーネントでアクティブになります。

ステップ 6 プロパティを表示するコンポーネントのいずれかのボタンをクリックします。

[作業（Work）] ペインに、そのコンポーネントのプロパティが表示されます。

ステップ 7 プロパティが正しく設定されていることを確認し、目的の設定に対して正しくない値を変更します。

ステップ 8 変更を加えた場合は、**[送信（Submit）]** をクリックします。アンインストールしない場合は、[キャンセル（Cancel）] をクリックします。

GUI を使用した非表示ポリシーの表示

デフォルトでは、ポート単位のポリシーなどの一部のポリシーは Cisco Application Policy Infrastructure Controller（APIC）に表示されません。これらのポリシーを表示するには、非表示のポリシーを表示するように Cisco APIC を設定する必要があります。

手順

ステップ 1 GUI の右上隅にある **[マイ プロファイルの管理（Manage My Profile）]** > **[設定（Settings）]** を選択します。

[アプリケーション設定（Application Settings）] ダイアログが開きます。

ステップ 2 **[非表示ポリシーの表示（Show Hidden Policies）]** ボックスにチェックを付けます。

ステップ 3 [OK] をクリックします。

GUI を使用した誤配線プロトコル インターフェイス ポリシーの作成（任意）

誤配線プロトコル（MCP）は、Link Layer Discovery Protocol（LLDP）、スパニング ツリー プロトコル（STP）が検出できない設定ミスを処理するために設計されました。MCP には、それを使用するレイヤ 2 パケットがあり、MCP はファブリック内のループを形成するポートを無効にします。Cisco Application Centric Infrastructure（ACI）ファブリック リーフ スイッチはスパニング ツリー プロトコル（STP）に参加せず、STP に関してハブとして動作します。MCP パケットが送信された後、ファブリックがパケットが戻ったことを確認し、ループが存在することを認識した場合、ファブリックはそのイベントに基づいてアクションを実行します。これが発生するとエラーとイベントが生成されます。MCP は、グローバルに、およびインターフェイスごとに有効にできます。デフォルトでは、MCP がグローバルに無効にされ、各ポートで

有効になっています。MCPが機能するには、インターフェイス単位の設定に関係なく、グローバルに有効にする必要があります。

次の手順では、GUI を使用して MPC インターフェイス ポリシーを作成します。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、**[インターフェイス ポリシー（Interface Policies）]** > **[ポリシー（Policies）]** > **[MCP インターフェイス（MCP Interface）]** の順に選択します。

ステップ 3 [作業（Work）] ペインで、**[アクション（Actions）]** > **[誤配線プロトコル インターフェイス ポリシーの作成（Create Mis-cabling Protocol Interface Policy）]** の順に選択します。

ステップ 4 [Create Mis-cabling Protocol Interface Policy] ダイアログボックスで、次の操作を実行します。

a) ポリシーの名前を入力します。

b) （任意） ポリシーの説明を入力します。

c) [Admin State] に対して、ポリシーを有効にするには [Enable] を選択し、ポリシーを無効にするには [Disable] を選択します。

d) MCP の操作モードとして **[精密（Strict）]** または **[非生命津（Non-strict）]** を選択します。

[精密（Strict）] を選択すると、次の追加フィールドが表示されます。

- **[初期遅延時間（秒）（Initial Delay Time（sec）]**: 外部レイヤ 2 ネットワークでの STP コンバージェンスの時間。デフォルト値は 0 です（レイヤー 2 ネットワークで STP が無効になっている場合）。STP が有効になっている場合、STP が収束するまでの初期遅延時間の範囲は、スケール/トポロジにもよりますが、45 ～ 60 秒です。
- **[送信頻度（秒、ミリ秒）（Tranmission Frequency（sec, msec）]**: 各レイヤ 2 インターフェイスの猶予期間まで、MCPパケットが送信される頻度を決めるタイマー。デフォルトの値は 500 ミリ秒です。
- 猶予期間 (秒、ミリ秒) : 早期ループ検出が行われる猶予期間の時間。ポートは、ループ検出に使用される MCP パケットを積極的に送信します。デフォルトの猶予期間の値は 3 秒です。

ステップ 5 [送信（Submit）] をクリックします。

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。