Cisco APIC システム管理構成ガイド、リリース 5.3(x)

最終更新：2025 年 11 月 5 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/

Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html. Cisco product warranty information is available at https://www.cisco.com/c/en/us/products/warranty-listing.html. US Federal Communications Commission Notices are found here https://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

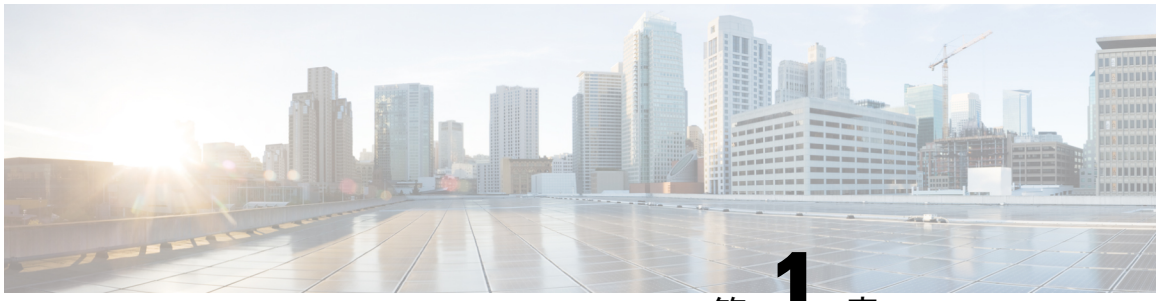
The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners.

Trademarks

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

目 次



第 1 章

新機能および変更された機能に関する情報

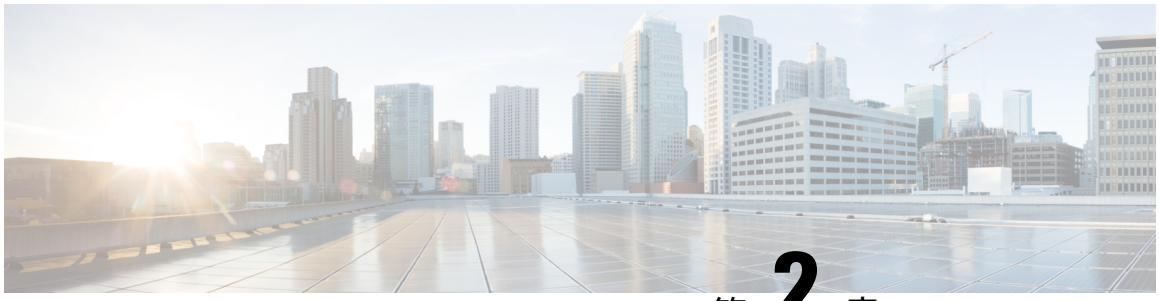
新機能および変更された機能に関する情報

この表は、特定のリリースに至るまでにガイドの編成と特徴に加えられた主な変更点の概要を示しています。ただし、そのリリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

表 *1 : Cisco APIC* リリース *6.1(x)* の新機能および動作変更

機能または変更	説明	参照先
サポートされているハードウェアの変更：新しいスイッチのリーフまたはスパインおよび PTP Telecom プロファイル（G.8275.1）用の N9K-9400-16W	• N9K-X9400-16W は、ACI 6.1(3) リリース以降のファブリック リンクでのみサポートされます。 • PTP Telecom プロファイル（G.8275.1）は、リーフ スイッチとして動作する特定のスイッチで変更されます。	• PTP 向けにサポートされるハードウェア • グランドマスターの展開 • PTP 制限事項

新機能および変更された機能に関する情報



第 2 章

エイリアス、注釈、およびタグ

エイリアス、注釈、およびタグ

オブジェクトの識別、アドレス指定、およびグループ化を簡素化するために、ACIは、ユーザがラベルメタデータをオブジェクトに追加するためのいくつかのメソッドを提供します。これらのメソッドは、以下のリストにまとめられています。

- **[名前エイリアス（Name Alias）]**：GUI エンティティの表面的な代用。
- **[グローバル エイリアス（Global Alias）]**：オブジェクトの識別名（DN）の代わりに使用できる、ファブリック内で一意のラベル。
- **[タグ インスタンス / 注釈（Tag Instance / Annotation）]**：簡単なメモまたは説明。
- **[ポリシー タグ（Policy Tag）]**：オブジェクトをグループ化するためのラベル。同じクラスである必要はありません。

Alias

ACI オブジェクト モデルでは、すべてのオブジェクトに一意の識別名（DN）があります。これは、親オブジェクト階層とそれ自体の名前を含む長い識別子であることがよくあります。たとえば、**aepg35** という名前のアプリケーション エンドポイント グループを含む、**ap13** という名前のアプリケーション プロファイルを含む **Tenant2468** という名前のテナントについて考えてみます。APIC によって生成された、そのアプリケーション エンドポイント グループの DN は次のとおりです。**uni/tn-Tenant2468/ap-ap13/epg-aepg35** これらの各オブジェクトが作成された後、ACIは通常、名前を変更することを許可しません。変更すると、名前が変更されたオブジェクトのすべての子孫オブジェクトのDNが変更されるためです。この不便さを克服するために、ACIは2つのエイリアス関数を提供します。GUI用の名前エイリアスとAPI用のグローバル エイリアスです。

名前エイリアス

名前エイリアス機能（または、設定がGUIに表示される場合は単に「エイリアス」）は、APIC GUIで表示されるオブジェクトの名前を変更します。基になるオブジェクト名は変更できませんが、管理者は、オブジェクト プロパティ メニューの **[エイリアス（Alias）]** フィールドに目的の名前を入力することにより、表示された名前を上書きできます。GUI では、*name_alias (object_name)* として、エイリアス名が括弧内に実際のオブジェクト名とともに表示されます。テナント、アプリケーション プロファイル、ブリッジドメイン、EPG などの多くのオブジェクト タイプは、エイリアス プロパティをサポートします。オブジェクト モデルでは、名前エイリアス プロパティは *objectClass.nameAlias* です。たとえば、テナント オブジェクトのプロパティは `fvTenant.nameAlias` です。

前述のテナントの例を使用して、管理者がテナント名「Tenant2468」ではなく「AcmeManufacturing」を表示したいとします。Tenant2468テナントプロパティの **[エイリアス（Alias）]** フィールドに優先名を入力すると、GUIは **AcmeManufacturing (Tenant2468)** を表示します。

名前エイリアス プロパティは、APIC GUI の単に表面的なものです。エイリアスはどの範囲でも一意である必要はなく、同じ値を他のオブジェクトの名前エイリアスとして使用できます。

グローバルエイリアス

グローバルエイリアス機能により、APIの特定のオブジェクトのクエリが簡素化されます。オブジェクトを照会するときは、固有のオブジェクトID（通常はオブジェクトのDN）を指定する必要があります。別の方法として、この機能を使用すると、ファブリック内で一意のラベルをオブジェクトに割り当てることができます。前の例を使用して、グローバルエイリアスを使用せずに、次の API リクエストを使用して DN でアプリケーション エンドポイントをクエリします。

```
GET: https://APIC_IP/api/mo/uni/tn-Tenant2468/ap-ap13/epg-aepg35.json
```

オブジェクト プロパティ メニューの **[グローバル エイリアス（Global Alias）]** フィールドで、より単純でありながら一意の名前を構成することにより、グローバル エイリアスを別の API コマンドとともに使用して、オブジェクトをクエリできます。

```
GET: https://APIC_IP/api/alias/global_alias.json
```

前の例を使用して、アプリケーション エンドポイント グループの構成プロパティの **[グローバル エイリアス（Global Alias）]** フィールドに「AcmeEPG35」と入力すると、クエリ URL は次のようになります。

```
GET: https://APIC_IP/api/alias/AcmeEPG35.json
```

APIC オブジェクト モデルでは、グローバル エイリアスは、エイリアスされるオブジェクトにアタッチされる子オブジェクト（tagAliasInst）です。前の例では、グローバル エイリアス オブジェクトは、アプリケーション エンドポイント グループ オブジェクトの子オブジェクトになります。

詳細については、『*APIC REST API* 構成ガイド』の「タグとエイリアス」の章を参照してください。

名前エイリアスまたはグローバル エイリアスの作成

この手順例は、テナントのアプリケーション プロファイルの名前エイリアスとグローバル エイリアスを作成する方法を示しています。他の多くのオブジェクトは、オブジェクトに移動した後、同じ手順を使用してこれらのエイリアス機能をサポートします。

手順

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[*tenant_name*]** > **[Application Profiles]** > **[*application_profile_name*]** の順に選択します。

ステップ 3 [Work] ペインで、[Policy] タブをクリックします。

アプリケーション プロファイルの **[プロパティ（Properties）]** ページが表示されます。

ステップ 4 **[エイリアス（Alias）]** フィールドに、エイリアスの名前を入力します。

エイリアスは、どの範囲でも一意である必要はありません。

ステップ 5 **[グローバル エイリアス（Global Alias）]** フィールドに、アプリケーション プロファイルの識別名（DN）のエイリアスを入力します。

グローバル エイリアスは、ファブリック内で一意である必要があります。

ステップ 6 **[送信（Submit）]** をクリックします。

名前エイリアスを構成した場合、アプリケーション プロファイルは**[ナビゲーション（Navigation）]** ペインで *alias*（*name*） として識別されます。たとえば、**[名前（Name）]**が **ap1234** で、**SanJose** として **[エイリアス（Alias）]** を構成した場合、アプリケーション プロファイルは **SanJose**（**ap1234**） として表示されます。

グローバル エイリアスを構成した場合、グローバル エイリアスをサポートする API コマンドで、アプリケーション プロファイルの識別名（DN）をその値に置き換えることができます。

注釈

メタデータの任意のキー：値ペアを注釈としてオブジェクトに追加できます。注釈は、説明、個人的なスクリプトまたはAPI呼び出しのマーカー、または監視ツールやCisco Nexus Dashboard Orchestrator（以前の Cisco Multi-Site Orchestrator（MSO））などのオーケストレーション アプリケーションのフラグなど、ユーザーのカスタム目的のために指定できます。APIC はこれらの注釈を無視し、それらを他のオブジェクト データとともに格納するだけなので、APIC によって課される形式またはコンテンツの制限はありません。

注釈をアタッチする方法は、オブジェクトに注釈を（プロパティとして）直接アタッチする方法と、注釈を子としてアタッチする方法（tagAnnotation）の2つがあります。注釈をオブジェクトに直接アタッチする場合、オブジェクトごとに1つの注釈のみが可能です。より柔軟な、tagAnnotationを使用することをお勧めします。tagAnnotationを使用する場合には、オブジェクトに複数の注釈をアタッチできるからです。

（注） Cisco Nexus Dashboard Orchestrator は直接の注釈を使用します。

注釈の進化

ユーザ定義の注釈情報の APIC サポートは、次の手順で時間の経過とともに変更されました。

- Cisco APIC リリース 4.2(4) より前は、APIC は単純な文字列を格納するタグ インスタンス（tagInst）をサポートしていました。APIC GUI メニューでは、これらは「タグ」としてラベル付けされていました。
- Cisco APICリリース 3.2(1) 以降では、構成可能なオブジェクトのプロパティとして注釈を直接アタッチできます。
- Cisco APIC リリース 4.2(4) では、多くの最新のシステムがキーと値のペアをラベルとして使用しているため、APIのメイン ラベル オプションとして key:value 注釈（tagAnnotation）に移動するように変更が加えられました。タグ インスタンス（**/api/tag/***your_tag***.json**）を介してオブジェクトをクエリするショートカット API は廃止されました。APIC GUI は、「Tags.」というラベルの付いた単純な文字列タグ インスタンス（tagInst）を引き続き使用していました。
- Cisco APIC リリース 5.1(1) では、タグ インスタンス（tagInst）は GUI で廃止されました。GUIメニューでは依然として「タグ」という用語が使用されていましたが、実際には注釈（tagAnnotation）が構成されていました。また、このリリース以降、すべての注釈のリストは、**[ファブリック（Fabric）] > [ファブリック ポリシー（Fabric policies）] > [タグ（Tags）]** から表示できます。
- Cisco APIC リリース 5.2(1) では、GUI メニュー ラベルが「タグ」から「注釈」に変更されました。この変更は、ポリシー タグとの混同を避けるために行われました。

注釈の作成

この手順例は、テナントの注釈を作成する方法を示しています。他の多くのオブジェクトは、オブジェクトに移動した後、同じ手順を使用して注釈機能をサポートします。

手順

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、***tenant_name*** を選択します。

ステップ 3 [Work] ペインで、[Policy] タブをクリックします。

テナントのプロパティメニューが表示されます。

ステップ 4 **[注釈（Annotations）]** の横にある **[+]** 記号をクリックして、新しい注釈を追加します。

ステップ 5 注釈キー ボックスで、既存のキーを選択するか、新しいキーを入力します。

ステップ 6 注釈値ボックスに値を入力します。

キーと値に使用できる英数字と記号は、a～z、A～Z、0～9、ピリオド、コロン、ダッシュ、またはアンダースコアです。

ステップ 7 ✓ 記号をクリックして注釈を保存します。

この手順を繰り返すと、注釈を追加できます。

ポリシー タグ

ポリシー タグ（`tagTag`）、または単にタグは、ACI 機能で使用するためのユーザ定義可能なキーと値のペアです。1 つのオブジェクトに複数のタグを構成でき、複数のオブジェクトに同じタグを適用できます。多くのオブジェクトクラスがポリシータグをサポートしているため、ポリシー タグを使用して異なるオブジェクトをグループ化できます。たとえば、ポリシー タグを使用して、Cisco APIC リリース 5.2(1) の ESG タグ セレクターを使用して、エンドポイント、サブネット、および VM を 1 つのエンドポイント セキュリティ グループ（ESG）としてグループ化できます。

ポリシー タグを使用する ACI 機能には次のものがあります。

- エンドポイントセキュリティ グループ（ESG）

ポリシー タグの作成

この手順例は、静的エンドポイントのポリシータグを作成する方法を示しています。他のいくつかのオブジェクトは、オブジェクトに移動した後、同じ手順を使用してポリシー タグをサポートします。

手順

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > **[*application_profile_name*]** > **[アプリケーション EPG（Application EPGs）]** > **[*application_epg_name*]** > **[静的エンドポイント（Static Endpoint）]** の順に展開します。

ステップ 3 **[作業（Work）]** ペインで、タグ付けする静的エンドポイントをダブルクリックします。

[静的エンドポイント プロパティ（Static Endpoint properties）] ダイアログボックスが表示されます。

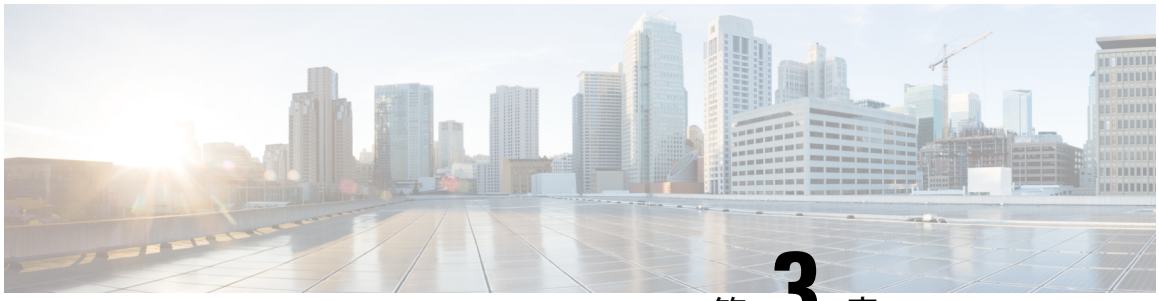
ステップ 4 **[ポリシー タグ（Policy Tags）]** の横にある **[+]** 記号をクリックして、新しいポリシー タグを追加します。

ステップ 5 タグ キー ボックスで、既存のキーを選択するか、新しいキーを入力します。

ステップ 6 タグ値ボックスにタグ値を入力します。

キーと値に使用できる英数字と記号は、a～z、A～Z、0～9、ピリオド、コロン、ダッシュ、またはアンダースコアです。

ステップ 7 ✓ 記号をクリックしてタグを保存します。



第 3 章

高精度時間プロトコル

PTP について

高精度時間プロトコル（PTP）は、ネットワークに分散したノード間で時刻同期を行うプロトコルで、IEEE 1588 に定義されています。PTP を使用すると、イーサネット ネットワークを介して 1 マイクロ秒未満の精度で、分散したクロックを同期できます。PTP の正確さは、Cisco Application Centric Infrastructure（ACI）ファブリック スパインおよびリーフスイッチでの PTP のハードウェア サポートによるものです。ハードウェア サポートにより、プロトコルはメッセージの遅延とネットワーク全体の変動を正確に補正できます。

（注） このドキュメントでは、IEEE1588-2008 標準規格が「スレーブ」と呼称するものに対して「クライアント」という用語を使用しています。例外は、Cisco Application Policy Infrastructure Controller（APIC）CLI コマンドまたは GUI に「スレーブ」という単語が埋め込まれている場合です。

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）を持つマスタークライアント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。

PTP プロセスは、マスタークライアント階層の確立とクロックの同期の 2 つのフェーズで構成されます。PTP ドメイン内では、オーディナリ クロックまたは境界クロックの各ポートが、次のプロセスを使用してステートを決定します。

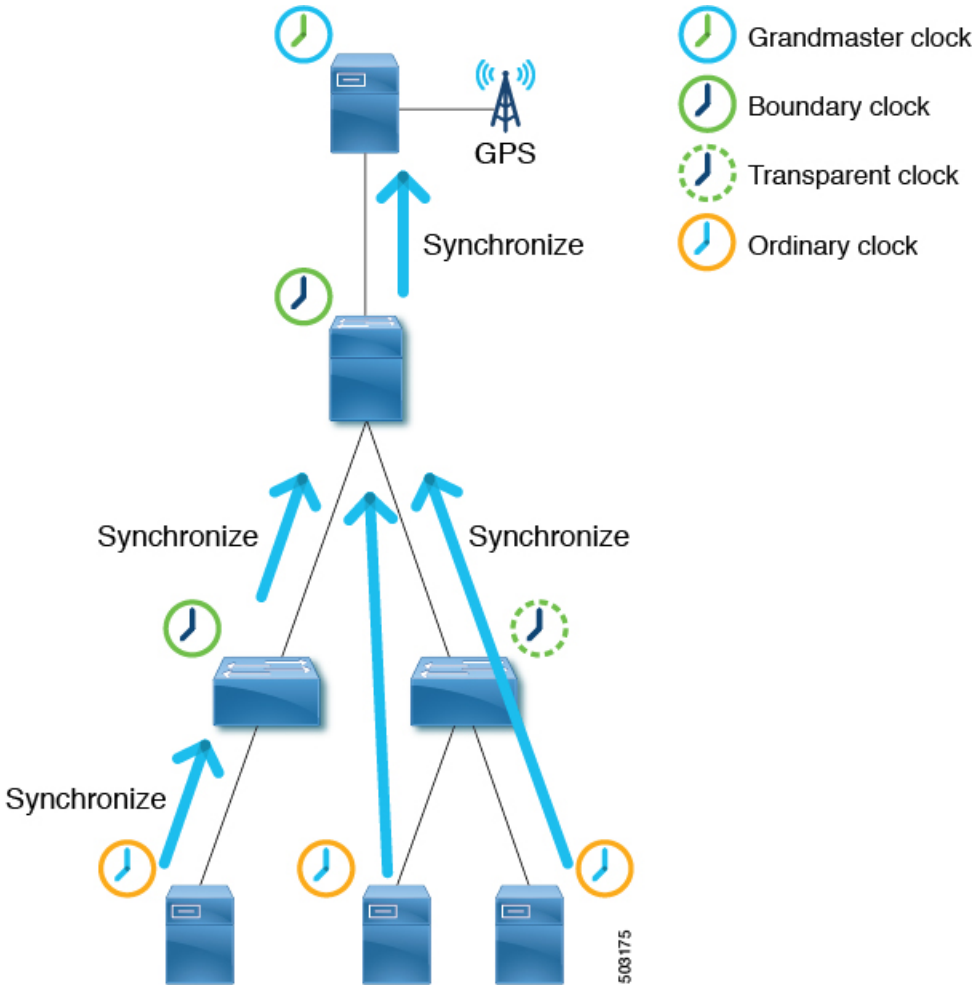
1. ベスト マスター クロック アルゴリズム（BMCA）を使用してマスター クライアント階層を確立します。

- 受信したすべての（マスター ステートのポートによって発行された）Announce メッセージの内容を検査します。
- 外部マスターのデータ セット（Announce メッセージ内）とローカル クロックで、優先順位、クロック クラス、正確度などを比較します。
- 自身のステートがマスターまたはクライアントのいずれであるかを決定します。

2. クロックの同期：
   - Sync や Delay_Req などのメッセージを使用して、マスターとクライアント間のクロックを同期します。

PTP クロック タイプ

次の図は、PTP クロック タイプの階層を示しています。

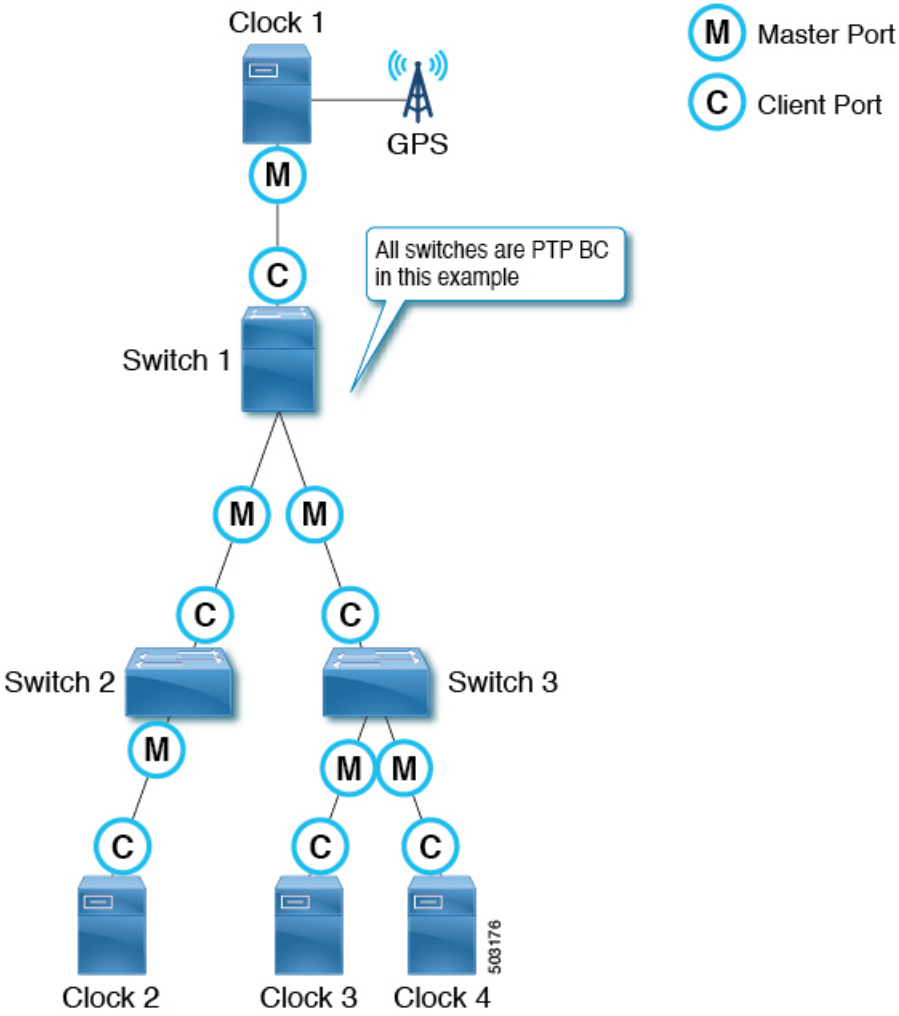


PTP には、次のクロック タイプがあります。

タイプ	説明
グランドマスタークロック（GM、GMC）	PTP トポロジ全体の時間のソース。グランドマスター クロックは、Best Master Clock Algorithm（BMCA）によって選択されます。
境界クロック(BC)	複数の PTP ポートを持つデバイス。PTP 境界クロックは BMCA に参加し、各ポートにはマスターまたはクライアントなどのステータスがあります。境界クロックはその親/マスターと同期するため、それ自体の背後にあるクライアント クロックは PTP 境界クロック自体に同期します。これを確実にするために、境界クロックは PTP メッセージを終了し、メッセージを転送する代わりにそれ自体で応答します。これにより、あるポートから別のポートに PTP メッセージを転送するノードによって引き起こされる遅延がなくなります。
トランスペアレントクロック（TC）	複数の PTP ポートを持つデバイス。PTP トランスペアレント クロックは BMCA に参加しません。このクロック タイプは、マスター クロックとクライアント クロックの間で PTP メッセージを透過的に転送するだけなので、それらが相互に直接同期できます。トランスペアレント クロックは、通過する PTP メッセージに滞留時間を付加するため、クライアントはトランスペアレント クロック デバイス内の転送遅延を考慮することができます。 ピアツーピア遅延メカニズムの場合、PTP トランスペアレント クロックは、メッセージを転送する代わりに PTP Pdelay_xxx メッセージを終了します。 （注） この ACI モードのスイッチは、トランスペアレント クロックにすることはできません。
オーディナリ クロック（OC）	グランドマスター クロックとして時間のソースとして機能するデバイス、またはクライアント（PTP クライアント）としての役割を持つ別のクロック（マスターなど）に同期するデバイス。

PTP トポロジ

マスター ポートとクライアント ポート



マスター ポートとクライアント ポートは次のように機能します。

- 各 PTP ノードは、GPS（図のクロック 1）などの最適な時刻ソースを持つグランドマスター クロックにクロックを直接または間接的に同期します。
- ベストマスタークロック アルゴリズム（BMCA）に基づいて、PTP トポロジ（ドメイン）全体に対して 1 つのグランドマスターが選択されます。BMCA は各 PTP ノードで個別に計算されますが、アルゴリズムにより、同じドメイン内のすべてのノードがグランドマスターと同じクロックを選択するようになります。
- BMCA に基づく PTP ノード間の各パスには、1 つのマスター ポートと少なくとも 1 つのクライアント ポートがあります。パスがポイントツーマルチポイントの場合、複数のクライアント ポートがありますが、各 PTP ノードは 1 つのクライアント ポートしか持つこと

ができません。各 PTP ノードは、クライアント ポートを使用して、もう一方の端のマスター ポートと同期します。これを繰り返すことにより、すべての PTP ノードは最終的に直接または間接的にグランドマスターに同期します。

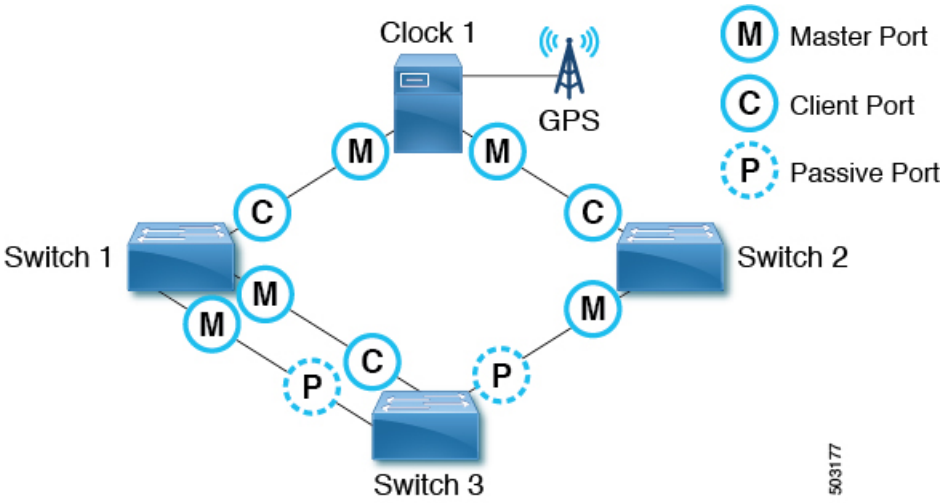
- スイッチ 1 から見ると、クロック 1 はマスターであり、グランドマスターです。
- スイッチ 2 から見ると、スイッチ 1 がマスターであり、クロック 1 がグランドマスターです。

- 各 PTP ノードにはクライアント ポートが 1 つだけあり、その背後にグランドマスターが存在します。グランドマスターは、数ホップ離れている場合があります。
- 例外は、BMCA に参加しない PTP トランスペアレント クロックです。スイッチ 3 が PTP トランスペアレント クロックの場合、クロックにはマスターやクライアントなどのポート ステータスがありません。クロック 3、クロック 4、およびスイッチ 1 は、マスターとクライアントの関係を直接確立します。

パッシブ ポート

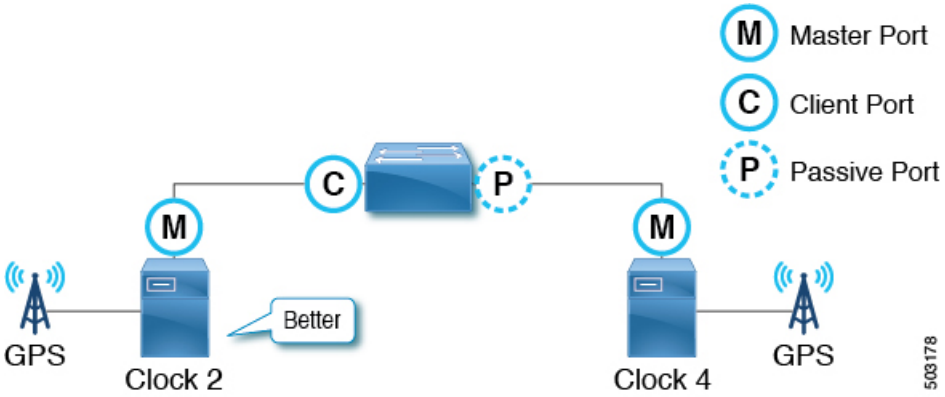
BMCA は、マスターとクライアントの上でパッシブ状態にある別の PTP ポートを選択できます。パッシブ ポートは、他のノードからの `Management` メッセージへの応答としての PTP `Management` メッセージなどのいくつかの例外を除いて、PTP メッセージを生成しません。

例 1



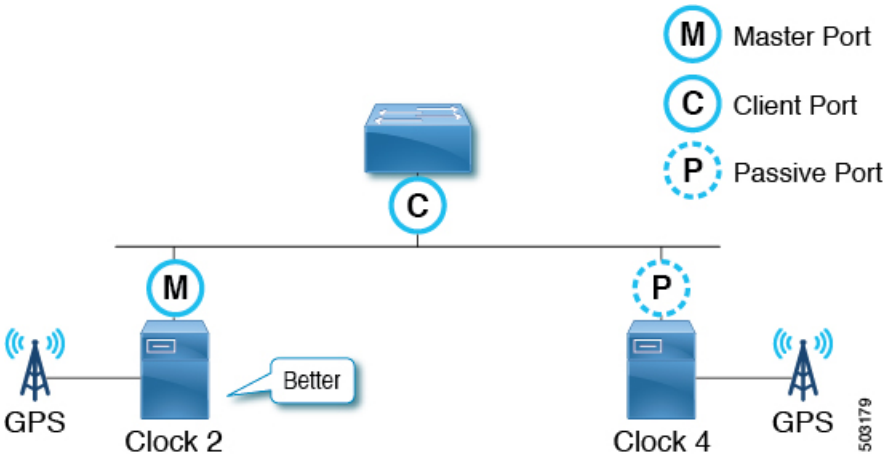
PTP ノードにグランドマスターへの複数のポートがある場合、そのうちの 1 つだけがクライアント ポートになります。グランドマスターへの他のポートはパッシブ ポートになります。

例 2



PTP ノードが 2 つのマスター専用クロック（グランドマスター候補）を検出した場合、グランドマスターとして選択された候補へのポートはクライアント ポートになり、もう一方はパッシブ ポートになります。他のクロックがクライアントである場合、パッシブではなくマスターとクライアントの関係を形成します。

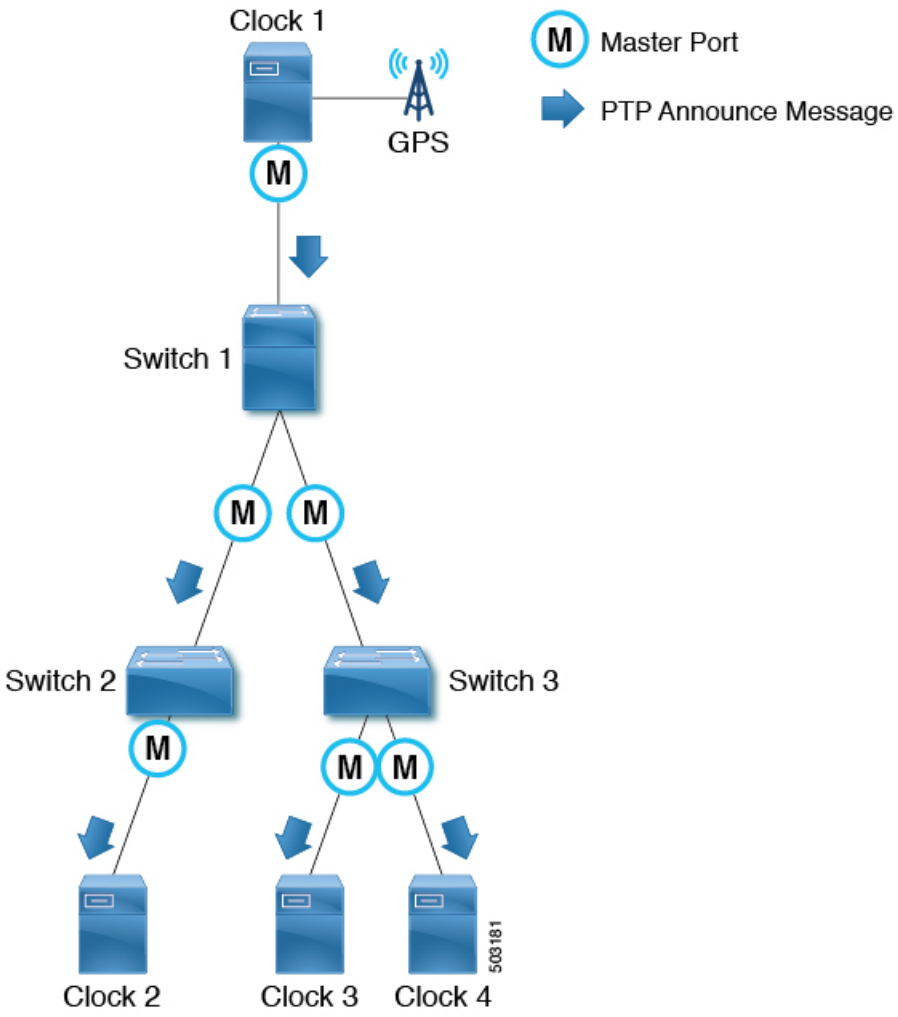
例 3



マスター専用クロック（グランドマスター候補）が、それ自体よりも優れた別のマスター専用クロックを検出すると、そのクロックはそれ自体を受動状態にします。これは、2 つのグランドマスター候補が同じ通信パス上にあり、間に PTP 境界クロックがない場合に発生します。

アナウンス メッセージ

Announce メッセージは、ベスト マスター クロック アルゴリズム（BMCA）を計算し、PTP トポロジ（マスター クライアント階層）を確立するために使用されます。



メッセージは次のように機能します。

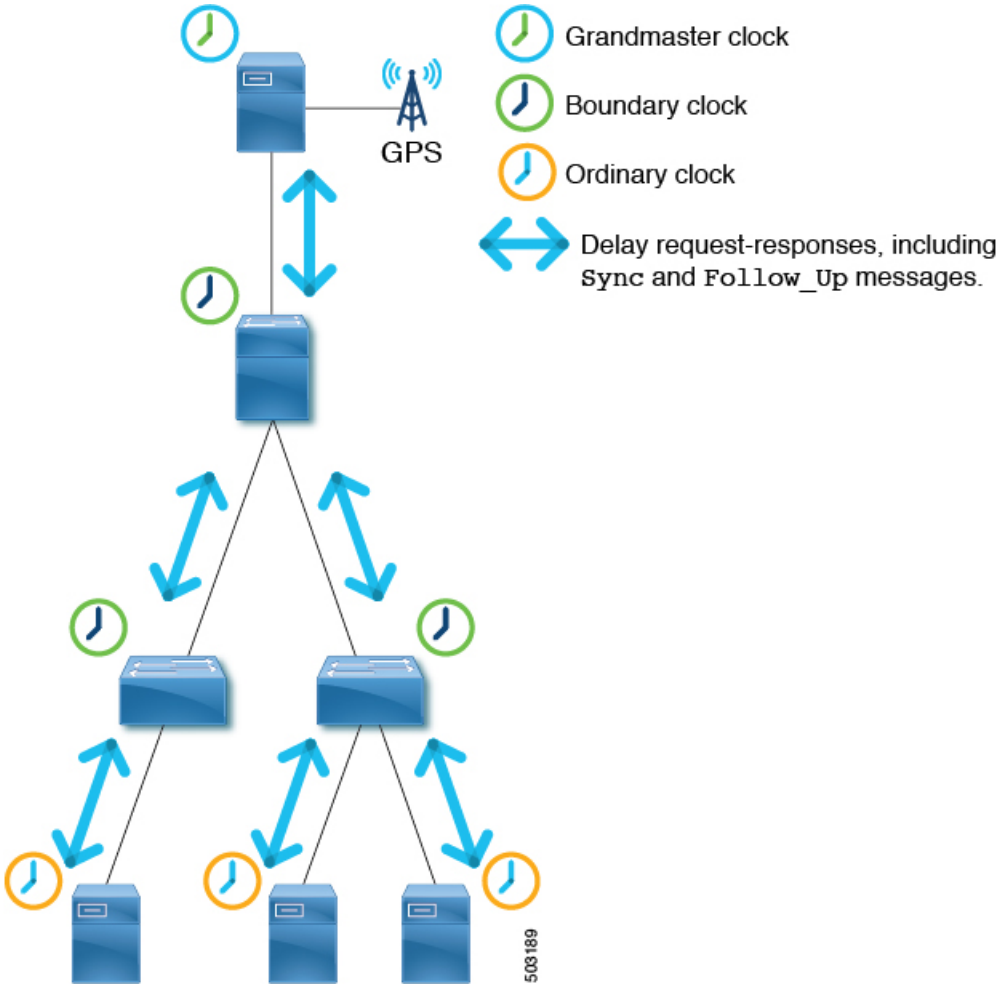
- PTP マスター ポートは、PTP over IPv4 UDP の場合、PTP `Announce` メッセージを IP アドレス 224.0.1.129 に送信します。
- 各ノードは、PTP `Announce` メッセージの情報を使用して、BMCA に基づいて同期階層（マスター/クライアント関係またはパッシブ）を自動的に確立します。
- PTP `Announce` メッセージに含まれる情報の一部は次のとおりです。
  - グランドマスター優先順位 1
  - グランドマスター クロックの品質（クラス、正確度、バリアンス）
  - グランドマスター優先順位 2
  - グランドマスター アイデンティティ
  - 削除されるステップ

• PTP Announce メッセージは、2 logAnnounceInterval 秒に基づく間隔で送信されます。

さまざまな PTP ノード タイプを持つ PTP トポロジ

エンドツーエンド境界クロックのみを持つ PTP トポロジ

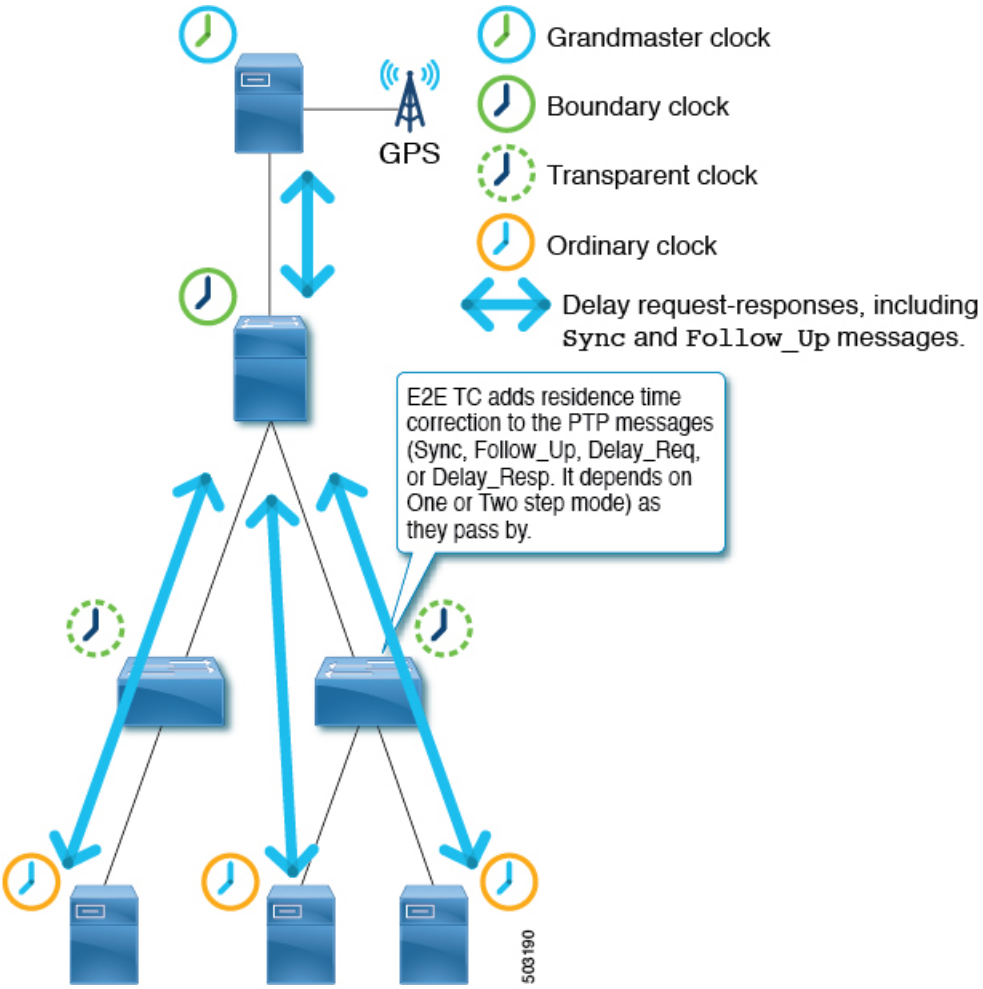
このトポロジでは、境界クロック ノードは、 Management メッセージを除き、すべてのマルチキャスト PTP メッセージを終了させます。



これにより、各ノードが最も近い親マスター クロックからの Sync メッセージを処理するようになり、ノードが高い精度を達成できるようになります。

境界クロックとエンドツーエンドの透過クロックを使用した PTP トポロジ

このトポロジでは、境界クロック ノードは、 Management メッセージを除き、すべてのマルチキャスト PTP メッセージを終了させます。



エンドツーエンド（E2E）透過クロックノードはPTPメッセージを終了しませんが、パケットが通過するときに、滞留時間（パケットがノードを通過するのにかかった時間）を PTP メッセージ修正フィールドに追加するだけです。それらを使用して、より良い正確度を達成します。ただし、これは、1つの境界クロックノードで処理する必要がある PTP メッセージの数が増えるため、拡張性が低くなります。

PTP BMCA

PTP BMCA パラメータ

各クロックには、ベストマスタークロックアルゴリズム（BMCA）で使用される IEEE 1588-2008 で定義されている次のパラメータがあります。

[順序（Order）]	パラメータ	使用可能な値	説明
1	優先順位 1	0 ～ 255	ユーザ構成可能な番号。この値は、通常、グランドマスター候補クロック（マスター対応デバイス）の場合は 128 以下、クライアント専用デバイスの場合は 255 です。
2	クロック品質 - クラス	0 ～ 255	クロック デバイスのステータスを表示します。たとえば、6 は GPS などのプライマリ リファレンス時間ソースを持つデバイス用です。7はプライマリ リファレンス時間ソースを持つように使用されるデバイス用です。127 以下は、マスター専用クロック（グランドマスター候補）用です。255はクライアント専用デバイス用です。
3	クロック品質 - 正確度	0 ～ 255	クロックの正確度。たとえば、33（0x21）は100 ns以下で、35（0x23）は 1 us 以下です。
4	クロック品質 - バリアンス	0 ～ 65535	PTP メッセージ内でのタイムスタンプのカプセル化の精度。
5	優先順位 2	0 ～ 255	ユーザ構成可能な別の番号。同一のクロック品質を持つ 2 つのグランドマスター候補で、そのうち 1 つはスタンバイであるセットアップの場合、このパラメータが通常使用されます。
6	クロック ID	この値は 8 バイトで、通常は MAC アドレスを使用して形成されます。	このパラメータは最終的なタイ ブレーカーとして機能し、通常はMAC アドレスです。

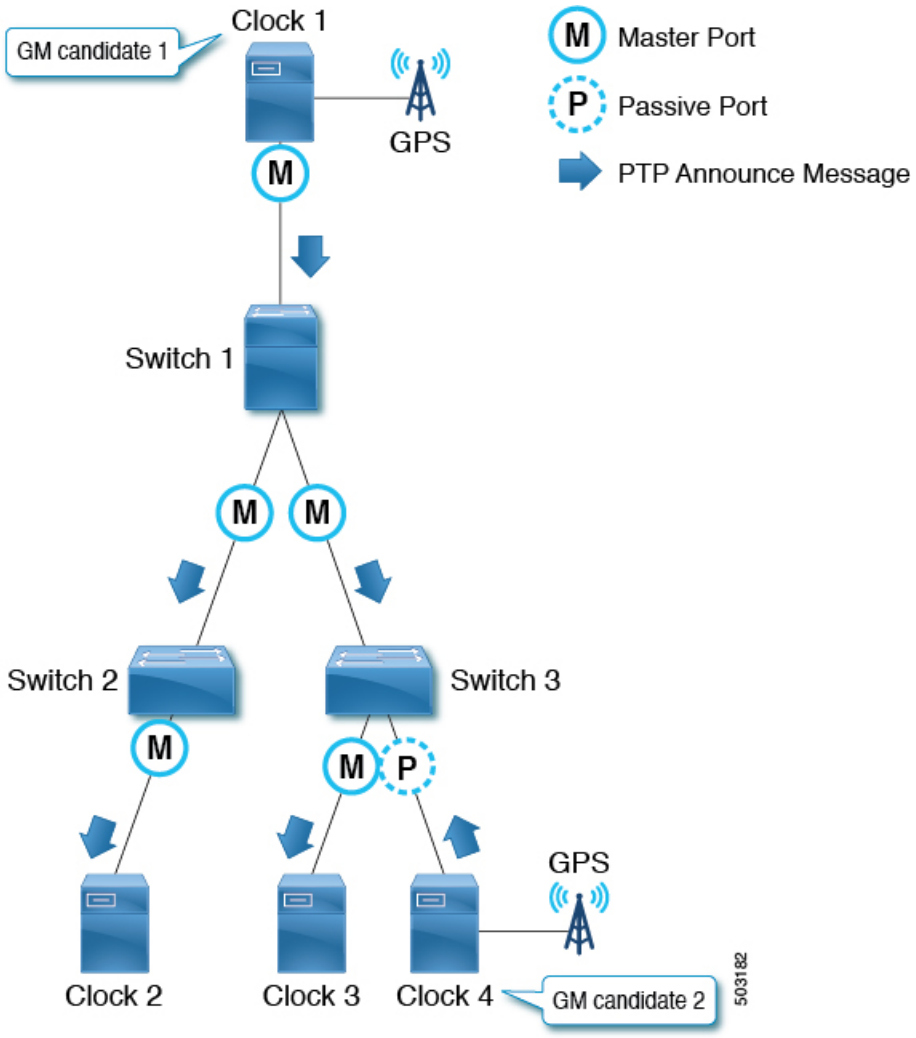
[順序（Order）]	パラメータ	使用可能な値	説明
7	削除されるステップ	設定不能	このパラメータは、2つの異なるポートからの同一のグランドマスターのクロックを受信したときのアナウンス済みクロックからのホップ数を表し、最終的なタイ ブレーカーです。削除されるステップが候補と同一の場合、ポート ID と番号はタイ ブレーカーとして使用されます。 このパラメータの値を構成することはできません。

グランドマスター クロックのこれらのパラメータは、PTP Announce メッセージによって運ばれます。各 PTP ノードは、ノードが受信するすべての Announce メッセージから受け取る表にリストされている順番、またそのノード自体の値の順番で、これらの値を比較します。すべてのパラメータで、より低い番号が選択されます。その後、各 PTP ノードはノードが認識するパラメータのうちのベスト クロックを持つパラメータを使用して Announce メッセージを作成し、ノードは自身のマスター ポートから次のクライアントデバイスにメッセージを送信します。

（注） 各パラメータの詳細については、IEEE 1588-2008 の 7.6 節を参照してください。

PTP BMCA の例

次の例では、クロック 1 とクロック 4 がこの PTP ドメインのグランドマスター候補です。



クロック 1 には、次のパラメータ値があります。

パラメータ	値
優先順位 1	127
クロック品質 - クラス	6
クロック品質 - 正確度	0x21（< 100ns）
クロック品質 - バリアンス	15652
優先順位 2	128
クロック ID	0000.1111.1111
削除されるステップ	*

クロック 4 には、次のパラメータ値があります。

パラメータ	値
優先順位 1	127
クロック品質 - クラス	6
クロック品質 - 正確度	0x21（< 100ns）
クロック品質 - バリアンス	15652
優先順位 2	129
クロック ID	0000.1111.2222
削除されるステップ	*

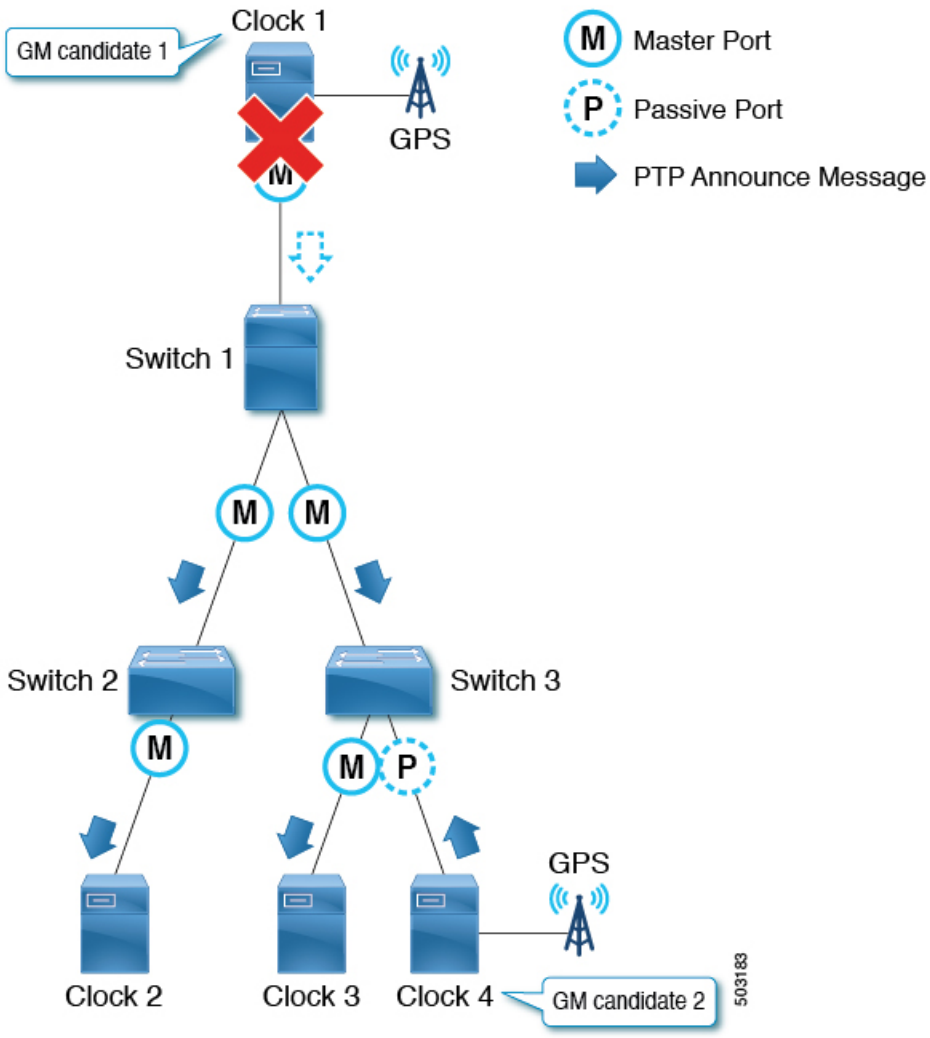
両方のクロックが PTP `Announce` メッセージを送信し、各 PTP ノードがメッセージ内の値を比較します。この例では、最初の 4 つのパラメータの値が同じであるため、`Priority 2` がアクティブなグランドマスター、つまりクロック 1 を決定します。

すべてのスイッチ（1、2、および 3）がクロック 1 が最良のマスター クロック（つまり、クロック 1 がグランドマスター）であることを認識した後、これらのスイッチは、マスター ポートからクロック 1 のパラメータを含む PTP `Announce` メッセージを送信します。スイッチ 3 では、クロック 4（グランドマスター候補）に接続されたポートがパッシブ ポートになります。これは、ポートがマスター専用クロック（クラス 6）からの PTP `Announce` メッセージを受信し、別のポートから受信されている現在のグランドマスターよりも優れていないパラメータを持つためです。

`Step Removed` パラメータは、グランドマスターからのホップ（PTP 境界クロック ノード）の数を示します。PTP 境界クロック ノードが PTP `Announce` メッセージを送信すると、メッセージ内の `Step Removed` 値が 1 ずつ増分します。この例では、スイッチ 2 は、クロック 1 のパラメータで `Step Removed` 値が `1` のスイッチ 1 から PTP `Announce` メッセージを受信します。クロック 2 は、`Step Removed` 値が `2` の PTP `Announce` メッセージを受信します。この値は、PTP `Announce` メッセージの他のすべてのパラメータが同じ場合にのみ使用されます。これは、メッセージが同じグランドマスター候補クロックからのものである場合に発生します。

PTP BMCA フェールオーバー

現在アクティブなグランドマスター（クロック 1）が使用できなくなった場合、各 PTP ポートはベスト マスター クロック アルゴリズム（BMCA）を再計算します。



可用性は、Announce メッセージを使用してチェックされます。各 PTP ポートは、Announce メッセージが Announce Receipt Timeout 時間を連続して欠落した後に、Announce メッセージのタイムアウトを宣言します。つまり、Announce Receipt Timeout x $2^{logAnnounceInterval}$ 秒の場合です。このタイムアウト期間は、IEEE 1588-2008 の 7.7.3 節で説明されているように、PTP ドメイン全体で均一である必要があります。タイムアウトが検出されると、各スイッチは、新しい最良のマスター クロック データを含む Announce メッセージを送信することにより、すべての PTP ポートで BMCA の再計算を開始します。ほとんどのスイッチは前のグランドマスターのみを認識しているため、再計算により、スイッチは最初にスイッチ自体が最良のマスタークロックであると判断する可能性があります。

グランドマスターに接続されたクライアント ポートがダウンした場合、ノード（またはポート）は、アナウンス タイムアウトを待つ必要がなく、新しい最良のマスター クロック データを含む Announce メッセージを送信することにより、BMCA の再計算をすぐに開始できます。

トポロジのサイズによっては、収束に数秒以上かかる場合があります。これは、各 PTP ポートが BMCA を最初から個別に再計算して新しい最適なクロックを見つけるためです。アクティ

ブなグランドマスターに障害が発生する前は、スイッチ 3 だけがクロック 4 を認識しており、アクティブなグランドマスターの役割を引き継ぐ必要があります。

また、ポートの状態が非マスターからマスターに変化した場合、ポートは最初に PRE_MASTER の状態に変化します。ポートが実際のマスターになるまでの Qualification Timeout 秒数は、通常は次のようになります。

```
(Step Removed + 1) x the announce interval
```

これは、他のグランドマスター候補がアクティブなグランドマスターと同じ（または近くに）接続されている場合、ポート ステータスの変更が最小限になり、コンバージェンス時間が短くなることを意味します。詳細については、IEEE 1588-2008 の 9.2 節を参照してください。

PTP 代替 BMCA（G.8275.1）

PTP テレコム プロファイル（G.8275.1）は、G.8275.1 で定義された代替のベスト マスター クロック アルゴリズム（BMCA）を使用します。これには、IEEE 1588-2008 で定義された通常の BMCA とは異なるアルゴリズムがあります。最大の違いの 1 つは、同じ品質のグランドマスター候補が 2 つある場合、G.8275.1 の代替 BMCA により、Clock Identity より前に Steps Removed を比較することで、すべての PTP ノードがグランドマスターと同じクロックを選択するのではなく、各 PTP ノードが最も近いグランドマスターを選択できることです。もう 1 つの違いは、新しいパラメータ Local Priority です。これにより、ユーザは、どのポートをクライアント ポートとして優先するかを手動で制御できます。これにより、各ノードの PTP テレコム プロファイルと SyncE の両方の送信元として同じポートを選択することが容易になります。これは、多くの場合、ハイブリッド モードの操作に適しています。

PTP 代替 BMCA パラメータ

各クロックには、PTP テレコム プロファイル（G.8275.1）の代替ベスト マスター クロック アルゴリズム（BMCA）で使用される G.8275.1 で定義された次のパラメータがあります。

[順序（Order）]	パラメータ	使用可能な値	説明
1	クロック品質 - クラス	0 ～ 255	クロック デバイスのステータスを表示します。たとえば、6 は GPS などのプライマリ リファレンス時間ソースを持つデバイス用です。7はプライマリ リファレンス時間ソースを持つように使用されるデバイス用です。127 以下は、マスター専用クロック（グランドマスター候補）用です。255はクライアント専用デバイス用です。
2	クロック品質 - 正確度	0 ～ 255	クロックの正確度。たとえば、33（0x21）は 100 ns 以下で、35（0x23）は 1 us 以下です。

[順序（Order）]	パラメータ	使用可能な値	説明
3	クロック品質 - バリアンス	0 ～ 65535	PTP メッセージ内でのタイムスタンプのカプセル化の精度。
4	優先順位 2	0 ～ 255	ユーザ構成可能な番号。同一のクロック品質を持つ2つのグランドマスター候補で、そのうち 1 つはスタンバイであるセットアップの場合、このパラメータが通常使用されます。
5	ローカル優先度	1 ～ 255	ノード自体のクロックは、ノードで構成されたクロック ローカル優先順位を使用します。別のノードから受信したクロックには、着信ポートに構成されたローカル優先順位が与えられます。
6	削除されるステップ	設定不能	このパラメータは、通知されたクロックからのホップ数を表します。これを比較することで、アクティブなグランドマスター候補が複数ある場合に、各テレコム境界クロックを、より近くにある別のグランドマスターと同期させることができます。削除されるステップが候補と同一の場合、ポート ID と番号はタイ ブレーカーとして使用されます。 この比較は、`Clock Quality - Class` 値が 127 以下の場合にのみ実行されます。これは、クロックがグランドマスター候補であることを示します。
7	クロック ID	この値は 8 バイトで、通常は MAC アドレスを使用して形成されます。	このパラメータは、`Clock Quality - Class` 値が 127 より大きい場合にタイブレーカーとして機能します。これは、クロックの品質がグランドマスターとして設計されていないことを示します。値は通常、MACアドレスです。

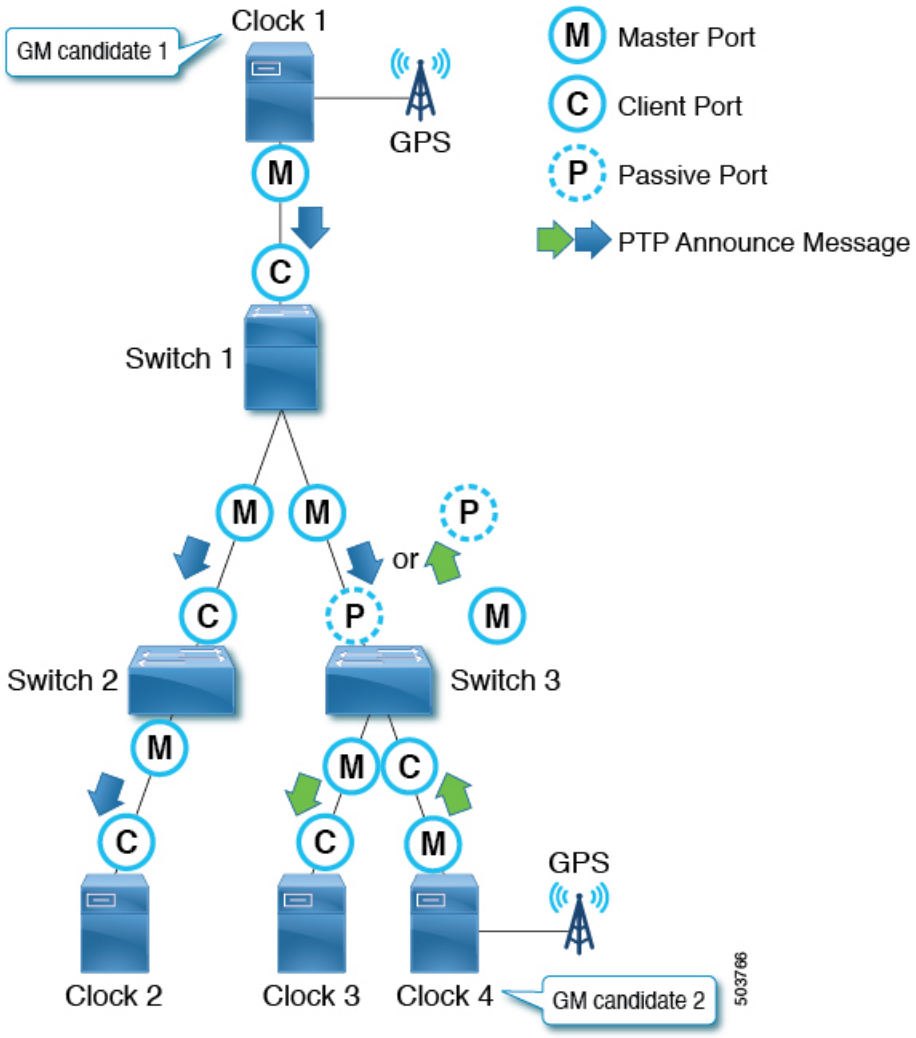
[順序（Order）]	パラメータ	使用可能な値	説明
8	削除されるステップ	設定不能	このパラメータは、2つの異なるポートからの同一のグランドマスターのクロックを受信したときのアナウンス済みクロックからのホップ数を表し、最終的なタイ ブレーカーです。削除されるステップが候補と同一の場合、ポートIDと番号はタイ ブレーカーとして使用されます。

グランドマスター クロックのこれらのパラメータは、`Local Priority` を除き、PTP `Announce` メッセージによって運ばれます。各 PTP ノードは、ノードが受信するすべての `Announce` メッセージから受け取る表にリストされている順番、またそのノード自体の値の順番で、これらの値を比較します。すべてのパラメータで、より低い番号が選択されます。その後、各PTPノードはノードが認識するパラメータのうちのベストクロックを持つパラメータを使用して`Announce` メッセージを作成し、ノードは自身のマスター ポートから次のクライアントデバイスにメッセージを送信します。

（注） 各パラメータの詳細については、G.8275.1 の 6.3 節を参照してください。

PTP 代替 BMCA の例

次の例では、クロック 1 とクロック 4 が、同じ品質と優先順位を持つこの PTP ドメインのグランドマスター候補です。



クロック 1 には、次のパラメータ値があります。

パラメータ	値
クロック品質 - クラス	6
クロック品質 - 正確度	0x21（< 100ns）
クロック品質 - バリアンス	15652
優先順位 2	128
削除されるステップ	*
クロック ID	0000.1111.1111

クロック 4 には、次のパラメータ値があります。

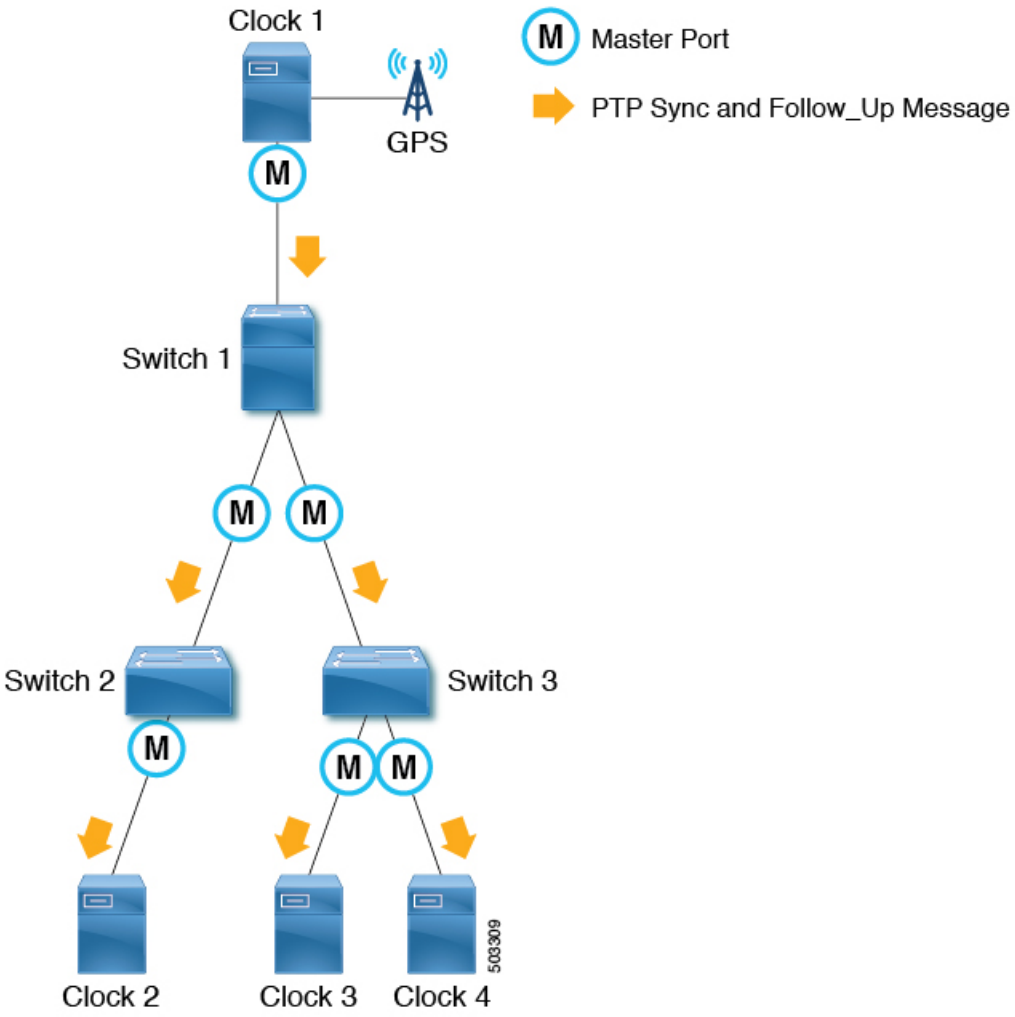
パラメータ	値
クロック品質 - クラス	6
クロック品質 - 正確度	0x21（< 100ns）
クロック品質 - バリアンス	15652
優先順位 2	128
削除されるステップ	*
クロック ID	0000.1111.2222

クロック 1 とクロック 4 の両方が PTP `Announce` メッセージを送信し、各 PTP ノードがメッセージ内の値を比較します。`Clock Quality - Class` から `Priority 2` までのパラメータの値は同じであるため、`Steps Removed` は各 PTP ノードのアクティブなグランドマスターを決定します。

スイッチ 1 および 2 の場合、クロック 1 がグランドマスターです。スイッチ 3 の場合、クロック 4 がグランドマスターです。

PTP クロック同期

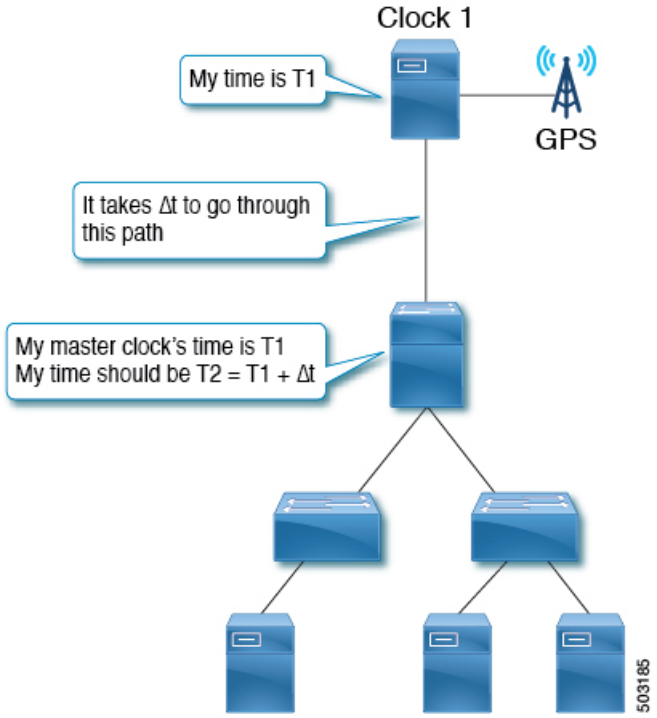
PTP マスター ポートは、PTP over IPv4 UDP の場合、PTP `Sync` および `Follow_Up` メッセージを IP アドレス 224.0.1.129 に送信します。



ワンステップ モードでは、Sync メッセージには、メッセージが送信されたときのタイムスタンプが含まれます。 Follow_Up メッセージは必要ありません。2 段階モードでは、Sync メッセージはタイムスタンプなしで送信されます。 Follow_Up メッセージは、Sync メッセージが送信されたときのタイムスタンプを使用して、各 Sync メッセージの直後に送信されます。クライアント ノードは、Sync または Follow_Up メッセージのタイムスタンプを使用して、meanPathDealy によって計算されたオフセットとともにクロックを同期します。Sync メッセージは、$2^{\text{logSyncInterval}}$ 秒に基づく間隔で送信されます。

PTP および meanPathDelay

meanPathDelay は、PTP パケットが PTP パスの一方の端からもう一方の端に到達するまでにかかる平均時間です。E2E 遅延メカニズムの場合、これは PTP マスター ポートとクライアント ポートの間を移動するのにかかる時間です。PTP は、分散された各デバイスの同期時間を正確に保つために、 meanPathDelay（次の図のΔt）を計算する必要があります。



meanPathDelay を計算するメカニズムは 2 つあります。

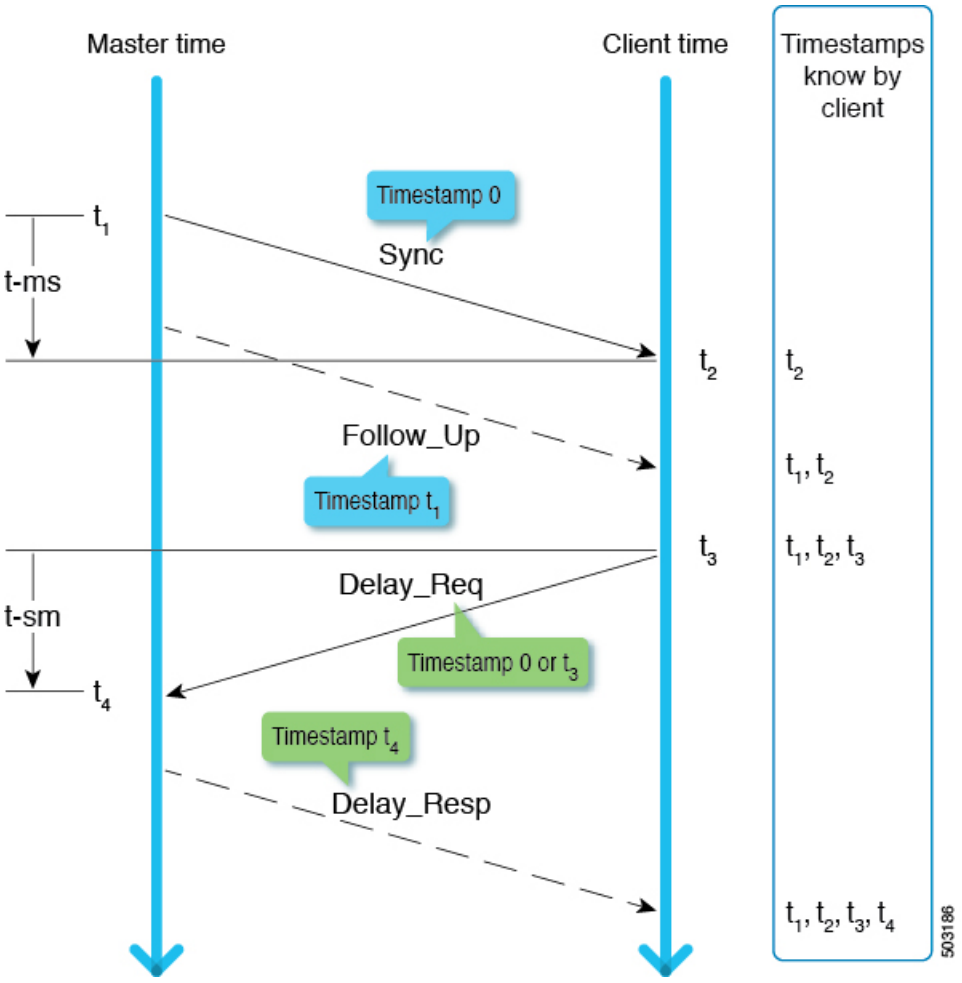
- 遅延要求応答（E2E）：エンドツーエンドの透過クロック ノードは、これのみをサポートできます。
- ピア遅延要求応答（P2P）：ピアツーピアの透過クロック ノードは、これのみをサポートできます。

境界クロック ノードは、定義により両方のメカニズムをサポートできます。IEEE 1588-2008 では、遅延メカニズムは「遅延」または「ピア遅延」と呼ばれます。ただし、遅延要求応答メカニズムは、より一般的に「E2E 遅延メカニズム」と呼ばれ、ピア遅延メカニズムは、より一般的に「P2P 遅延メカニズム」と呼ばれます。

meanPathDelay 測定

遅延要求応答

遅延要求応答（E2E）メカニズムはクライアント ポートによって開始され、meanPathDelay はクライアント ノード側で測定されます。このメカニズムは、E2E 遅延メカニズムに関係なく、マスター ポートから送信される Sync および Follow_Up メッセージを使用します。meanPathDelay 値は、4 つのメッセージからの 4 つのタイムスタンプに基づいて計算されます。



t-ms (t2 – t1) は、マスターからクライアントへの方向の遅延です。 t-sm (t4 – t3) は、クライアントからマスター方向への遅延です。 `meanPathDelay` は次のように計算されます。

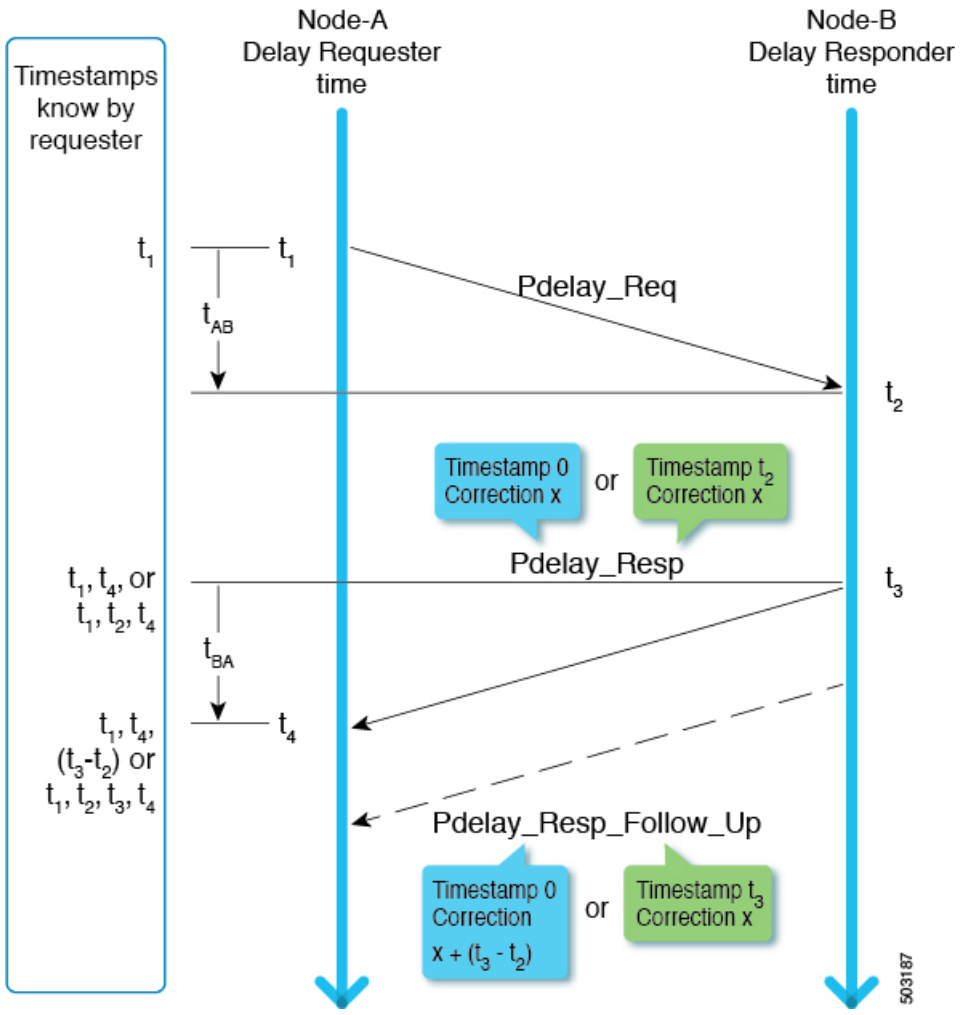
```
(t-ms + t-sm) / 2
```

`Sync` は、2 ^{logSyncInterval} 秒に基づく間隔で送信されます。 `Delay_Req` は、2 ^{logMinDelayReqInterval} 秒に基づく間隔で送信されます。

（注） この例では、2 ステップ モードに焦点を当てています。送信タイミングの詳細については、IEEE 1588-2008 の 9.5 節を参照してください。

ピア遅延要求応答

ピア遅延要求応答（P2P）メカニズムは、マスターポートとクライアント ポートの両方によって開始され、 `meanPathDelay` は要求側ノード側で測定されます。 `meanPathDelay` は、この遅延メカニズム専用の 3 つのメッセージからの 4 つのタイムスタンプに基づいて計算されます。



2 ステップ モードでは、次のいずれかの方法で t2 と t3 がリクエスト送信者に配信されます。

- （t3-t2）として `Pdelay_Resp_Follow_Up` を使用
- t2 として `Pdelay_Resp` を使用し 、 t3 として `Pdelay_Resp_Follow_Up` を使用

`meanPathDelay` は、次のとおり計算されます。

```
(t4-t1) - (t3-t1) / 2
```

`Pdelay_Req` は、2 $^{\text{logMinPDelayReqInterval}}$ 秒に基づく間隔で送信されます。

（注） Cisco Application Centric Infrastructure（ACI）スイッチは、ピア遅延要求応答（P2P）メカニズムをサポートしていません。

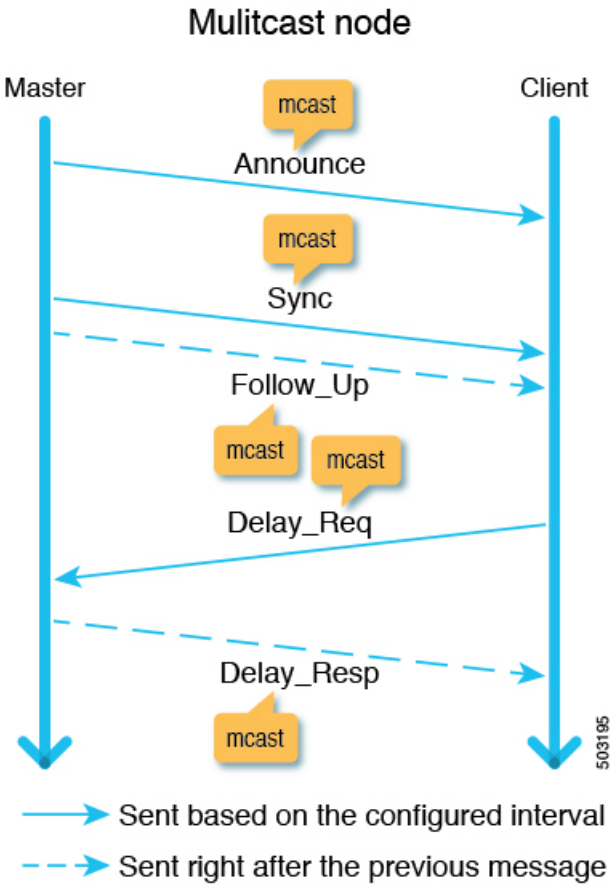
送信タイミングの詳細については、IEEE 1588-2008 の 9.5 節を参照してください。

PTP マルチキャスト、ユニキャスト、および混在モード

次のセクションでは、遅延要求応答（E2E遅延）メカニズムを使用したさまざまなPTPモードについて説明します。

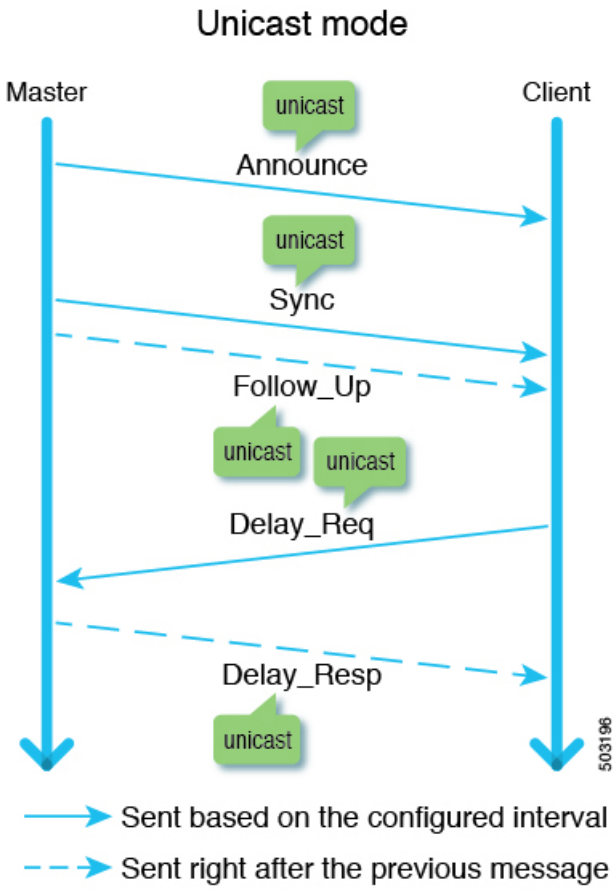
マルチキャスト モード

すべてのPTPメッセージはマルチキャストです。マスターとクライアント間の透過的なクロックまたはPTP非認識ノードは、`Delay`メッセージの非効率的なフラッディングを引き起こします。ただし、これらのメッセージはすべてのクライアントノードに送信する必要があるため、フラッドは、`Announce`、`Sync`、および`Follow_Up`メッセージに対して効率的です。



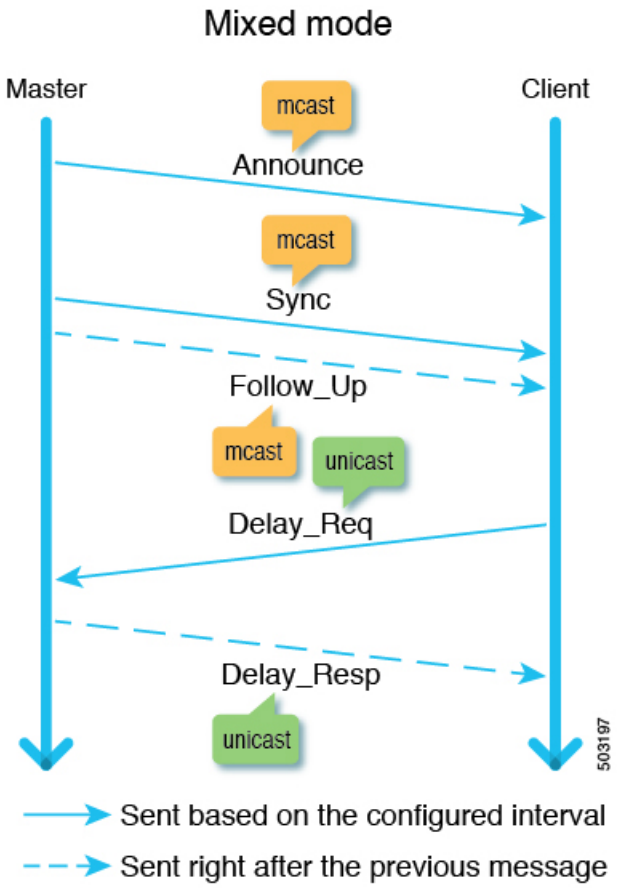
ユニキャスト モード

すべてのPTPメッセージはユニキャストであるため、マスターが生成する必要のあるメッセージの数が増えます。したがって、1つのマスターポートの背後にあるクライアントノードの数などの規模が影響を受けます。



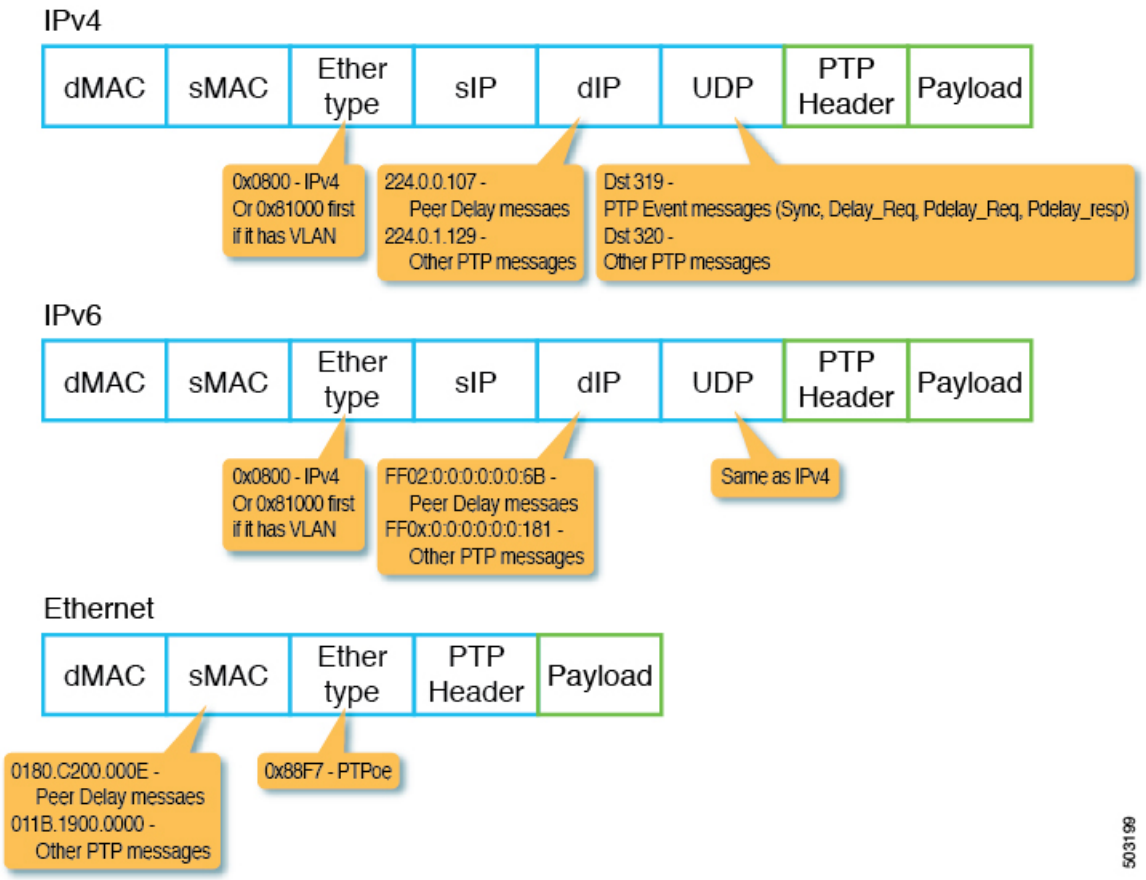
混合モード

`Delay` メッセージのみがユニキャストであり、マルチキャストモードとユニキャストモードに存在する問題を解決します。



PTP トランスポートプロトコル

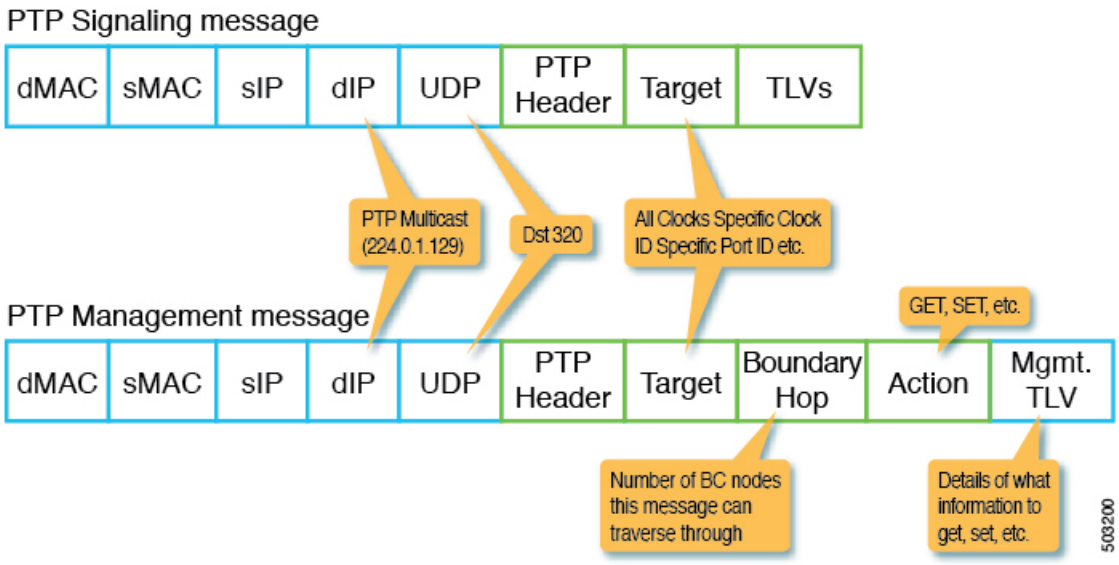
次の図は、PTP がサポートする主要なトランスポートプロトコルに関する情報を示しています。



（注） Cisco Application Centric Infrastructure（ACI）スイッチは、PTP トランスポートプロトコルとして IPv4 とイーサネットのみをサポートします。

PTP シグナリングおよび管理メッセージ

次の図は、IPv4 UDP 上の PTP のヘッダー パケットの `Signaling` および `Management` メッセージ パラメータを示しています。



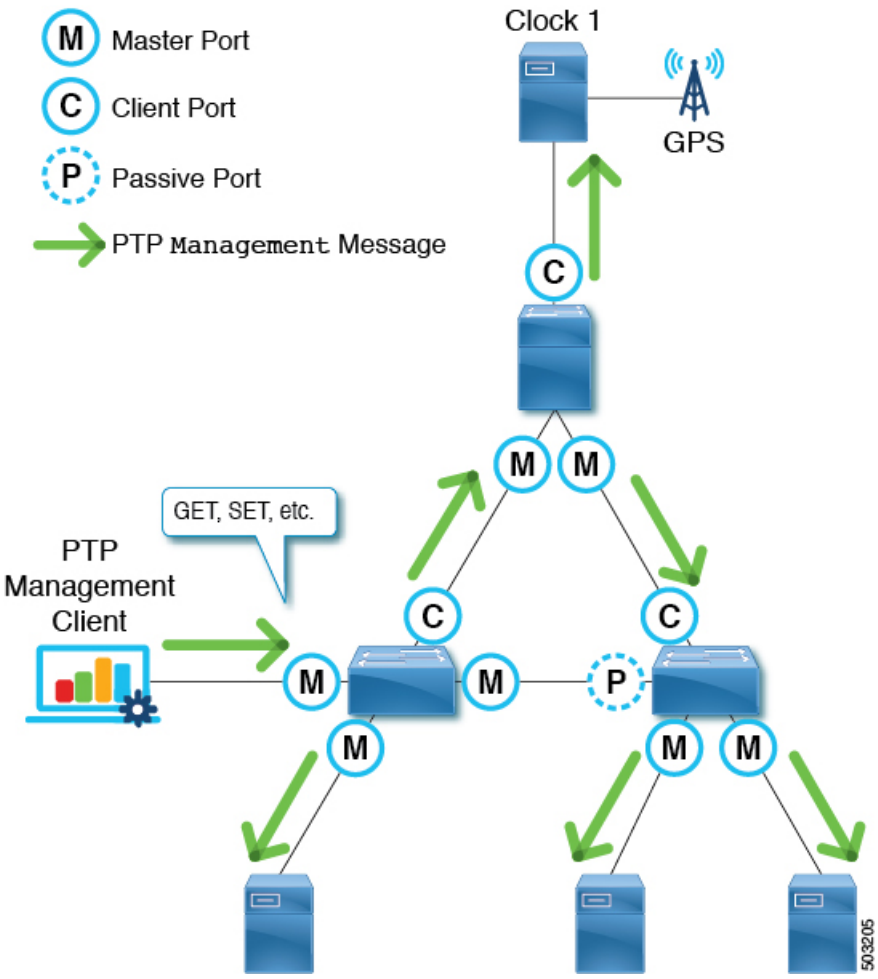
Management メッセージは、現在のクロックやマスターからのオフセットなどの PTP パラメータを構成または収集するために使用されます。このメッセージにより、単一の PTP 管理ノードは、アウトオブバンド モニタリング システムに依存することなく、PTP 関連のパラメータを管理およびモニタできます。

Signaling メッセージは、追加の操作を行うためのさまざまなタイプのタイプ、長さ、および値（TLV）も提供します。他のメッセージに付加されて使用される他の TLV があります。たとえば、IEEE 1588-2008 の 16.2 節で定義されている PATH_TRACE TLV は、PTP トポロジの各境界クロック ノードのパスを追跡するために、Announce メッセージに追加されます。

（注） Cisco Application Centric Infrastructure（ACI）スイッチは、管理、シグナル、またはその他のオプションの TLV をサポートしていません。

PTP 管理メッセージ

PTP Management メッセージは、管理タイプ、長さ、および値（TLV）を一度に複数の PTP ノードに、または特定のノードに転送するために使用されます。



ターゲットは、targetPortIdentity（clockID および portNumber）パラメータで指定されます。PTP Management メッセージには、GET、SET、COMMAND などのアクションを指定する actionField があり、配信された管理 TLV の処理方法をターゲットに通知します。

PTP Management メッセージは、PTP 境界クロックによって、マスター、クライアント、未調整、または Pre_Master ポートにのみ転送されます。メッセージがこれらのポートに転送されるのは、メッセージがマスター、クライアント、未校正、または Pre_Master ポートのポートで受信された場合のみです。メッセージが転送されると、メッセージ内の BoundaryHops が 1 ずつ減ります。

SMTPE ST2059-2 プロファイルは、グランドマスターが、オーディオ/ビデオ信号の同期に必要な同期メタデータ TLV とともにアクション COMMAND を使用して PTP Management メッセージを送信する必要があることを定義します。

（注） Cisco Application Centric Infrastructure（ACI）スイッチは Management メッセージを処理しませんが、それらを転送して SMTPE ST2059-2 PTP プロファイルをサポートします。

PTP プロファイル

Precision Time Protocol（PTP）には、*PTP* プロファイル と呼ばれる概念があります。PTP プロファイルは、PTPのさまざまなユースケースに最適化されたさまざまなパラメータを定義するために使用されます。これらのパラメータの一部には、PTP メッセージ間隔の適切な範囲とPTP トランスポートプロトコルが含まれますが、これらに限定されません。PTPプロファイルは、さまざまな業界の多くの組織/標準規格によって定義されています。次に例を示します。

- IEEE 1588-2008：この標準規格は、デフォルト プロファイル と呼ばれるデフォルトの PTP プロファイルを定義します。
- AES67-2015：この標準規格は、オーディオ要件の PTP プロファイルを定義します。このプロファイルは、メディア プロファイル とも呼ばれます。
- SMPTE ST2059-2：この標準規格は、ビデオ要件の PTP プロファイルを定義します。
- ITU-T G.8275.1：フル タイミング サポートを備えたテレコム プロファイルとしても知られています。この標準規格は、フル タイミング サポートを備えた通信に推奨されます。フル タイミング サポートは、すべてのホップで PTP G.8275.1 プロファイルをデバイスに提供できる電気通信ネットワークを表すために ITU によって定義された用語です。Cisco Application Centric Infrastructure（ACI）でサポートされていない G.8275.2 は、パスに PTP をサポートしないデバイスが含まれる可能性がある部分的なタイミング サポート用です。

  電気通信業界では、周波数と時間/位相の同期の両方が必要です。G.8275.1は、時間とフェーズを同期するために使用されます。周波数は、Cisco ACI によってサポートされていない別の PTP G.8265.1 プロファイルとパケット ネットワークを介して PTP を使用するか、同期デジタル階層（SDH）、同期光ネットワーク（SONET）などの物理層を使用して、専用回路、またはイーサネット経由の同期イーサネット（SyncE）を介して同期できます。SyncE を使用して周波数を同期し、PTP を使用して時間/位相を同期することをハイブリッド モード と呼びます。

  他のプロファイルと比較した G.8275.1 の主な違いは次のとおりです。

  - G.8275.1 は、他のプロファイルには存在しない追加パラメータ Local Priority を使用して、代替 BMCA を使用します。
  - G.8275.1 は、選択可能な同じ接続先 MAC アドレス（転送可能および転送不可）を使用するすべての PTP メッセージで PTP over Ethernet を使用します。
  - G.8275.1 は、テレコム境界クロック（T-BC）が G.8273.2 で定義された正確度（最大時間誤差、max|TE|）に従うことを期待しています。
    - クラス A：100 ns
    - クラス B：70 ns
    - クラスC：30ns

次の表は、各PTPプロファイルの各標準規格で定義されているパラメータの一部を示しています。

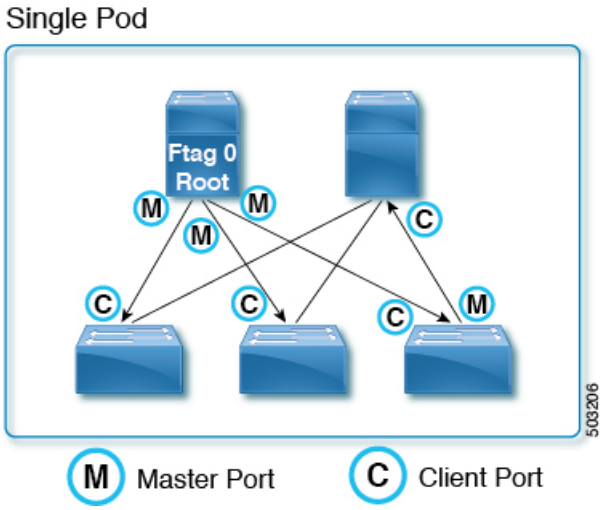
プロファイル	logAnnounce 間隔	logSync 間隔	logMinDelayReq 間隔	AnnounceReceipt タイムアウト	ドメイン番号	モード	トランスポートプロトコル
[デフォルトプロファイル（Default Profile）]	0 ー 4（1） [= 1 ～ 16 秒]	-1 ～ +1（0） [= 0.5 ～ 2 秒]	0 ー 5（0） [= 1 ～ 32 秒]	2 ～ 10 のアナウンス間隔（3）	0 ～ 255（0）	マルチキャスト / ユニキャスト	Any/IPv4
AES67-2015（メディアプロファイル）	0 ー 4（1） [= 1 ～ 16 秒]	-4 ー +1（-3） [= 1/16 ～ 2 秒]	-3 ー +5（0） [= 1/8 ～ 32 秒] または *logSyncInterval* から *logSyncInterval* + 5 秒	2 ～ 10 のアナウンス間隔（3）	0 ～ 255（0）	マルチキャスト / ユニキャスト	UDP/IPv4
SMTPE ST2059-2-2015	-3 ～ +1（-2） [= 1/8 ～ 2 秒]	-7 ～ -1（-3） [= 1/128 ～ 0.5 秒]	*logSyncInterval* から *logSyncInterval* + 5 秒	2 ～ 10 のアナウンス間隔（3）	0 ～ 127（127）	マルチキャスト / ユニキャスト	UDP/IPv4
ITU-T G.8275.1	-3	-4	-4	2 ～ 4	24～43（24）	マルチキャストのみ	イーサネット

Cisco ACI および PTP

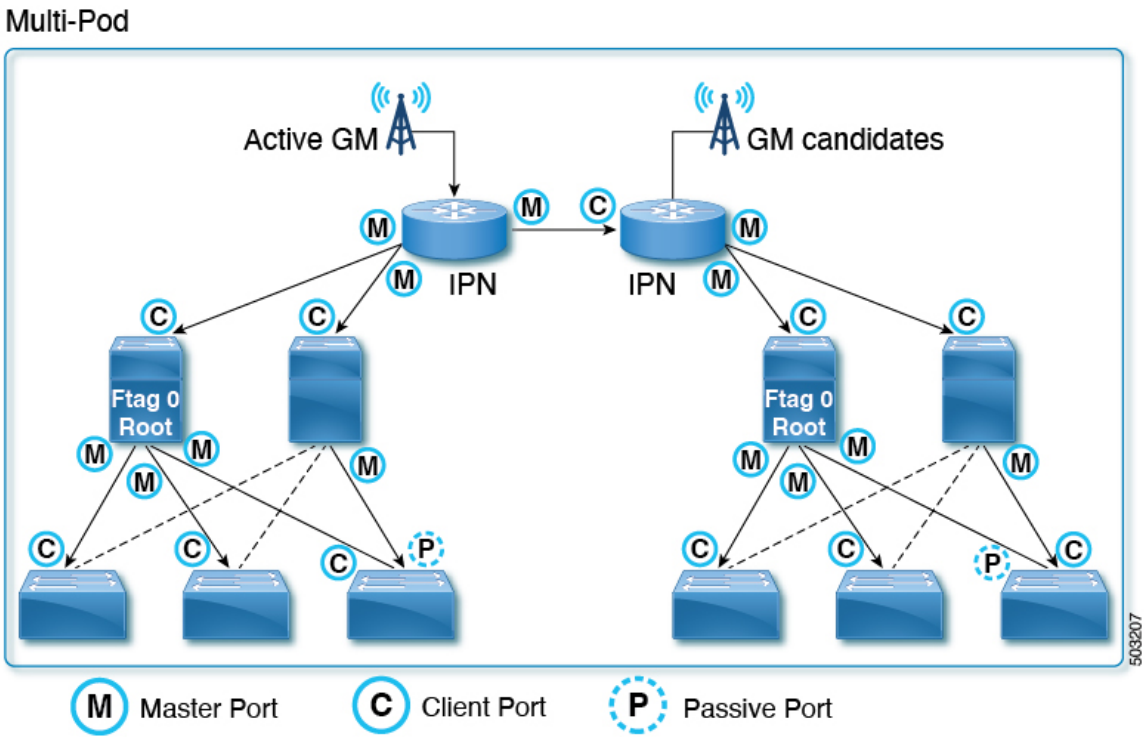
Cisco Application Centric Infrastructure（ACI）ファブリックでは、Cisco Application Policy Infrastructure Controller（APIC）で PTP 機能がグローバルに有効になっている場合、ソフトウェアは、サポートされているすべてのスパインおよびリーフスイッチの特定のインターフェイスで PTP を自動的に有効にして、ファブリック内に PTP マスター/クライアント トポロジを確立します。Cisco APIC リリース 4.2(5) 以降、リーフスイッチのフロント パネル ポートで PTP を有効にして、PTP トポロジをファブリックの外部に拡張できます。外部グランドマスター クロックがない場合、スパイン スイッチの 1 つがグランドマスターとして選択されます。マスター スパイン スイッチには、他のスパインおよびリーフスイッチよりも 1 低い別の PTP 優先順位が与えられます。

Cisco APIC リリース 3.0(1) での導入

Cisco Application Policy Infrastructure Controller（APIC）リリース 3.0(1) から、Cisco Application Centric Infrastructure（ACI）ファブリック スイッチ内でのみ時間を同期するために、PTP が部分的に導入されました。PTP は、Cisco APIC リリース 3.0(1) でも導入された遅延測定機能を提供する必要がありました。この目的のために、PTP をグローバルに有効または無効にする単一のオプションが導入されました。PTP がグローバルに有効になっている場合、すべてのリーフ スイッチとスパイン スイッチが PTP 境界クロックとして構成されます。PTP は、ID 0 の ftag ツリー（ftag0 ツリー）によって使用されるすべてのファブリック ポートで自動的に有効になります。これは、各ポッドのすべてのリーフスイッチおよびスパイン スイッチ間のループフリー マルチキャスト接続向けに Cisco ACI infra ISIS に基づいて自動的に構築される内部ツリー トポロジの 1 つです。ポッド間ネットワーク（IPN）に外部グランドマスターがない場合、ftag 0 ツリーのルート スパイン スイッチは、グランドマスターになるように PTP priority1 254 で自動的に構成されます。他のスパインおよびリーフスイッチは、PTP priority1 255 で構成されます。



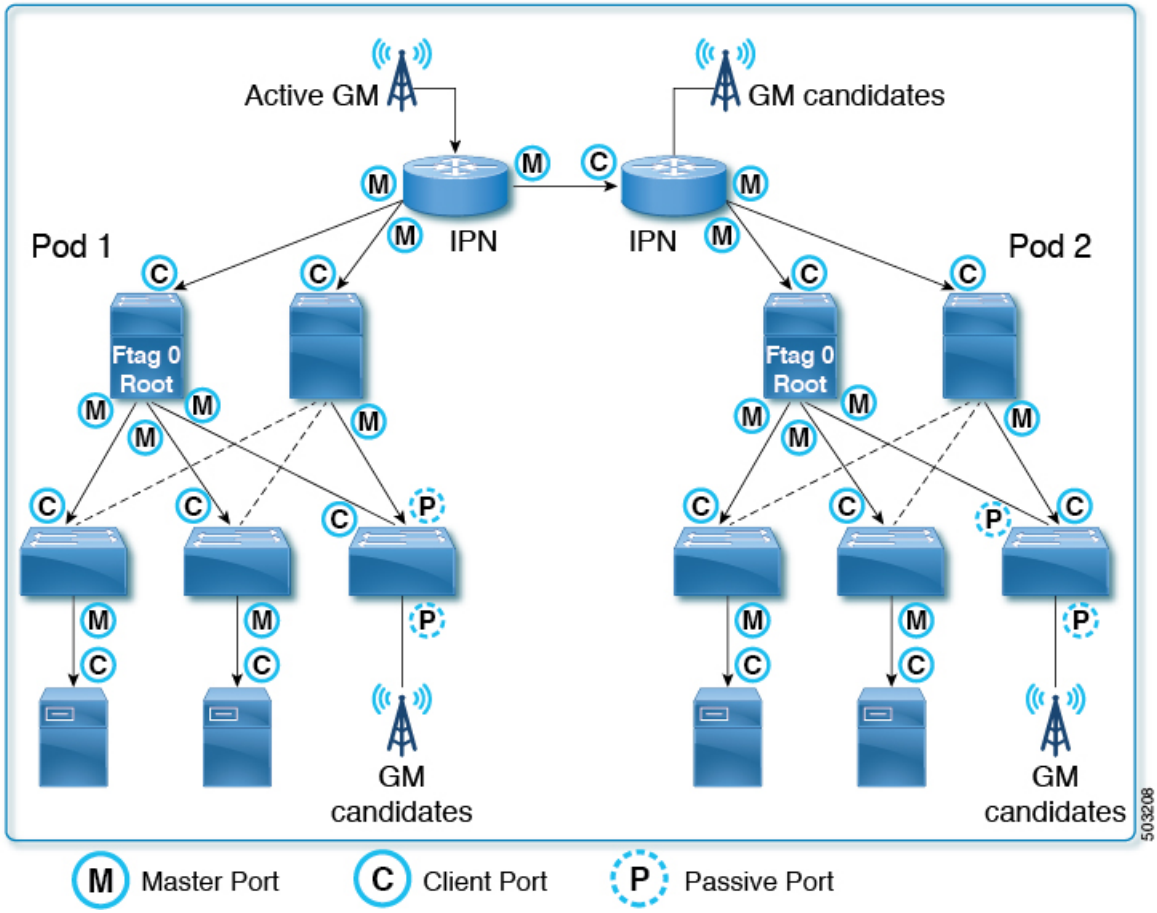
Cisco ACI マルチポッド セットアップで、PTP をグローバルに有効にすると、tn-infra Multi-Pod L3Out の IPN 接続用に構成されたサブインターフェイスで、PTP は自動的に有効になります。Cisco APIC リリース 4.2(5) まで、または 5.1(1) では、これが外部向きのインターフェイスで PTP を有効にする唯一の方法です。これにより、 Cisco ACI ファブリックを IPN を介して外部グランドマスターにロックできます。高い精度が必要な場合は、GPS/GNSS などのプライマリ基準時刻ソースを備えた外部グランド マスターを使用することをお勧めします。Cisco ACI マルチポッド セットアップで外部グランド マスターなしで PTP を有効にした場合、IPN で PTP が有効になっていて、IPN の PTP BMCA パラメータ（PTP プライオリティなど）がスパイン スイッチのパラメータよりも優れていないとすると、スパイン スイッチの 1 台がすべてのポッドのグランド マスターになる可能性があります。スパイン スイッチをグランド マスターとして使用している場合、新しいポッドを追加すると、意図していなくても新しいポッドから新しいグランド マスターが選択され、ファブリック全体の PTP 同期で一時的にチャーンが発生する可能性があります。外部グランド マスターに関係なく、グランド マスターからのホップ数が少ない優れた PTP トポロジを実現するため、ファブリック内のすべてのスパイン スイッチを IPN に接続することを推奨します。ユーザーは、各ポッド内で PTP トポロジを決定する ftag0 ツリーの構成方法を制御できないためです。



Cisco APIC リリース 3.0(1) では、リーフスイッチのダウン リンク（フロント パネル ポート）など、他のインターフェイスで PTP をオンデマンドで有効にすることはできません。

Cisco APIC リリース 4.2(5) および 5.1(1) での導入

Cisco APIC リリース 4.2(5) および 5.1(1) 以降、リーフスイッチのフロント パネル ポートで PTP を有効にして、PTP ノード、クライアント、またはグランドマスターを接続できます。ファブリック ポートの PTP 実装は、ファブリック ポートの PTP パラメータを調整できるようになったことを除いて、以前のリリースと同じです。この変更により、Cisco ACI ファブリックを使用して、 Cisco ACI スイッチのある PTP を使用した時間同期を、PTP 境界クロック ノードとしてで伝搬できます。それ以前は、Cisco ACI は PTP マルチキャストまたはユニキャスト メッセージを、あるリーフスイッチから別のリーフスイッチにトンネルとして PTP 非認識スイッチとして透過的に転送するしか方法がありませんでした。



（注） 5.0(x) リリースは、4.2(5) および 5.1(1) リリースで導入された PTP 機能をサポートしていません。

Cisco ACI ソフトウェアおよびハードウェア要件

PTP 向けにサポートされるソフトウェア

次の機能は、Cisco Application Policy Infrastructure Controller（APIC）リリース 3.0(1) からサポートされています。

- 遅延測定機能のファブリック内のみの PTP

次の機能は、Cisco APIC リリース 4.2(5) からサポートされています。

- リーフスイッチによる外部デバイスとの PTP
- リーフスイッチの前面パネル ポートの PTP

- 構成可能な PTP メッセージ間隔
- 構成可能な PTP ドメイン番号
- 構成可能な PTP 優先順位
- PTP マルチキャスト ポート
- リーフスイッチのフロント パネル ポートの PTP ユニキャスト マスター ポート
- IPv4/UDP 上の PTP
- PTP プロファイル（デフォルト、AES67、および SMTPE ST2059-2）

次の機能は、Cisco APIC リリース 5.2(5) からサポートされています。

- PTP マルチキャスト マスター専用ポート
- PTP オーバー イーサネット
- フル タイミング サポートを備えた PTP テレコム プロファイル（ITU-T G.8275.1）

PTP 向けにサポートされるハードウェア

N9K-X9732C-EX や N9K-C93180YC-FX など、製品 ID に -EX 以降が付いているリーフスイッチ、スパイン スイッチ、およびラインカードがサポートされています。

PTPテレコムプロファイル（G.8275.1）は、**リーフスイッチとして動作する**これらのスイッチでのみサポートされます。

- SyncE とともに使用する場合、クラス B （G.8273.2）の精度で N9K-C93180YC-FX3
- SyncE とともに使用する場合、クラス C （G.8273.2）の精度の N9K-C9332D-H2R
- SyncE とともに使用する場合、クラス C （G.8273.2）の精度の N9K-C93400LD-H1

これらのリーフ スイッチはサポートされていません。

- N9K-C9332PQ
- N9K-C9372PX
- N9K-C9372PX-E
- N9K-C9372TX
- N9K-C9372TX-E
- N9K-C9396PX
- N9K-C9396TX
- N9K-C93120TX
- N9K-C93128TX

N9K-C9408 シャーシでこれらのリーフスイッチラインカードはサポートされていません。

- N9K-X9400-8D
- N9K-X9400-16W（ACI 6.1(3) リリース以降のファブリック リンクでのみサポート）
- N9K-X9400-22L

このスパイン ボックス スイッチはサポートされていません。

- N9K-C9336PQ

N9K-C9504、N9K-C9508、および N9K-C9516 シャーシでこのスパイン スイッチ ライン カードはサポートされていません。

- N9K-X9736PQ

N9K-C9408 シャーシでこれらのスパイン スイッチラインカードはサポートされていません。

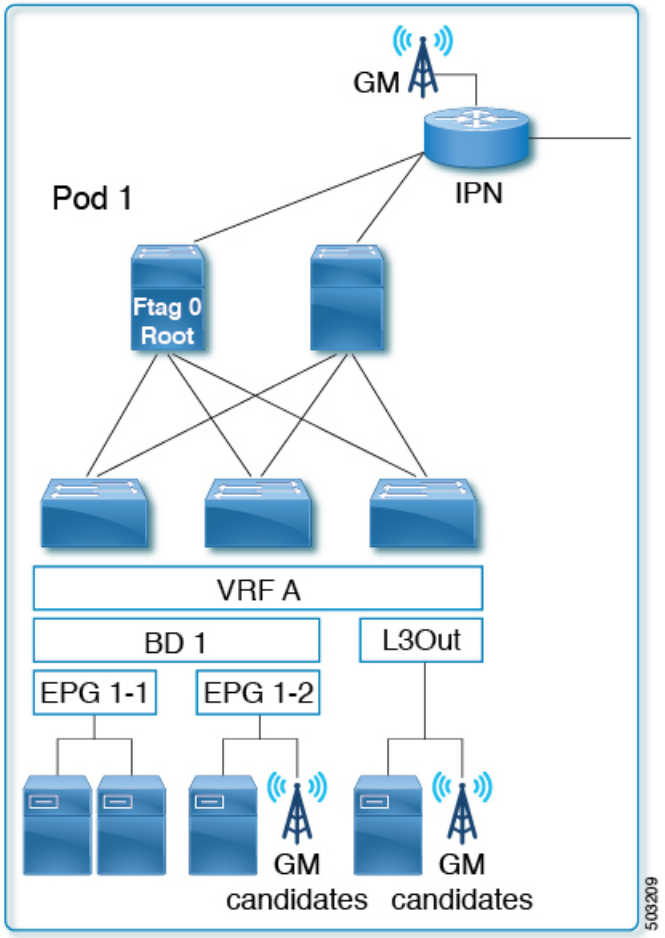
- N9K-X9400-8D
- N9K-X9400-16W（ACI 6.1(3) リリース以降のファブリック リンクでのみサポート）

PTP 接続

サポート対象 PTP ノード接続

外部 PTP ノードは、次の方法を使用して Cisco Application Centric Infrastructure（ACI）ファブリックに接続できます。

- ポッド間ネットワーク
- EPG（リーフスイッチ上）
- L3Out（リーフスイッチ上）



PTP は、スタンドアロン NX-OS スイッチと同じように VRF に依存しません。すべての PTP メッセージは、各 Cisco ACI スイッチ ノードのインターフェイス レベルで PTP 境界クロックとして終了、処理、および生成されます。VRF、ブリッジドメイン、EPG、または VLAN に関係なく、ベスト マスター クロック アルゴリズム（BMCA）は、各 Cisco ACI スイッチのすべてのインターフェイスにわたって計算されます。ファブリック全体に対して PTP ドメインは 1 つだけです。

E2E 遅延メカニズム（delay req-resp）を備えた PTP ノードは、PTP 境界クロックとして実行されている Cisco ACI スイッチに接続できます。

（注） Cisco ACI スイッチは、ピア遅延（P2P）メカニズムをサポートしていません。したがって、P2P トランスペアレント クロック ノードは Cisco ACI スイッチに接続できません。

サポート対象 PTP インターフェイス接続

Connection Type	インターフェイス タイプ	リーフスイッチ タイプ（リーフ、リモート リーフ、tier-2 リーフ）	サポート/非サポート（非テレコム プロファイル）	サポート/非サポート（G.8275.1）
ファブリック リンク（リーフスイッチとスパイン スイッチ間）	サブインターフェイス（非PC）	-	サポート対象	サポート対象外
ファブリック リンク（tier-1 と tier-2 リーフスイッチ間）	サブインターフェイス（非PC）	-	サポート対象	サポート対象外
スパイン（IPN 向き）	サブインターフェイス（非PC）	-	サポート対象	サポート対象外
リモート リーフ (IPN 向き)	サブインターフェイス（非PC）	-	サポート対象	サポート対象
リモート リーフ（ピア リンク、バックツーバック リンク）	物理	-	サポート対象	サポート対象
リモートリーフ（ユーザー l3out、ルーテッド サブ）	サブインターフェイス（非PC）	リモート リーフ	サポート対象	サポート対象
通常のEPG（トランク、アクセス、802.1P）	物理、ポートチャネル、vPC	すべて	サポート対象	サポート対象
L3Out（ルーテッド、ルーテッド サブ）	物理、ポートチャネル	すべて	サポート対象	サポート対象
L3Out（SVI– トランク、アクセス、802.1P）	物理、ポートチャネル、vPC	すべて	サポート対象外	サポート対象外
L2Out（トランク）	物理、ポートチャネル、vPC	すべて	サポート対象外	サポート対象外
tn-mgmt の EPG/L3Out	物理、ポートチャネル、vPC	すべて	サポート対象外	サポート対象外
サービス EPG（トランク）[1]	物理、ポートチャネル、vPC	すべて	サポート対象外	サポート対象外

Connection Type	インターフェイス タイプ	リーフ スイッチ タイプ（リーフ、リモート リーフ、tier-2 リーフ）	サポート/非サポート（非テレコム プロファイル）	サポート/非サポート（G.8275.1）
任意のタイプの FEX インターフェイス	すべて	すべて	サポート対象外	サポート対象外
ブレークアウトポート[2]	すべて	すべて	サポート対象	サポート対象外
アウトオブバンド管理インターフェイス	物理	-	サポート対象外	サポート対象外

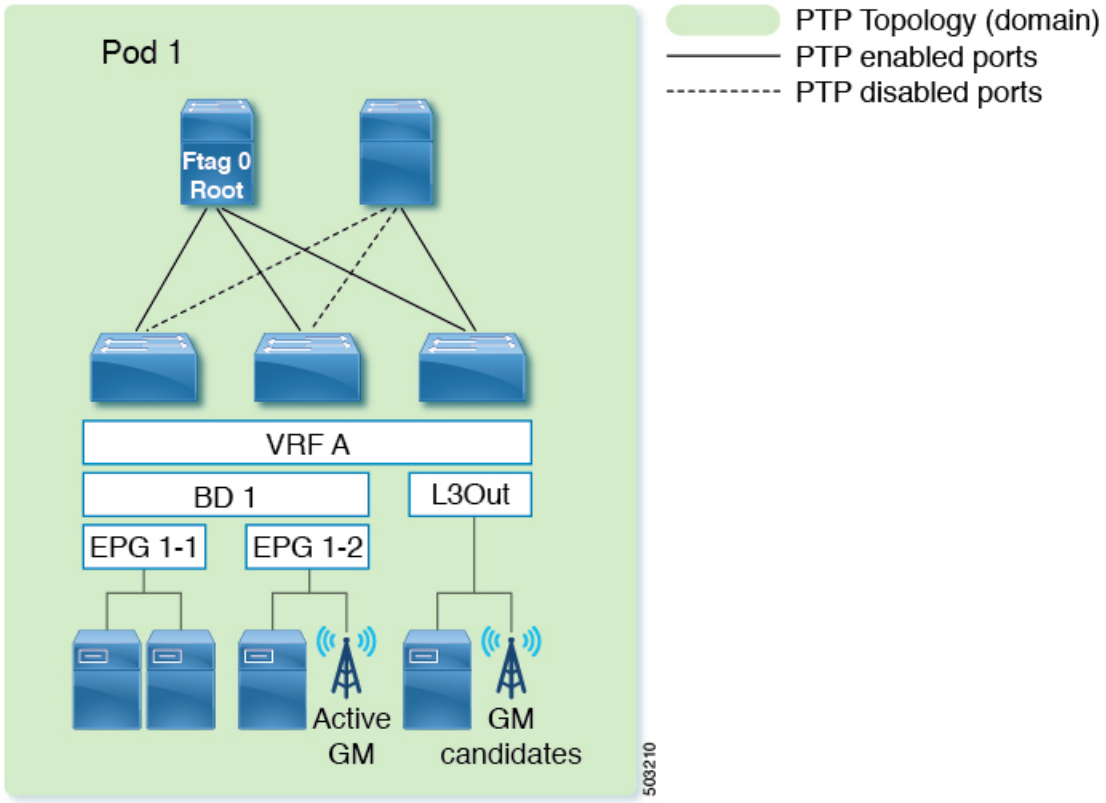
[1] サービス EPG は、レイヤ 4 からレイヤ 7 のサービス グラフ用に作成された内部 EPG です。
[2] ファブリック リンクとダウンリンクの両方。

グランドマスターの展開

次のいずれかの方法を使用して、グランドマスター候補を展開できます。

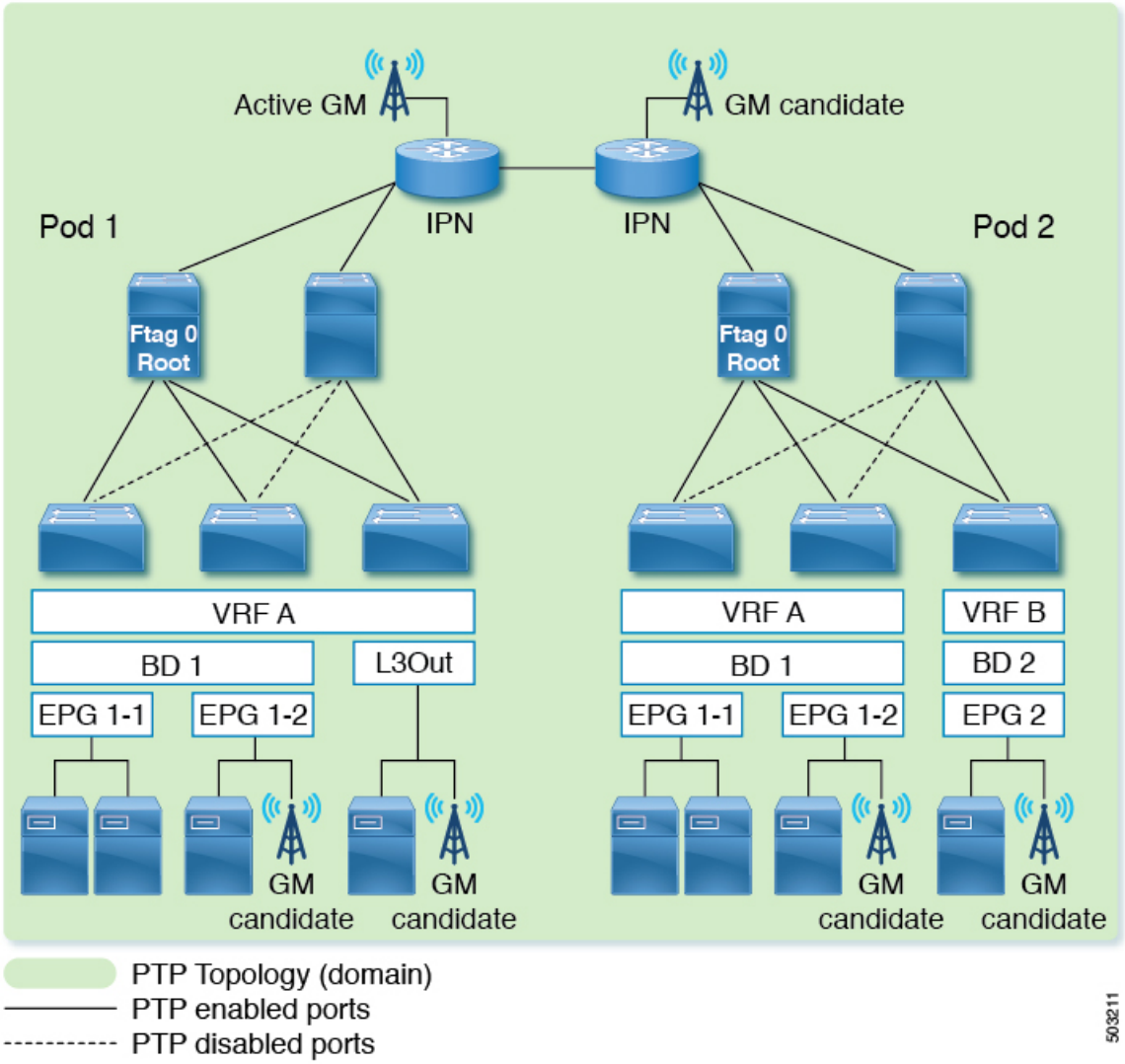
シングル ポッド

単一のポッド展開では、グランドマスター候補をファブリック内のどこにでも展開できます（L3Out、EPG、またはその両方）。ベストマスタークロック アルゴリズム（BMCA）は、それらすべての中からアクティブなグランドマスターを 1 つ選択します。



複数のポッドにまたがる BMCA を備えたマルチポッド

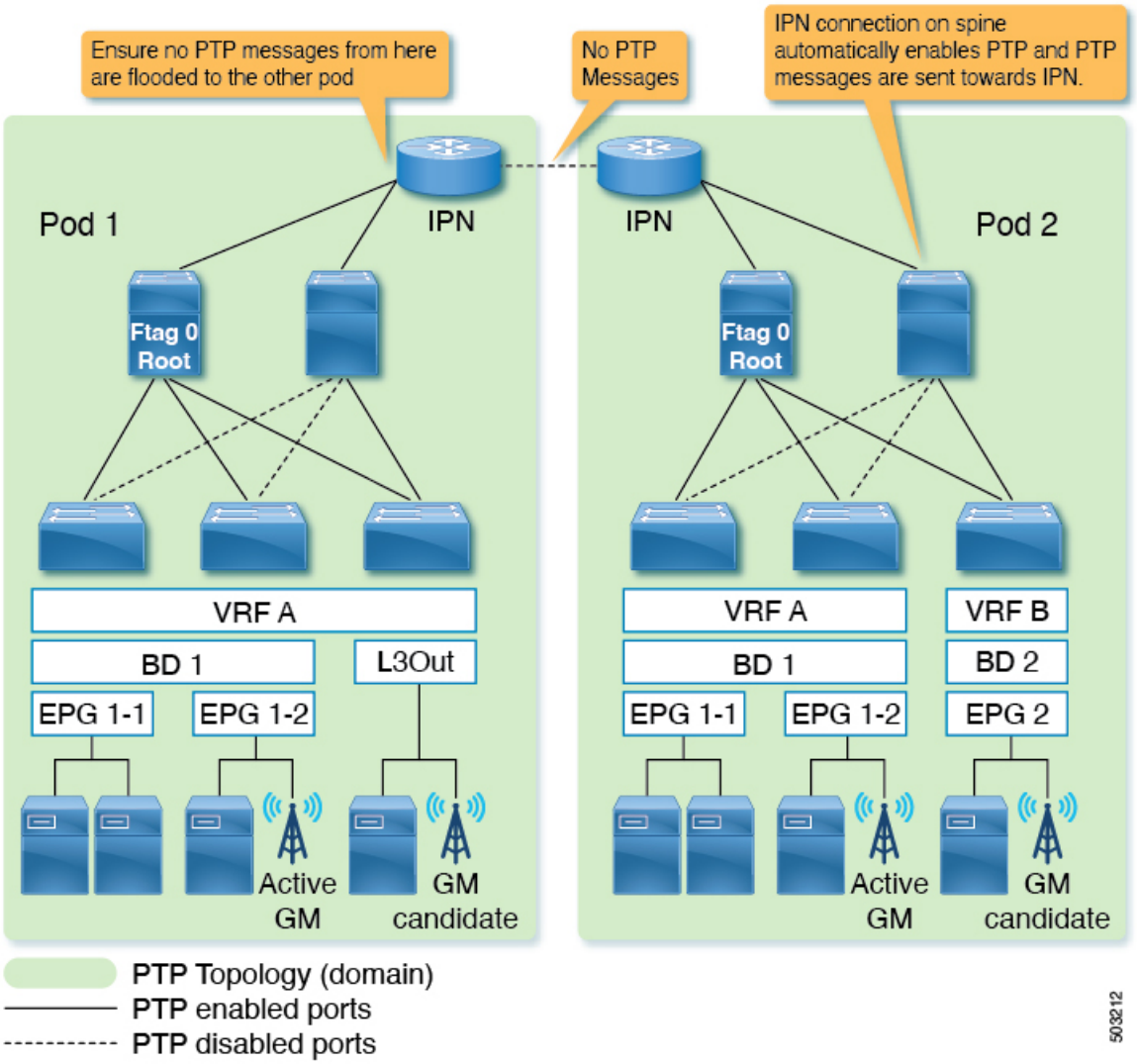
グランドマスター候補は、ファブリック内のどこにでも展開できます（ポッド間ネットワーク、L3Out、EPG、またはそれらすべて）。BMCA は、ポッド全体でアクティブなグランドマスターを 1 人選択します。ポッド内の PTP クライアントがアクティブなグランドマスターに対して同数のホップを持つように、グランドマスターをポッド間ネットワーク（IPN）に配置することが推奨されています。さらに、アクティブなグランドマスターが使用できなくなっても、マスター/クライアント ツリー トポロジが大幅に変更されることはありません。



各ポッドにBMCAを備えたマルチポッド

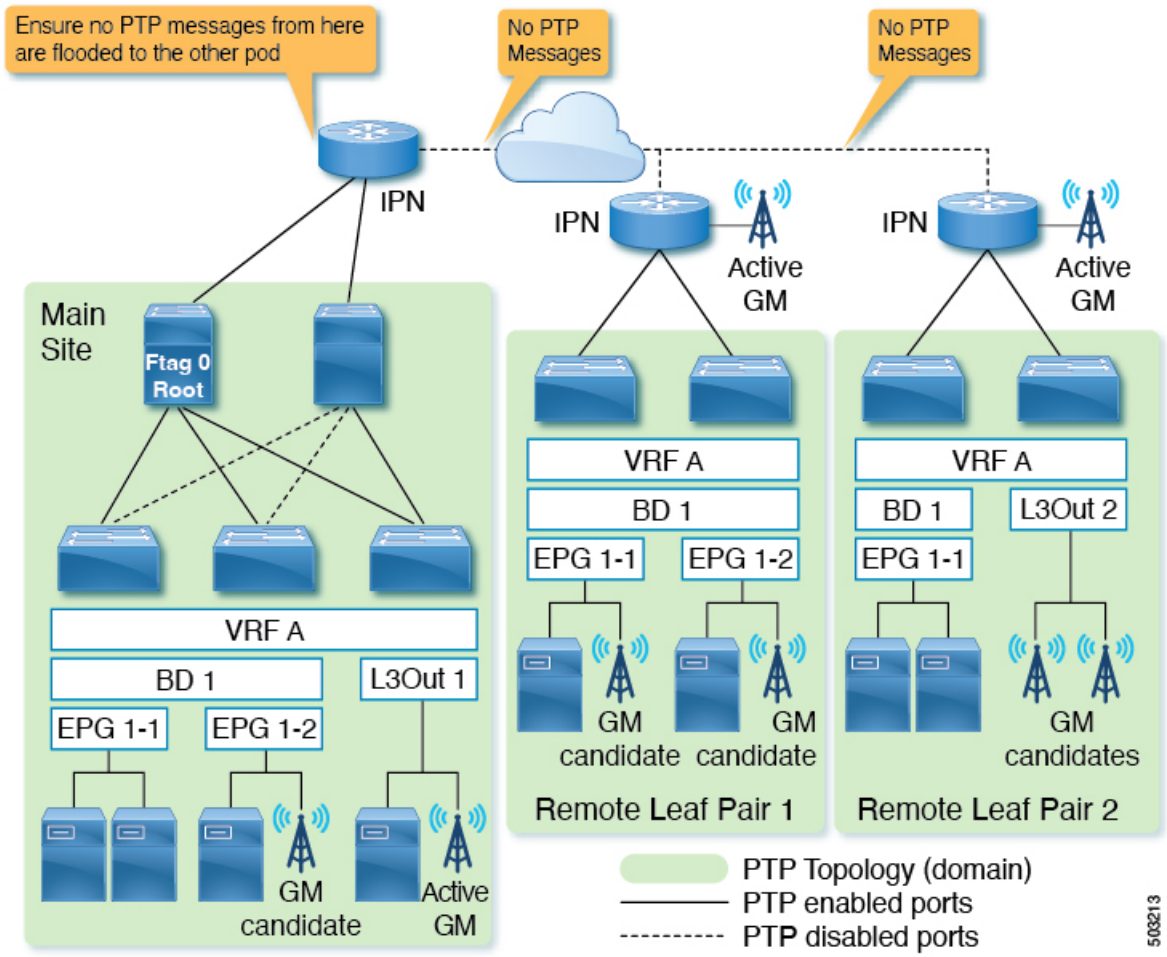
IPN ドメインを介して PTP の正確度が大幅に低下するために各ポッドにアクティブなグランドマスターが必要な場合、PTP メッセージはポッド間で IPN を通過してはなりません。この構成を完成させるには以下のいずれかの方法を実行します。

- オプション 1：IPN とスパイン スイッチ間でサブインターフェイスが使用されていることを確認し、IPN で PTP を無効にします。
- オプション 2：PTP グランドマスターが各ポッドの IPN に接続されていても、PTP トポロジを分離する必要がある場合は、ポッド間の IPN インターフェイスで PTP を無効にします。



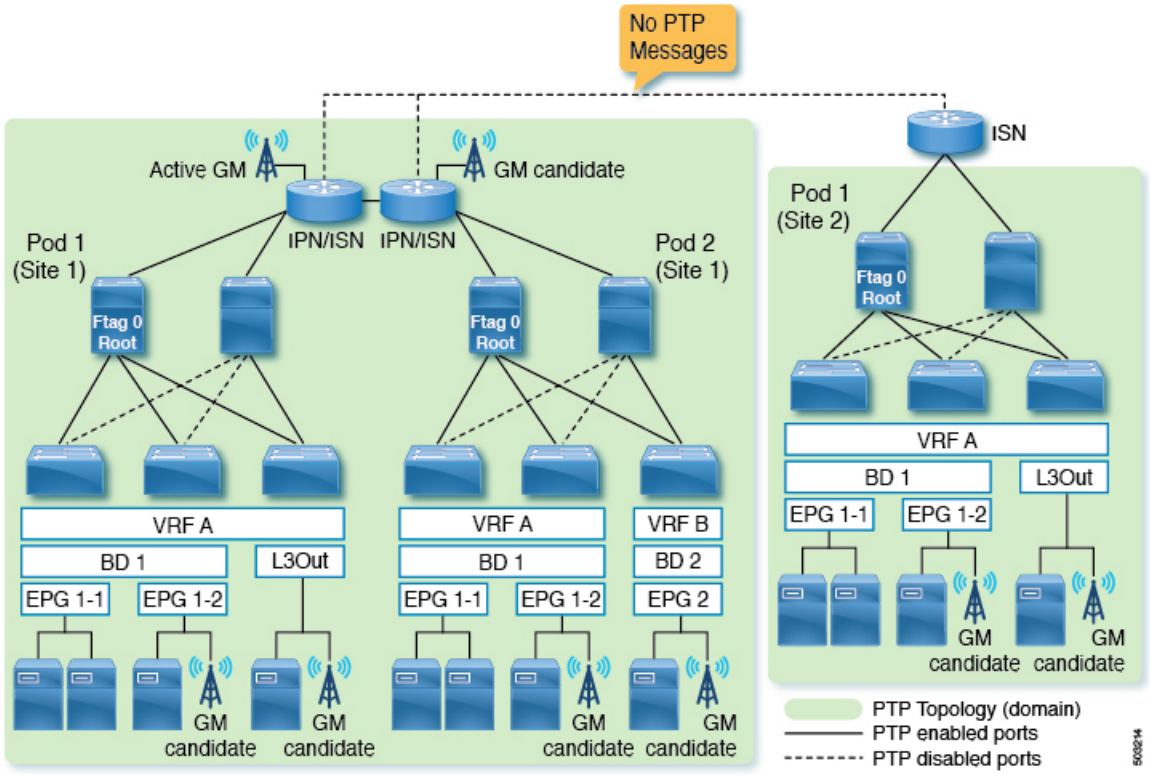
リモートのリーフスイッチ

通常、リモート リーフスイッチ サイトは、メイン データセンターや相互に近くになく、遅延と修正の正確な測定値を使用して各場所に PTP メッセージを伝播することは困難です。したがって、PTP メッセージが各サイト（場所）を通過しないようにして、各サイト（場所）内で PTP トポロジが確立されるようにすることが推奨されます。一部の遠隔地は、互いに近接している場合があります。このような場合、それらの IPN 間の PTP を有効にして、それらの場所で 1 つの PTP トポロジを形成できます。*Multipod With BMCA in Each Pod* で説明されているのと同じオプションを使用して、PTP メッセージの伝播を防ぐことができます。



Cisco ACI マルチサイト

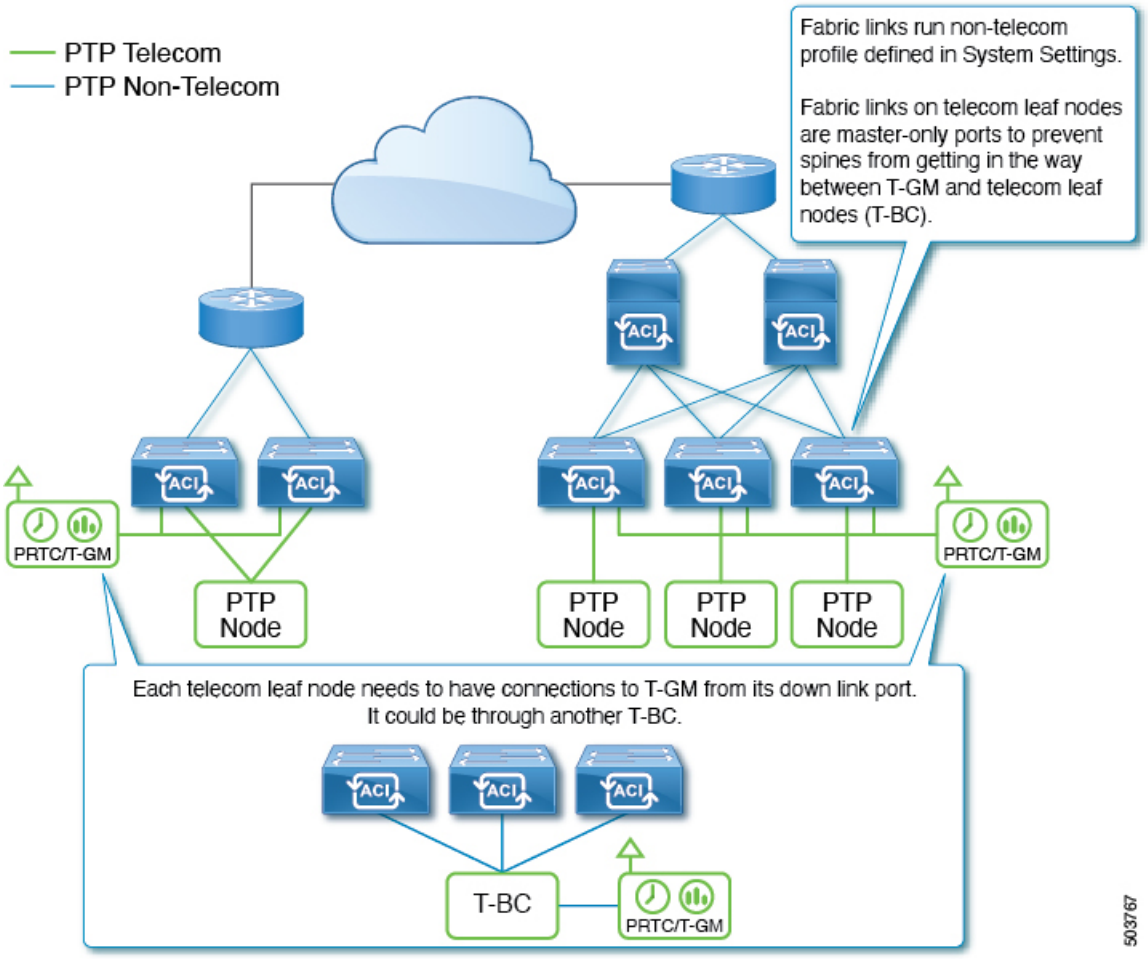
通常、各サイトは互いに近接しておらず、遅延と修正の正確な測定値を使用して各サイトに PTP メッセージを伝播することは困難です。したがって、PTP メッセージが各サイトを通過しないようにして、各サイト内で PTP トポロジが確立されるようにすることが推奨されます。*Multipod With BMCA in Each Pod* で説明されているのと同じオプションを使用して、PTP メッセージの伝播を防ぐことができます。また、Cisco ACI マルチサイトは PTP を構成するための可視性も機能もありません。



Telecom プロファイル（G.8275.1）

Cisco Application Centric Infrastructure（ACI）の PTP Telecom プロファイル（G.8275.1）では、SyncE がクラス B または、C（G.8273.2）の精度を達成する必要があります。また、PTP Telecom プロファイル（G.8275.1）と SyncE の両方が、特定のスイッチ モデルのリーフ ノードでのみサポートされます（「PTP でサポートされるハードウェア」を参照）。その結果、スパイン ノードを使用して、Telecom プロファイル（G.8275.1）の時間、位相、および周波数の同期を配布することはできません。

このため、テレコム リーフ ノード（G.8275.1 用に構成されたリーフ ノード）のファブリック リンクは、PTP マルチキャスト マスター専用モードで実行されます。これにより、テレコム リーフ ノードがスパイン ノードを介してクロックをロックしないようにします。これは、Cisco ACI の PTP テレコム プロファイル（G.8275.1）のグランドマスター展開では、各テレコム リーフ ノードがノードのそれぞれのダウン リンク ポートからタイミングを受信する必要があることを意味します。



PTP 制限事項

一般的なサポートと実装情報については、PTP 向けにサポートされるソフトウェア （42 ページ）、PTP 向けにサポートされるハードウェア （43 ページ） および PTP 接続 （44 ページ）を参照してください。

次の制限が PTP に適用されます。

- Cisco Application Centric Infrastructure（ACI）リーフおよびスパイン スイッチは、PTP 境界クロックとして機能できます。スイッチは PTP トランスペアレント クロックとして機能できません。
- E2E 遅延メカニズム（遅延要求/応答メカニズム）のみがサポートされています。P2P 遅延メカニズムはサポートされていません。
- デフォルト/メディア/SMPTE PTP プロファイル用の PTP over IPv4/UDP と、テレコム（G.8275.1）PTP プロファイル用の PTP over Ethernet がサポートされています。IPv6 を介した PTP はサポートされていません。

- PTPv2 のみがサポートされています。
  - リーフスイッチのフロントパネルポートのいずれかでPTPが有効になっている場合、PTPv1 パケットは引き続き CPU にリダイレクトされますが、パケットは CPU で破棄されます。
- PTP 管理 TLV は Cisco ACI スイッチによって認識されませんが、IEEE1588-2008 で定義されているように SMTPE PTP プロファイルをサポートするために引き続き転送されます。
- Cisco ACI スイッチのシステム クロックとして PTP を使用することはできません。
- PTP は、Cisco Application Policy Infrastructure Controller（APIC）でサポートされません。
- NTP は、ファブリック内のすべてのスイッチに必要です。
- PTPオフロードはサポートされていません。この機能は、拡張性を向上させるために、モジュラ スパイン スイッチ上の各ラインカードCPUにPTPパケット処理をオフロードすることです。
- ハードウェアの制限により、トラフィック負荷がある場合、1G/100M速度のインターフェイスは10Gインターフェイスよりも正確度が低くなります。5.2(3) 以降のリリースでは、この制限は 1G 速度の Cisco N9K-C93108TC-FX3P スイッチには適用されません。
- PTP オフセット補正が高いため、PTP は 100M インターフェイスでは完全にはサポートされていません。
- PTP Telecom プロファイル（G.8275.1）は、1G/10G 速度のポートではサポートされていません。
- `Sync` および `Delay_Request` メッセージは、最大 -4 間隔（1/16 秒）をサポートできます。-5 から -7 の間隔値はサポートされていません。

  グローバル PTP ポリシーのデフォルトの間隔値は、同期間隔 -3（2^-3 = 1/8 秒）および遅延要求間隔 -2（2^-2 = 1/4 秒）のメディア プロファイル（AES67-2015）です。これらの間隔はテスト済みであり、サポートされているほとんどのスイッチ モデルで低い PTP 補正を提供することがわかっています。ただし、N9K-C9332D-H2R、N9K-C93400LD-H1、およびN9K-X9400-16W（N9K-C9408）は、同期間隔 -3 および遅延要求間隔 -3 の使用率が向上することが知られています。

（注） パフォーマンスは、PTP ピアデバイスの仕様などの外部要因にも依存します。ご使用の環境でテストして、最適な間隔を微調整することをお勧めします。

- リーフスイッチのフロント パネル ポートの場合、PTP はインターフェイスおよび VLAN ごとに有効にできますが、PTPがグローバルに有効化された後に、PTP はすべての適切なファブリック リンク（リーフスイッチとスパイン スイッチ、tier-1 および tier-2 リーフスイッチ間のインターフェイス、およびIPN/ISN向けのインターフェイス）で自動的に有効化されます。適切なファブリック リンクは、ftag0ツリーに属するインターフェイスです。

- Cisco ACI インターフェイス上の IPN/ISN への PTP は、ネイティブ VLAN 1 で有効で、VLAN タグなしで送信されます。ISN/IPN ノードのインターフェイスは、VLAN タグなしで、または VLAN ID 4 を使用して Cisco ACI スパイン スイッチに PTP パケットを送信できます。これは、PTP に関係なく、IPN/ISN 接続で自動的に有効です。
- リーフスイッチのフロントパネルインターフェイスでPTPを使用するには、PTPをグローバルに有効にする必要があります。つまり、ファブリック リンクで PTP を有効にしないと、リーフスイッチのフロント パネル ポートで PTP を有効にすることはできません。
- `tn-mgmt` および `tn-infra` を使用した PTP 構成はサポートされていません。
- PTP は、インターフェイスごとに 1 つの VLAN でのみ有効にできます。
- L3Out SVI のインターフェイスおよび VLAN で PTP を有効にすることはできません。EPG を使用して、同じインターフェイス上の別の VLAN で PTP を有効にすることができます。
- ユニキャスト マスター ポートとして構成できるのは、リーフスイッチのフロント パネル インターフェイスだけです。インターフェイスをユニキャスト クライアント ポートとして構成することはできません。ユニキャスト ポートはスパイン スイッチではサポートされていません。
- ユニキャスト ネゴシエーションはサポートされていません。
- PC または vPC が個々のメンバー ポートで PTP を構成する NX-OS などのデバイスに接続されている場合、ユニキャスト モードは PC または vPC では機能しません。
- PTP と MACSec を同じインターフェイスに構成することはできません。
- PTP がグローバルに有効になっている場合、ファブリックを通過するトラフィックの遅延を測定するために、Cisco ACI はある ACI スイッチ ノードから別の ACI スイッチ ノードに移動するトラフィックに Cisco タイムスタンプ タグ付け（TTag）を追加します。これにより、このようなトラフィックに 8 バイトが追加されます。通常、パケットが ACI ファブリックの外部に送信されるときに TTag が削除されるため、ユーザはこの導入に関してアクションを実行する必要はありません。ただし、Cisco ACI マルチポッド のセットアップが構成されている場合、ポッド間を通過するユーザー トラフィックは、VXLAN の内部ヘッダーに TTag を保持します。このような場合、IPN 内のすべての非 ACIデバイスとともに、Inter-Pod Network（IPN）に面する ACI スパイン スイッチ インターフェイスで MTU サイズを 8 バイト増やします。TTag は VXLAN ペイロード内に埋め込まれているため、IPN デバイスは TTag をサポートする必要も、認識する必要もありません。
- PTP がグローバルに有効になっている場合、スパイン ノードを通過して ERSPAN 接続先に到達する ERSPAN トラフィックには、イーサタイプ 0x8988 の Cisco タイムスタンプ タギング（TTag）があります。元のユーザ トラフィックへの影響はありません。
- PTP をサポートしないリーフスイッチが存在する場合は、IPN または PTP をサポートするリーフスイッチを使用して、外部グランドマスターをすべてのスパイン スイッチに接続する必要があります。グランドマスターがスパイン スイッチの 1 つまたはサブセットに接続されている場合、スパインからの PTP メッセージは、ftag0 ツリーのステータスに応じて、他のスイッチに到達する前に、サポートされていないリーフスイッチによってブロックされる場合があります。リーフおよびスパイン スイッチ内の PTP は、各ポッド内のすべて

のリーフおよびスパイン スイッチ間のループフリー マルチキャスト接続のために Cisco ACI インフラ ISIS に基づいて自動的に構築される ftag0 ツリーに基づいて有効になります。

- PTP テレコム プロファイルが展開されている場合、T-BC が T-GM とロックするには、テレコム グランドマスター クロック（T-GM）とテレコム境界クロック（T-BC）のタイムスタンプが 2 秒以内である必要があります。
- VMM ドメイン統合を使用してリーフ ノード インターフェイスに展開されている VLAN で PTP を有効にすることはできません。
- ACI リリース 6.1(3) 以降、PTP はファブリック リンク（ACI リーフ ノードとスパイン ノード間のリンク）でのみ N9K-C9408 の N9K-X9400-16W でサポートされます。ファブリック リンクの PTP は、ファブリック全体のグローバル設定であることに注意してください。有効にすると、サポートされていないモジュールまたはスイッチを除き、ファブリック内のすべてのファブリック リンクで有効になります。ただし、N9K-C9408 は、サポートされていない場合でも、すべてのモジュールで PTP を有効にします。たとえば、N9K-C9408 に PTP で認定されていない N9K-X9400-8D または N9K-X9400-22L が含まれている場合、N9K-C9408 のすべてのファブリック リンクで PTP が有効になります。ただし、このようなサポートされていないモジュールを介したクロック同期は信頼できません。サポートされていないモジュールを介したクロック同期を使用しないでください。

PTP の設定

PTP 構成の基本フロー

以下のステップで、PTP 構成プロセスの概要を示します。

手順

ステップ 1 PTP をグローバルに有効にし、すべてのファブリック インターフェイスの PTP パラメータを設定します。

ステップ 2 PTP テレコム プロファイル（G.8275.1）の場合のみ、PTP ノード ポリシーを作成し、スイッチ ポリシー グループを介してスイッチ プロファイルに適用します。

ステップ 3 **[ファブリック（Fabric）] > [アクセスポリシー（Access Policies）] > [ポリシー（Policies）] > [グローバル（Global）]** の下でリーフ フロント パネル インターフェイスの PTP ユーザープロファイルを作成します。

ステップ 4 PTP ユーザープロファイルを使用して、**[EPG] > [静的ポート（Static Ports）]** で PTP を有効にします。

ステップ 5 PTP ユーザープロファイルを使用して、**[L3Out] > [論理インターフェイス プロファイル（Logical Interface Profile）] > [ルーテッドまたはサブインターフェイス（Routed or Sub-Interface）]** で PTP を有効にします。

PTP ポリシーをグローバルに構成し、GUI を使用したファブリック インターフェイス向け PTP ポリシーの構成

この手順では、Cisco Application Policy Infrastructure Controller（APIC）GUI を使用して、高精度時間プロトコル（PTP）をグローバルに、およびファブリック インターフェイスに対して有効にします。PTP がグローバルに有効になっている場合、進行中の TEP から TEP への遅延測定は自動的に有効になります。

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）]** の順に選択します。

ステップ 2 ナビゲーションウィンドウで、**[PTP と遅延測定（PTP and Latency Measurement）]** を選択します。

ステップ 3 [Work（作業）] ペインで、目的の構成に合わせてインターフェース プロパティを設定します。少なくとも、**[高精度時間プロトコル（Precision Time Protocol）]** を **[有効（Enabled）]** に設定する必要があります。

フィールドの詳細については、オンライン ヘルプ ページを参照してください。指定した間隔値が選択済みの PTP プロファイル標準規格の範囲外である場合、その構成は拒否されます。

PTP プロファイル、間隔、およびタイムアウト フィールドは、ファブリック リンクに適用されます。他のフィールドは、すべてのリーフスイッチとスパイン スイッチに適用されます。

ステップ 4 [送信（Submit）] をクリックします。

GUI を使用したスイッチ ポリシーを使用して PTP ノードポリシーを構成、およびポリシーをスイッチ プロファイルに適用する

リーフ ノードが PTP テレコム プロファイル（G.8275.1）を実行するには、PTP ノード ポリシーが必要です。これは、追加のパラメータで代替 BMCA を使用するためです。また、ドメイン番号、優先度 1、優先度 2 の許容範囲が他の PTP プロファイルと異なります。リーフスイッチ プロファイルとポリシー グループを使用して、PTP ノード ポリシーをリーフスイッチに適用できます。

（注） メディア プロファイルの展開では、ノード ポリシーを作成する必要はありません。

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）] ウィンドウで、**[スイッチ（Switches）] > [リーフ スイッチ（Leaf Switches）] > [プロファイル（Profiles）]** をクリックします。

ステップ 3 **[プロファイル（Profiles）]** を右クリックして **[リーフ プロファイルの作成（Create Leaf Profile）]** を選択します。

ステップ 4 **[リーフ プロファイルの作成（Create Interface Profile）]** ダイアログボックスの **[名前（Name）]** フィールドに、プロファイルの名前を入力します。

ステップ 5 **[リーフ セレクター（Leaf Selectors）]** セクションで、**[+]** をクリックします。

ステップ 6 名前を入力し、スイッチを選択して、ポリシー グループの作成を選択します。

ステップ 7 **[アクセス スイッチ ポリシー グループの作成（Create Access Switch Policy Group）]** ダイアログで、ポリシー グループの名前を入力します。

ステップ 8 **[PTP ノード ポリシー（PTP Node Policy）]** ドロップダウンリストで、**[PTP ノード プロファイルの作成（Create PTP Node Profile）]** を選択します。

ステップ 9 **[PTP ノード プロファイルの作成（Create PTP Node Profile）]** ダイアログで、構成に必要な値を設定します。

- **[ノード ドメイン（Node Domain）]**：値は 24 ～ 43 の間である必要があります。同じ PTP トポロジにある必要があるテレコム リーフ ノードは、同じドメイン番号を使用する必要があります。
- **[優先順位 1（Priority 1）]**：値は 128 にする必要があります。
- **[優先順位 2（Priority 2）]**：値は 0 ～ 255（0 と 255 を含む）である必要があります。

フィールドの詳細については、オンライン ヘルプ ページを参照してください。

ステップ 10 **[送信（Submit）]** をクリックします。

[PTP ノード プロファイルの作成（Create PTP Node Profile）] ダイアログボックスが閉じます。

ステップ 11 **[アクセス スイッチ ポリシー グループの作成（Create Access Switch Policy Group）]** ダイアログで、構成に必要な他のポリシーを設定します。

ステップ 12 **[送信（Submit）]** をクリックします。

[アクセス スイッチ ポリシー グループの作成（Create Access Switch Policy Group）] ダイアログが閉じます。

ステップ 13 **[リーフ セレクター（Leaf Selectors）]** セクションで、**[更新（Update）]** をクリックします。

ステップ 14 [次へ（Next）] をクリックします。

ステップ 15 **[ステップ 2（STEP 2）] > [関連付け（Associations）]** 画面で、必要に応じてインターフェイス プロファイルを関連付けます。

ステップ 16 **[完了（Finish）]** をクリックします。

GUI を使用したリーフスイッチ フロント パネル ポート用 PTP ユーザープロファイルの作成

この手順では、Cisco Application Policy Infrastructure Controller（APIC）GUI を使用してリーフスイッチのフロント パネル ポートの PTP ユーザープロファイルを作成します。PTP ユーザー

プロファイルは EPG または L3Out を使用してリーフスイッチ フロント パネル インターフェイスに適用されます。

始める前に

外部デバイスに面するリーフスイッチのフロント パネル ポートで PTP を使用するには、PTP をグローバルに有効にする必要があります。

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 ナビゲーションウィンドウで、**[ポリシー（Policies）]** > **[グローバル（Global）]** > **[PTP ユーザープロファイル（PTP User Profile）]** を選択します。

ステップ 3 **[PTP ユーザープロファイル（PTP User Profile）]** を右クリックし、**[PTP ユーザープロファイルの作成（Create PTP User Profile）]** を選択します。

ステップ 4 **[PTP ユーザープロファイルの作成（Create PTP User Profile）]** ダイアログで、構成に必要な値を設定します。

フィールドの詳細については、オンライン ヘルプ ページを参照してください。指定した間隔値が選択済みの PTP プロファイル標準規格の範囲外である場合、その構成は拒否されます。

ステップ 5 [送信（Submit）] をクリックします。

GUI を使用して EPG 静的ポートで PTP を有効化する

この手順では、Cisco Application Policy Infrastructure Controller（APIC）GUI を使用して EPG 静的ポートで PTP を有効にします。PTP は、マルチキャスト ダイナミック、マルチキャスト マスター、またはユニキャスト マスター モードで有効にできます。

始める前に

最初にリーフスイッチのフロント パネル ポートの PTP ユーザープロファイルを作成し、PTP をグローバルに有効にする必要があります。

手順

ステップ 1 メニュー バーで、[テナント（Tenants）] > [すべてのテナント（ALL Tenants）] の順に選択します。 >

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーションウィンドウで、**[テナント（Tenant）*tenant_name*]** > **[アプリケーション プロファイル（Application Profiles）** > **[*app_profile_name*]** > **[アプリケーション EPG（Application EPGs）]** > **[*app_epg_name*]** > **[静的ポート（Static Ports）]** > **[*static_port_name*]** の順に選択します。

ステップ 4 [作業（Work）] ペインの **[PTP 状態（PTP State）]** トグルで、**[有効（Enable）]** を選択します。**[PTP 状態（PTP State）]** を表示するには、下にスクロールする必要がある場合があります。

PTP 関連のフィールドが表示されます。

ステップ 5 構成に必要な PTP フィールドを構成します。

- **[PTP モード（PTP Mode）]**：必要に応じて、**[マルチキャスト ダイナミック（multicast dynamic）]**、**[マルチキャスト マスター（multicast master）]**、または **[ユニキャスト マスター（unicast master）]** を選択します。
- **[PTP 送信元アドレス（PTP Source Address）]**：このインターフェイスおよびVLANからのPTPパケットは、指定された IP アドレスを送信元として送信されます。リーフスイッチの TEP アドレスは、デフォルトで、または値として「0.0.0.0」を入力した場合に使用されます。この値は、マルチキャスト モードではオプションです。ユニキャスト モードには、ブリッジドメイン SVI または EPG SVI を使用します。送信元 IP アドレスは、ユニキャスト モードでは接続済み PTP ノードによって到達可能である必要があります。
- **[PTP ユーザープロファイル（PTP User Profile）]**：リーフスイッチのフロント パネル ポート用に作成した PTP ユーザープロファイルを選択して、メッセージ間隔を指定します。

さらにフィールドの詳細については、オンライン ヘルプ ページを参照してください。

ノード レベルの構成は、PTP テレコム プロファイル（G.8275.1）が展開されているノードのファブリック レベルの構成よりも優先されます。

ステップ 6 [送信（Submit）] をクリックします。

GUI を使用して L3Out インターフェイスで PTP を有効化する

この手順では、Cisco Application Policy Infrastructure Controller（APIC）GUI を使用して L3Out インターフェイスでPTPを有効にします。PTPは、マルチキャスト ダイナミック、マルチキャスト マスター、またはユニキャスト マスター モードで有効にできます。

始める前に

最初にリーフスイッチのフロント パネル ポートの PTP ユーザープロファイルを作成し、PTP をグローバルに有効にする必要があります。

手順

ステップ 1 メニュー バーで、[テナント（Tenants）] > [すべてのテナント（ALL Tenants）] の順に選択します。 >

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーションウィンドウから、**[テナント（Tenant）]*[tenant_name]*** > **[ネットワーキング（Networking）]** > **[L3Outs]** > ***[l3Out_name]*** > **[論理ノード プロファイル（Logical Node Profiles）]** > ***[node_profile_name]*** > **[論**

理インターフェイス プロファイル（**Logical Interface Profiles**）] > ***[interface_profile_name]*** の順に移動します。

ステップ 4 [作業（Work）]ペインで、必要に応じて**[Policy（ポリシー）]**>**[ルーテッドサブインターフェイス（Routed Sub-interfaces）]**、または**[Policy（ポリシー）]**>**[ルーテッドインターフェイス（Routed Interfaces）]** を選択します。

ステップ 5 既存の L3Out で PTP を有効にする場合は、次のサブステップを実行します。

a) 目的のインターフェイスをダブルクリックして、そのプロパティを表示します。

b) 必要に応じて下にスクロールしてPTPプロパティを見つけ、**[PTP状態（PTP State）]**を**[有効（Enable）]**に設定して、EPG 静的ポートに使用したのと同じ値を入力します。

フィールドの詳細については、オンライン ヘルプ ページを参照してください。

c) **[送信（Submit）]** をクリックします。

ステップ 6 新しい L3Out で PTP を有効にする場合は、次のサブステップを実行します。

a) 表の右上にある **[+]** をクリックします。

b) **[ステップ 1（Step 1）] > [アイデンティティ（Identity）]** で、適切な値を入力します。

c) **[ステップ 2（Step 2）] > [PTP の構成（Configure PTP）]** で、**[PTP 状態（PTP State）]** を **[有効（Enable）]** に設定し、EPG 静的ポートに使用したのと同じ値を入力します。

フィールドの詳細については、オンライン ヘルプ ページを参照してください。

d) **[完了（Finish）]** をクリックします。

PTP ポリシーをグローバルに構成し、REST API を使用したファブリック インターフェイス向け PTP ポリシーの構成

この手順では、REST API を使用して、ファブリック インターフェイスに対して PTP をグローバルに有効にします。PTP がグローバルに有効になっている場合、進行中の TEP から TEP への遅延測定は自動的に有効になります。

ファブリック インターフェイスに対して PTP ポリシーをグローバルに構成するには、次の例のような REST API POST を送信します。

POST: `/api/mo/uni/fabric/ptpmode.xml`

```
<latencyPtpMode
    state="enabled"                         # PTP admin state
    systemResolution="11"                   # Latency Resolution (can be skipped for
    prio1="255"                             PTP)
    prio2="255"                             # Global Priority1
    globalDomain="0"                        # Global Priority2
    fabProfileTemplate="aes67"              # Global Domain
    fabAnnounceIntvl="1"                    # PTP Profile
    fabSyncIntvl="-3"                       # Announce Interval (2^x sec)
    fabDelayIntvl="-2"                      # Sync Interval (2^x sec)
    fabAnnounceTimeout="3"                  # Delay Request Interval (2^x sec)
/>                                          # Announce Timeout
```

REST API を使用したスイッチ ポリシーを使用して PTP ノード ポリシーを構成、およびポリシーをスイッチ プロファイルに適用する

リーフ ノードが PTP テレコム プロファイル（G.8275.1）を実行するには、PTP ノード ポリシーが必要です。これは、追加のパラメータで代替 BMCA を使用するためです。また、ドメイン番号、優先度 1、優先度 2 の許容範囲が他の PTP プロファイルと異なります。リーフスイッチ プロファイルとポリシー グループを使用して、PTP ノード ポリシーをリーフスイッチに適用できます。

POST: `/api/mo/uni.xml`

```
<infraInfra>
    <!-- Switch Profile -->
    <infraNodeP name="L101_SWP" dn="uni/infra/nprof-L101_SWP">
        <infraRsAccPortP tDn="uni/infra/accportprof-L101_IFP"/>
        <infraLeafS name="L101" type="range">
            <infraNodeBlk name="L101" to_="101" from_="101"/>
            <!-- Associate Switch Policy Group for node-101 -->
            <infraRsAccNodePGrp tDn="uni/infra/funcprof/accnodepgrp-Telecom_PG_1"/>
        </infraLeafS>
    </infraNodeP>

    <infraFuncP>
        <!-- Switch Policy Group with PTP Node and SyncE Policy -->
        <infraAccNodePGrp name="Telecom_PG_1"
          dn="uni/infra/funcprof/accnodepgrp-Telecom_PG_1">
            <infraRsSynceInstPol tnSynceInstPolName="SyncE_QL1"/>
            <infraRsPtpInstPol tnPtpInstPolName="Telecom_domain24"/>
        </infraAccNodePGrp>
    </infraFuncP>

    <!-- PTP Node policy -->
    <ptpInstPol
      dn="uni/infra/ptpInstP-Telecom_domain24"
      name="Telecom_domain24"
      operatingMode="hybrid"
      nodeProfile="telecom_full_path"
      nodePrio1="128"
      nodePrio2="128"
      nodeDomain="24"/>

    <!-- SyncE Node policy -->
    <synceInstPol
      dn="uni/infra/synceInstP-SyncE_QL1"
      name="SyncE_QL1"
      qloption="op1"
      adminSt="disabled"/>
</infraInfra>
```

REST API を使用したリーフスイッチ フロント パネル ポート用 PTP ユーザープロファイルの作成

PTP ユーザープロファイルは EPG または L3Out を使用してリーフスイッチ フロント パネル インターフェイスに適用されます。また、外部デバイスに面するリーフスイッチのフロント パネル ポートで PTP を使用するには、PTP をグローバルに有効にする必要があります。

PTP ユーザープロファイルを作成するには、次の例のように REST API POST を送信します。

POST: `/api/mo/uni/infra/ptpprofile-Ptelecomprofile.xml`

```
<ptpProfile
    name="Ptelecomprofile"                  # PTP user profile name
    profileTemplate="telecom_full_path"     # PTP profile
    announceIntvl="-3"                      # Announce interval (2^x sec)
    syncIntvl="-4"                          # Sync interval (2^x sec)
    delayIntvl="-4"                         # Delay request interval (2^x sec)
    announceTimeout="3"                     # Announce timeout
    annotation=""                           # Annotation key

                                            (Only for Telecom ports)
    ptpoeDstMacType="forwardable"           # Destination MAC for PTP messages
    ptpoeDstMacRxNoMatch="replyWithCfgMac"  # Packet handling
    localPriority="128"                     # Port local priority

                                            (Only for non-Telecom ports on a telecom
    nodeProfileOverride="no"                leaf)
/>                                          # Node profile override
```

REST API を使用した EPG 静的ポートでの PTP の有効化

EPG 静的ポートで PTP を有効にする前に、最初にリーフスイッチのフロント パネル ポートの PTP ユーザープロファイルを作成し、PTP をグローバルに有効にする必要があります。

EPG 静的ポートで PTP を有効にするには、次の例のように REST API POST を送信します。

POST: `/api/mo/uni/tn-TK/ap-AP1/epg-EPG1-1.xml`

マルチキャスト モード

```
<fvRsPathAtt
  tDn="topology/pod-1/paths-101/pathep-[eth1/1]"
  encap="vlan-2011">
    <ptpEpgCfg
      ptpMode="multicast">                          # PTP mode
        <ptpRsProfile                               # PTP user profile
          tDn="uni/infra/ptpprofile-PTP_AES"/>
    </ptpEpgCfg>
</fvRsPathAtt>
```

`ptpMode` パラメータに可能な値は次のとおりです。

- `multicast`：マルチキャスト ダイナミック。
- `multicast-master`：マルチキャスト マスター。

ユニキャスト モード

```
<fvRsPathAtt
  tDn="topology/pod-1/paths-101/pathep-[eth1/1]"
  encap="vlan-2011">
    <ptpEpgCfg
      srcIp="192.168.1.254"                         # PTP source IP address
      ptpMode="unicast-master">                     # PTP mode
        <ptpRsProfile                               # PTP user profile
          tDn="uni/infra/ptpprofile-PTP_AES"/>      # PTP unicast destination
        <ptpUcastIp dstIp="192.168.1.11"/>            IP address
    </ptpEpgCfg>
</fvRsPathAtt>
```

ptpEpgCfg が存在する場合は、PTP が有効になっていることを意味します。そのインターフェイスで PTP を無効にする必要がある場合は、ptpEpgCfg を削除します。

REST API を使用して L3Out インターフェイスで PTP を有効化する

この手順では、REST API を使用して L3Out インターフェイスで PTP を有効にします。L3Out インターフェイスで PTP を有効にする前に、最初にリーフスイッチのフロント パネル ポートの PTP ユーザープロファイルを作成し、PTP をグローバルに有効にする必要があります。

L3Out インターフェイスで PTP を有効にするには、次の例のように REST API POST を送信します。

POST: /api/node/mo/uni/tn-TK/out-BGP/lnodep-BGP_nodeProfile/lifp-BGP_IfProfile.xml

マルチキャスト モード

```
<l3extRsPathL3OutAtt
  tDn="topology/pod-1/paths-103/pathep-[eth1/11]"
  addr="11.0.0.1/30" ifInstT="l3-port">
    <ptpRtdEpgCfg
      ptpMode="multicast">                          # PTP mode
        <ptpRsProfile                               # PTP user profile
          tDn="uni/infra/ptpprofile-PTP_AES"/>
    </ptpRtdEpgCfg>
</l3extRsPathL3OutAtt>
```

ptpMode パラメータに可能な値は次のとおりです。

- multicast：マルチキャスト ダイナミック。
- multicast-master：マルチキャスト マスター。

ユニキャスト モード

```
<l3extRsPathL3OutAtt
  tDn="topology/pod-1/paths-103/pathep-[eth1/11]"
  addr="11.0.0.1/30" ifInstT="l3-port">
    <ptpRtdEpgCfg
      srcIp="11.0.0.1"                              # PTP source IP address
      ptpMode="unicast-master">                     # PTP mode
        <ptpRsProfile                               # PTP user profile
          tDn="uni/infra/ptpprofile-PTP_AES"/>      # PTP unicast destination
        <ptpUcastIp dstIp="11.0.0.4"/>                IP address
    </ptpRtdEpgCfg>
</l3extRsPathL3OutAtt>
```

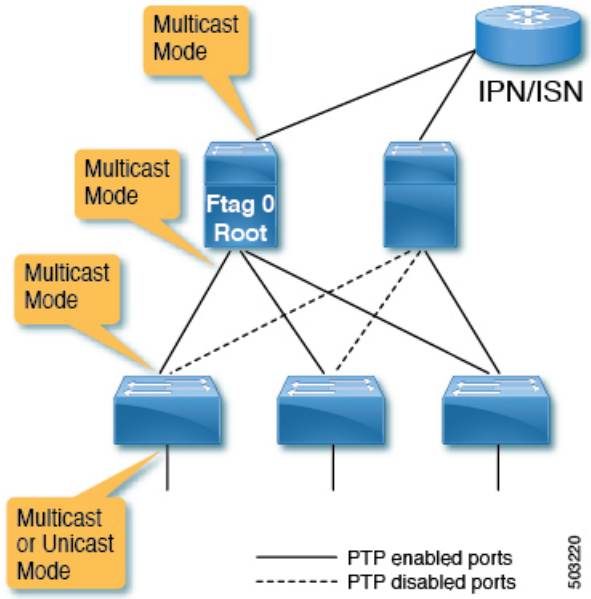
ptpRtdEpgCfg が存在する場合は、PTP が有効になっていることを意味します。そのインターフェイスで PTP を無効にする必要がある場合は、ptpRtdEpgCfg を削除します。

Cisco ACI の PTP ユニキャスト、マルチキャスト、および混合モード

デフォルトでは、すべての PTP インターフェイスはマルチキャスト モードで実行されます。ユニキャスト モードで構成できるのは、リーフスイッチのフロント パネル インターフェイス

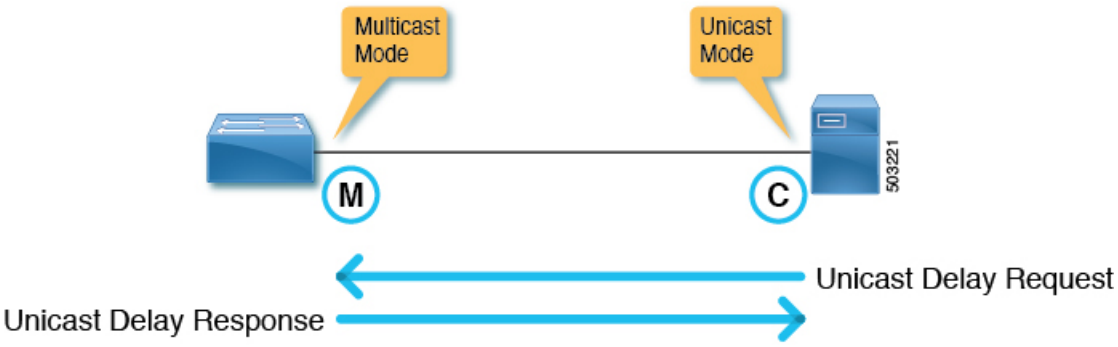
だけです。ユニキャスト マスター ポートのみがサポートされます。ユニキャスト クライアント ポートはサポートされていません。

図 *1*: マルチキャストまたはユニキャスト モード



混合モード（ユニキャスト遅延応答で応答する PTP マルチキャスト ポート）は、ポートがユニキャスト遅延要求を受信すると、マルチキャスト モードの PTP マスター ポートで自動的にアクティブになります。混合モードは、本質的にマルチキャスト マスターとユニキャスト クライアントです。

図 *2*: 混合モード



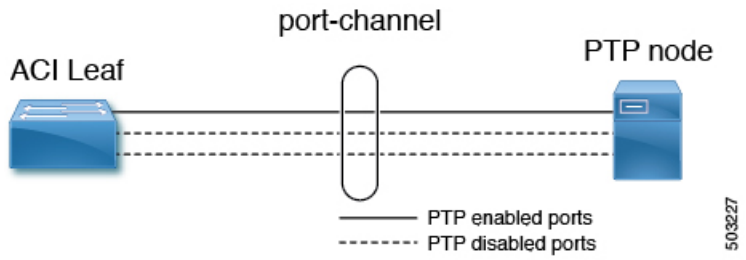
1 つのリーフスイッチは、複数の PTP ユニキャスト マスター ポートを持つことができます。各ユニキャスト マスター ポートでサポートされるクライアント スイッチ IP アドレスの数は 2 です。さらに多くの IP アドレスを構成できますが、修飾することはできません。PTP ユニキャスト マスター ポートと PTP マルチキャスト ポートは、同じスイッチに構成できます。

Cisco ACI での PTP ユニキャスト モードの制限事項

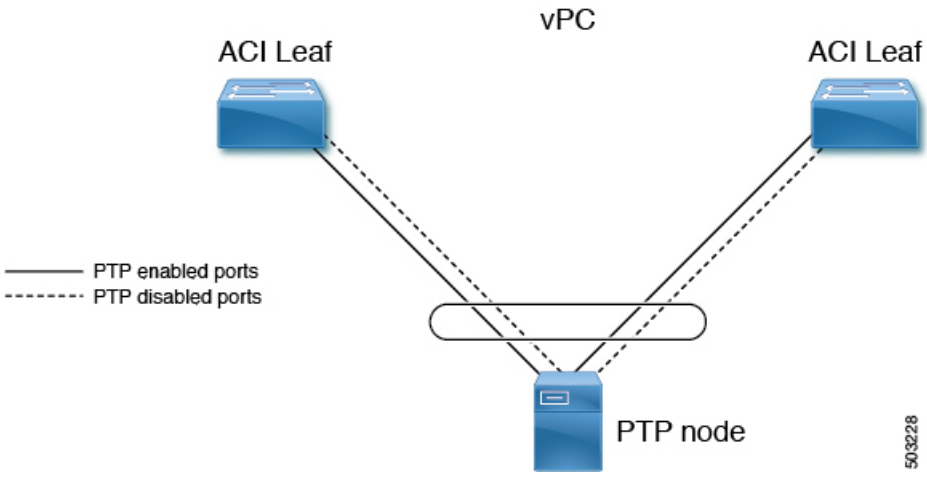
PTP ユニキャスト ネゴシエーションはサポートされていません。Cisco Application Centric Infrastructure（ACI）には、Cisco ACI が他のノードからの要求を許可する、または要求するメッセージを要求するユニキャスト ネゴシエーションがないため、Cisco ACI PTP ユニキャスト マスター ポートは、クライアント ノードから要求を受信せずに、Cisco Application Policy Infrastructure Controller（APIC）を使用して構成された間隔で、`Announce`、`Sync`、および `Follow_Up` メッセージを送信します。ユニキャスト `Delay_Response` メッセージは、ユニキャスト クライアント ノードからの `Delay_Request` メッセージへの応答として送信されます。ユニキャスト マスター ポートはユニキャスト要求をリッスンせずに `Sync` などの PTP メッセージを送信するため、Cisco ACI PTP ユニキャスト ポートではベスト マスター クロック アルゴリズム（BMCA）が計算されません。

Cisco ACI での PTP PC および vPC の実装

ポート チャネル（PC）および仮想ポート チャネル（vPC）の場合、メンバー ポートごとではなく、PC または vPC ごとに PTP が有効になります。 Cisco Application Centric Infrastructure（ACI）では、親 PC または vPC の各メンバー ポートで個別に PTP を有効にすることはできません。



Cisco ACI PC または vPC で PTP が有効になっている場合、リーフスイッチは PTP が有効になっている PC からメンバー ポートを自動的に選択します。PTP 対応のメンバー ポートに障害が発生すると、リーフスイッチは、まだ稼働している別のメンバー ポートを選択します。PTP ポートのステータスは、以前の PTP 対応メンバー ポートから継承されます。



PTP が Cisco ACI vPC ポートで有効になっている場合、vPC は 2 つのリーフスイッチ上の 2 つのポートチャネルの論理バンドルですが、動作は通常のポートチャネルで有効になっている PTP と同じです。vPC ピア リーフスイッチ間の PTP 情報の同期など、vPC には特定の実装はありません。

（注） PC または vPC が個々のメンバー ポートで PTP を構成する NX-OS などのデバイスに接続されている場合、ユニキャスト モードは PC または vPC では機能しません。

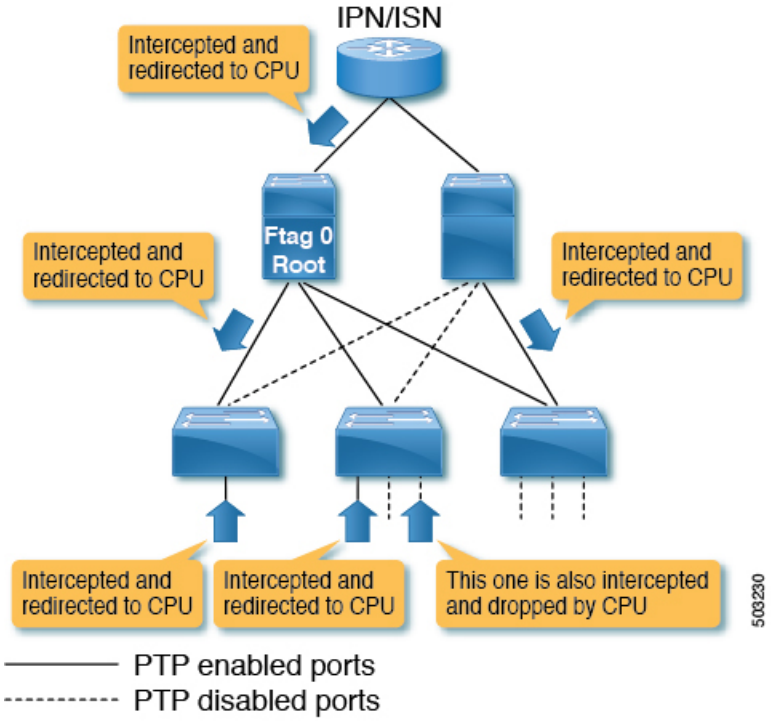
PTP パケット フィルタリングおよびトンネリング

PTP パケット フィルタリング

PTPがファブリック ポートでパケットを処理し、PTPがグローバルに有効になっている場合、すべてのスパインおよびリーフスイッチには、ファブリック ポートからのすべての着信 PTP パケットを CPU にリダイレクトするための内部フィルタがあります。

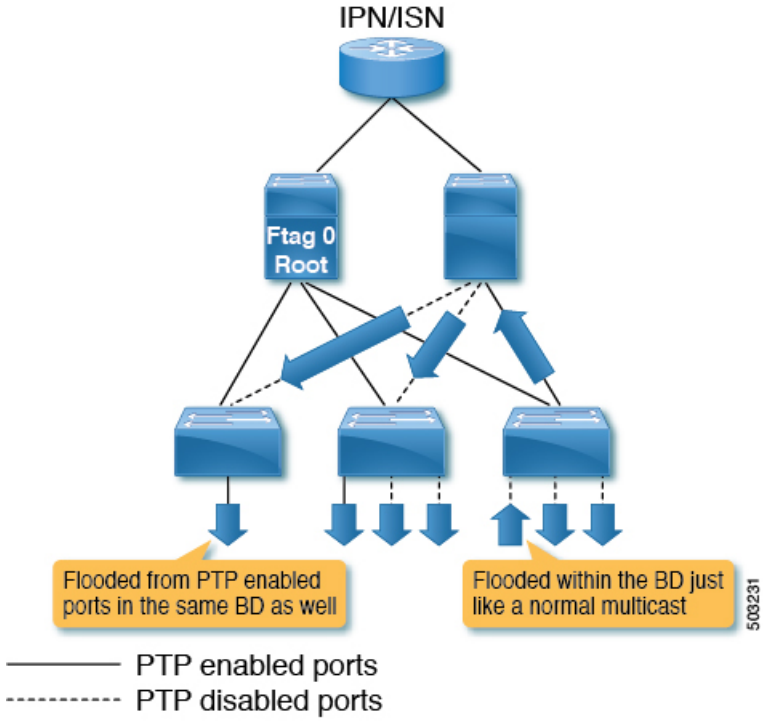
PTP がフロント パネル ポートでパケットを処理し、特定のリーフスイッチの少なくとも 1 つのリーフスイッチ フロント パネル ポートで PTP が有効になっている場合、リーフスイッチには、フロント パネル ポートからのすべての着信 PTP パケットをリダイレクトする内部フィルタがあります。PTP が有効になっていないフロント パネル ポートから PTP パケットを受信した場合でも、パケットは引き続き代行受信され、CPU にリダイレクトされた後、破棄されます。

図 *3: PTP* 対応フロント パネル ポートを備えたリーフスイッチのフロント パネルでのパケット フィルタリング



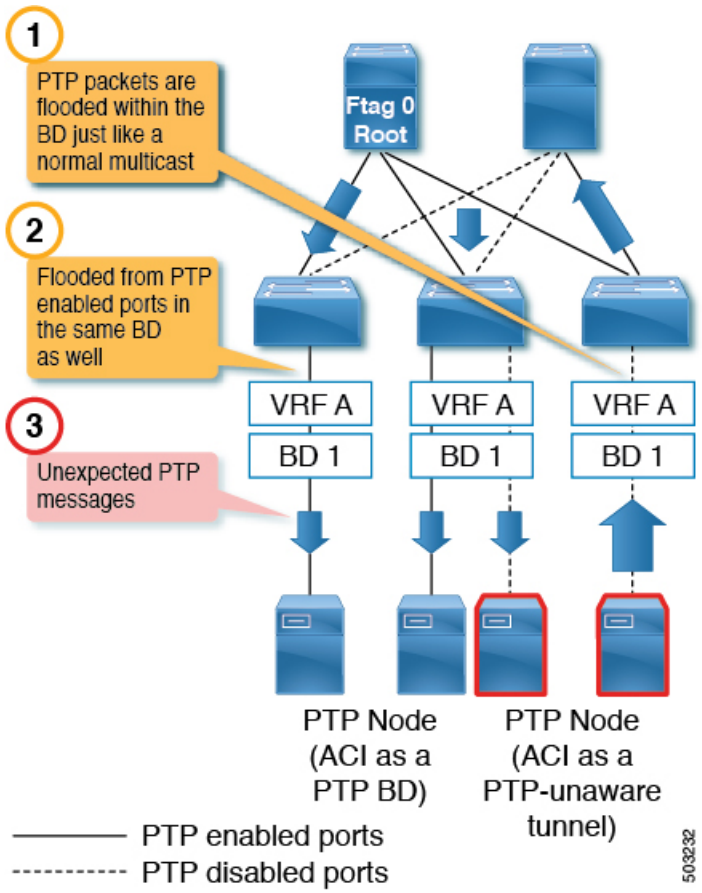
PTP がフロント パネル ポートでパケットを処理し、特定のリーフスイッチのすべてのリーフスイッチ フロント パネル ポートで PTP が有効になっていない場合、リーフスイッチには、フロント パネル ポートからの PTP パケットをリダイレクトする内部フィルタがありません。このようなリーフスイッチのフロント パネル ポートで PTP パケットを受信すると、パケットは通常のマルチキャスト パケットとして処理され、VxLAN を使用して他のスイッチに転送またはフラッディングされます。Cisco Application Centric Infrastructure（ACI）スイッチによって代行受信されることになっている PTP パケットは、リーフスイッチとスパイン スイッチの間でも VxLAN でカプセル化されないため、他のスイッチもこれを通常のマルチキャスト パケットとして処理します。これにより、フロントパネルのポートで PTP が有効になっている他のリーフスイッチで、予期しない PTP 動作が発生する可能性があります。詳細については、Cisco ACI PTP 境界クロックまたは PTP 非認識トンネルとして （69 ページ） を参照してください。

図 *4 : PTP* 対応フロント パネル ポートを装備しないリーフスイッチのフロント パネルでのパケット フィルタリング

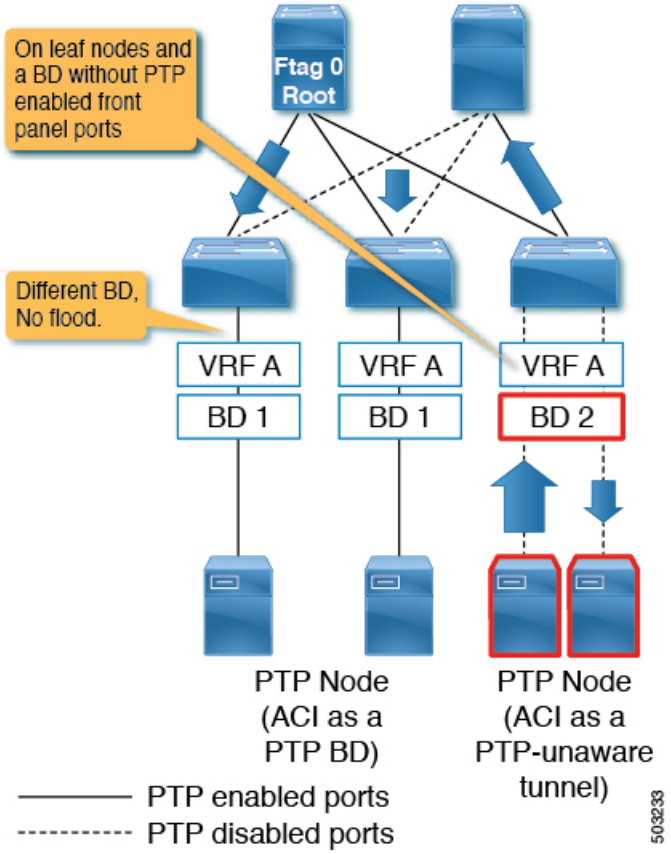


Cisco ACI PTP 境界クロックまたは PTP 非認識トンネルとして

PTP フロント パネル ポートのないリーフスイッチからの PTP パケットは、ブリッジドメインでフラッディングされます。次の図に示すように、Cisco Application Centric Infrastructure（ACI）が PTP メッセージを PTP 境界クロックとして再生成することを期待する同じブリッジドメイン内の PTP ノードに対しても、パケットはフラッディングされます。

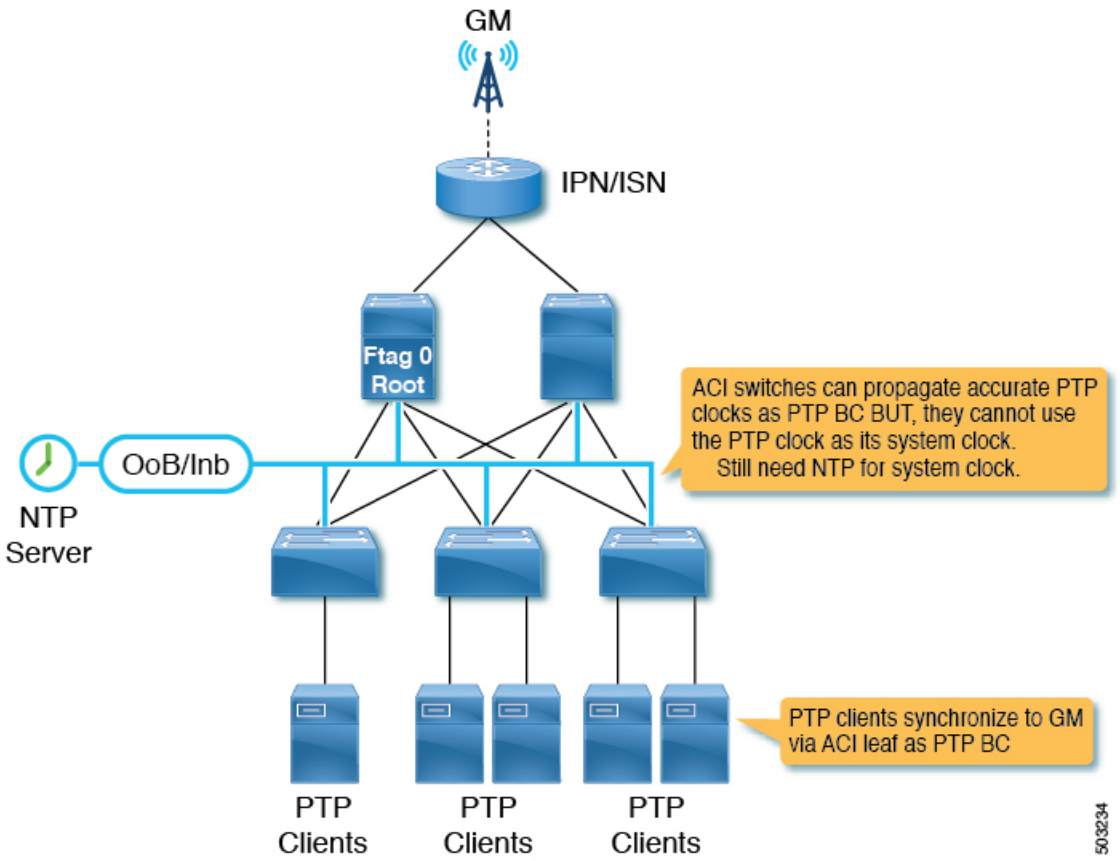


これにより、予期しないPTPパケットが原因で、PTPノードとその時間計算が混乱します。一方、PTP フロント パネル ポートを備えたリーフスイッチからの PTP パケットは常に代行受信され、PTPが有効になっていないポートでパケットが受信された場合でもトンネリングされません。したがって、同じブリッジドメインおよび同じリーフスイッチ上で、Cisco ACI がPTP境界クロックである必要がある PTP ノードと、Cisco ACI が PTP 非認識トンネルである必要があるPTPノードを混在させないでください。次の図に示す構成（異なるブリッジドメイン、異なるリーフスイッチ）がサポートされています。



PTP および NTP

Cisco Application Centric Infrastructure（ACI）スイッチは PTP 境界クロックとして動作し、グランドマスターから PTP クライアントに正確なクロックを提供します。ただし、Cisco ACI スイッチおよび Cisco Application Policy Infrastructure Controller（APIC）は、それらの PTP クロックを独自のシステム クロックとして使用できません。Cisco ACI スイッチと Cisco APIC には、独自のシステム クロックを更新するために NTP サーバーが必要です。



（注） Cisco ACI で PTP が正確かつ継続的に機能するためには、すべてのスイッチに NTP を構成して、システム クロックを PTP グランドマスターと同じように 100 ミリ秒の順番で正確に保つ必要があります。つまり、システム クロックの差は、PTP グランドマスターと比較して 100 ミリ秒未満でなければなりません。

PTP 検証

PTP 検証 CLI コマンドの概要

リーフスイッチの 1 つにログインし、次のコマンドを使用して PTP 構成を確認できます。

コマンド	目的
show ptp port interface *slot/port*	特定のインターフェイスの PTP パラメータを表示します。
show ptp brief	PTP のステータスを表示します。

コマンド	目的
show ptp clock	ローカルクロックのプロパティ（クロック ID など）を表示します。
show ptp parent	PTP の親のプロパティを表示します。
show ptp clock foreign-masters record	PTP プロセスが認識している外部マスターの状態を表示します。外部マスターごとに、出力に、クロック ID、基本的なクロック プロパティ、およびクロックがグランドマスターとして使用されているかどうかが表示されます。
show ptp counters [all |interface Ethernet *slot/port***]**	すべてのインターフェイスまたは指定したインターフェイスの PTP パケットカウンタを表示します。
show ptp corrections	最後の数個の PTP 修正を表示します。

PTP ポート情報の表示

次の例は、ポート インターフェイス情報を示しています。

```
f2-leaf1# vsh -c 'show ptp port int e1/1'
PTP Port Dataset: Eth1/1
Port identity: clock identity: 00:3a:9c:ff:fe:6f:a4:df
Port identity: port number: 0
PTP version: 2
Port state: Master
VLAN info: 20                              <--- PTP messages are sent on this PI-VLAN
Delay request interval(log mean): -2
Announce receipt time out: 3
Peer mean path delay: 0
Announce interval(log mean): 1
Sync interval(log mean): -3
Delay Mechanism: End to End
Cost: 255
Domain: 0
```

次の例は、指定された VLAN の情報を示しています。

```
f2-leaf1# show vlan id 20 extended

 VLAN Name                             Encap            Ports
 ---- -------------------------------- ---------------- ------------------------
 20   TK:AP1:EPG1-1                    vlan-2011        Eth1/1, Eth1/2, Eth1/3
```

PTP ポート ステータスの表示

次の例は、ポート ステータスの簡易バージョンを示しています。

```
f2-leaf1# show ptp brief

PTP port status
-----------------------------------
Port                  State
--------------------- ------------
```

```
Eth1/1                Master
Eth1/51               Passive
Eth1/52               Slave
```

PTP スイッチ情報の表示

次の例は、スイッチ ステータスの簡単なバージョンを示しています。

```
f2-leaf1# show ptp clock
PTP Device Type : boundary-clock
PTP Device Encapsulation : layer-3
PTP Source IP Address : 20.0.32.64            <--- Switch TEP. Like a router-id.
                                                   This is not PTP Source Address you
                                                   configure per port.
Clock Identity : 00:3a:9c:ff:fe:6f:a4:df      <--- PTP clock ID. If this node is
                                                   the grandmaster, this ID is the
                                                   grandmaster's ID.

Clock Domain: 0
Slave Clock Operation : Two-step
Master Clock Operation : Two-step
Slave-Only Clock Mode : Disabled
Number of PTP ports: 3
Configured Priority1 : 255
Priority1 : 255
Priority2 : 255
Clock Quality:
        Class : 248
        Accuracy : 254
        Offset (log variance) : 65535
Offset From Master : -8                       <--- -8 ns. the clock difference from the
                                                       closest parent (master)
Mean Path Delay : 344                         <--- 344 ns. Mean path delay measured by
                                                       E2E mechanism.
Steps removed : 2                             <--- 2 steps. 2 PTP BC nodes between the
                                                       grandmaster.

Correction range : 100000
MPD range : 1000000000
Local clock time : Thu Jul 30 01:26:14 2020
Hardware frequency correction : NA
```

グランドマスターと親（マスター）情報の表示

次の例は、PTP グランドマスターと親（マスター）の情報を示しています。

```
f2-leaf1# show ptp parent

PTP PARENT PROPERTIES

Parent Clock:
Parent Clock Identity: 2c:4f:52:ff:fe:e1:7c:1a          <--- closest parent (master)
Parent Port Number: 30
Observed Parent Offset (log variance): N/A
Observed Parent Clock Phase Change Rate: N/A

Parent IP: 20.0.32.65                                   <--- closest parent's PTP
                                                        source IP address
Grandmaster Clock:
Grandmaster Clock Identity: 00:78:88:ff:fe:f9:2b:13     <--- GM
Grandmaster Clock Quality:                              <--- GM's quality
        Class: 248
        Accuracy: 254
        Offset (log variance): 65535
```

```
        Priority1: 128
        Priority2: 255
```

次の例は、PTP 外部マスター クロック レコードを示しています。

```
f2-leaf1# show ptp clock foreign-masters record

P1=Priority1, P2=Priority2, C=Class, A=Accuracy,
OSLV=Offset-Scaled-Log-Variance, SR=Steps-Removed
GM=Is grandmaster

---------   ----------------------  ---  ----  ----  ---  -----  --------
Interface         Clock-ID          P1   P2    C     A    OSLV   SR
---------   ----------------------  ---  ----  ----  ---  -----  --------

Eth1/51   c4:f7:d5:ff:fe:2b:eb:8b    128  255   248   254  65535  1
Eth1/52   2c:4f:52:ff:fe:e1:7c:1a    128  255   248   254  65535  1
```

出力には、グランドマスター情報をスイッチおよびスイッチの接続インターフェイスに送信するマスタークロックが表示されます。ここでのクロック IDは、最も近いマスターの IDです。ID はグランドマスターの ID ではありません。このスイッチは 2 つの異なるポートからグランドマスターのデータを受信しているため、ポートの 1 つがパッシブになりました。

カウンターの表示

次の例は、マスター ポートのカウンターを示しています。

```
f2-leaf1# show ptp counters int e1/1

PTP Packet Counters of Interface Eth1/1:
------------------------------------------------------------------
Packet Type                TX                      RX
----------------    --------------------    --------------------
Announce                            4                       0
Sync                               59                       0
FollowUp                           59                       0
Delay Request                       0                      30
Delay Response                     30                       0
PDelay Request                      0                       0
PDelay Response                     0                       0
PDelay Followup                     0                       0
Management                          0                       0
```

マスター ポートは次のメッセージを送信する必要があります。

- アナウンス
- 同期
- FollowUp
- 対応遅延

マスター ポートは次のメッセージを受信する必要があります。

- 遅延要求

次の例は、クライアント ポートのカウンターを示しています。

```
f2-leaf1# show ptp counters int e1/52

PTP Packet Counters of Interface Eth1/52:
```

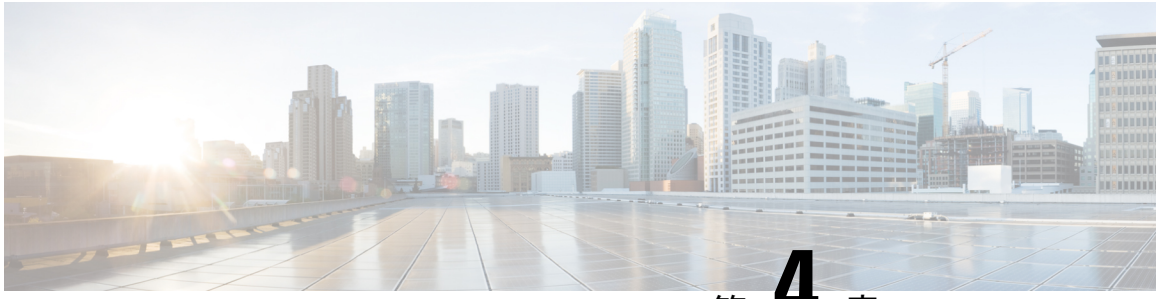
```
------------------------------------------------------------------
Packet Type                TX                    RX
---------------    --------------------    --------------------
Announce                            0                       4
Sync                                0                      59
FollowUp                            0                      59
Delay Request                      30                       0
Delay Response                      0                      30
PDelay Request                      0                       0
PDelay Response                     0                       0
PDelay Followup                     0                       0
Management                          0                       0
```

送受信されるメッセージは、マスター ポートの逆です。たとえば、`Delay Request` の Rx と `Delay Response` の Tx がマスター ポートでゼロである場合、クライアントは E2E 遅延メカニズムの `Delay Request` を開始する必要があるため、反対側は構成されていないか、クライアントとして正しく機能していません。

実際には、ポートの状態が過去に変更された可能性があるため、カウンター情報は例示されているほど整っていない場合があります。このような場合は、次のコマンドでカウンターをクリアします。

```
f2-leaf1# clear ptp counters all
```

（注） `PDelay_xxx` カウンターは P2P メカニズム用で、Cisco Application Centric Infrastructure（ACI）ではサポートされていません。



第 4 章

同期イーサネット（SyncE）

同期イーサネット（SyncE）について

サービスプロバイダー ネットワークで、Synchronous Optical Networking（SONET）と同期デジタル階層（SDH）機器を段階的に置き換えるイーサネット機器を使用する場合、イーサネットポート経由で高品質なクロック同期を提供するためには周波数を同期化することが必要です。周波数またはタイミング同期は、ネットワーク全体に精密周波数を配布する機能です。この文脈でのタイミングとは、精密な時刻ではなく、精密周波数を示します。

ITU G.781 に記述されている同期イーサネット（SyncE）により、必要な同期が物理レベルで実現します。SyncE を使用するイーサネット リンクは、SONET/SDH と同じ方法で、つまり高品質なストラタム 1 追跡可能クロック信号とビット クロックのタイミングを取ることで同期されます。

SyncE リンクを維持するには、一連の処理メッセージが必要です。これらのメッセージは、ノードが常に最も信頼できるソースからタイミング情報を取得していることを確認し、SyncE リンクのクロック制御に使用されているタイミング ソースの品質情報を転送します。SONET/SDH ネットワークでは、これらは同期ステータスメッセージ（SSM）と呼ばれます。SyncE は、Ethernet Synchronization Message Channel（ESMC）を使用して SSM を転送します。

パケット ネットワークを使用するユーザは、時分割多重（TDM）回線で複数のリモートネットワーク要素（NE）にタイミングを提供することは難しいでしょう。SyncE 機能は、パケットネットワークを介してリモート NE に有効なタイミングを提供することにより、この問題を解決することができます。SyncE は、イーサネット ポート上でクロック周波数を同期し、イーサネットの物理層を利用して周波数をリモートサイトに送信します。SyncE の機能性と正確性は、その物理レイヤの特性により、SONET/SDH ネットワークに類似しています。

SONET/SDH は、メッセージの転送で SONET/SDH オーバーヘッド フレームの 2 つの S バイトから 4 ビットを使用します。イーサネットは、メッセージの転送で IEEE 802.3 構成固有の低速プロトコルに基づく ESMC に依存します。同期パス上の各 NE は SyncE をサポートし、SyncE

はパスの周波数を効果的に提供します。SyncE は相対時間（位相整列など）も絶対時間（時刻）もサポートしません。

SyncEは、既知で共通の精密周波数基準の周波数の配布をイーサネット物理レイヤ ネットワーク レベルで提供します。SyncE で使用するクロックは、SONET/SDH 同期ネットワークで使用されるクロックと互換性があります。ネットワーク同期を行う場合は、出力クロックのパフォーマンスを備えた同期ネットワーク接続を経由するネットワークから同期情報が送信されます。

ESMC は同期証跡のタイミング品質を識別する品質レベル（QL）ID を伝送します。QL-TLV の QL 値は、SONET および SDH SSM に定義した QL 値と同じです。ネットワークの送信中に SSM QL によって提供される情報により、最も信頼できるソースから適切なタイミングでノードを取得することができるようになり、タイミング ループが回避されます。ESMCは同期選択アルゴリズムとともに使用されます。イーサネットネットワークはすべてのリンクまたはすべての場所で同期している必要がないため、ESMCチャネルはこのサービスを提供します。G.8264 に記述されている ESMC は、標準イーサネット ヘッダーから構成されます。ヘッダーの内容は、構成固有の低速プロトコル、ITU-T OUI、固有の ITU-T サブタイプ、ESMC 固有のヘッダー、フラグ フィールド、およびタイプ、長さ、値（TLV）構造です。フラグと TLV を使用することにより、SyncE リンクと関連するタイミングの変更の管理体制が向上します。

ソースおよび選択ポイント

周波数同期の実装には、ソースと選択ポイントが含まれます。

ソースは、システムに周波数信号を入力するか、システムから周波数信号を送信します。ソースには次の 4 つのタイプがあります。

- SyncE インターフェイスを含む回線インターフェイス。
- クロック インターフェイス。これらは、BITS、UTI および GPS などの他のタイミング信号を接続するための外部コネクタです。
- PTP クロック。IEEE 1588 バージョン 2 がルータに設定されている場合、時刻と周波数のソースとして PTP クロックが周波数の同期に使用できることがあります。
- 内部発振器。これはフリーランの内部発振器チップです。

各ソースには、関連する品質レベル（QL）があり、クロックの正確度を指定します。このQL情報は、ESMCによって伝送されるSSMを使用してネットワーク全体に送信されます。QL 情報は、システム内のデバイスが同期できる最適な利用可能なソースを決定するために使用されます。

事前定義されたネットワーク同期フローを定義し、タイミング ループを防止するために、スイッチの各ソースに優先順位の値を割り当てることができます。複数のソースが同じ QL を持つ場合、ユーザが割り当てた優先順位の値によって、ソース間の相対的な優先度が決まります。

選択ポイントは、いくつかの利用可能な周波数信号から選択が行われるスイッチ内のプロセスです。QL 情報およびユーザ割り当ての優先順位レベルを組み合わせることにより、ITU 標準 G.781 に従って SyncE インターフェイスを同期化するソースを各スイッチが選択できるようになります。

SyncE の注意事項と制限事項

SyncE には、次の注意事項および制限事項があります。

- SyncE は N9K-C93180YC-FX3 スイッチでサポートされています。
- SyncE は、ダウンストリームのフロント パネル ポートでのみ有効にできます。インターフェイスは、スイッチング、ルーティング、またはサブインターフェイスにすることができます。
- SyncE は、SVI またはそのメンバー インターフェイスではサポートされていません。
- SyncE は、ダウンストリームのフロント パネル ポートでのみ有効にできます。インターフェイスは、スイッチ、またはルーテッド物理インターフェイス、ポートチャネル、またはサブインターフェイスにすることができます。
- 仮想ポートチャネル（vPC）およびポートチャネルインターフェイスでの SyncE がサポートされています。これらのインターフェイスで SyncE を有効にすると、SyncE は vPC またはポートチャネルごとに構成され、そのすべてのメンバーインターフェイスで有効になります。vPC またはポートチャネル メンバー インターフェイスごとの SyncE の有効化はサポートされていません。
- SyncE はローカル リーフ ファブリックポートではサポートされていません。
- SyncE はリモート リーフ ファブリックポートでサポートされています。
- 別のリーフスイッチに接続されている非ファブリック ポートで SyncE を構成することは推奨しません。
- SyncE のローカル配布がサポートされています。これは、参照元とクライアントの両方が同じリーフスイッチ上にある場合です。リーフスイッチは、ポッドまたはリモート リーフスイッチ内に配置できます。
- SyncE は、2 つのリモート リーフスイッチ間のピア リンクでサポートされます。
- Precision Time Protocol（PTP）を使用したハイブリッド モードは、テレコム プロファイル ITU-T G8275.1 でサポートされています。
- スイッチは、最大 4 つのダウンリンク SyncE 送信元をモニタできます。スイッチは、これらの送信元のいずれかにロックできます。
- PHYの各クワッドポート グループは、1つの基準クロックを提供します。たとえば、インターフェイス 1/1 ～ 1/4 が 4 つの異なる送信元に接続されている場合、リーフスイッチは 1 つの送信元をモニタしてロックできます。
- 拡張 SSM または拡張 QL TLV フォーマットはサポートされていません。
- GPS および GNSS はサポートされていません。
- SyncE は、銅線ギガビット イーサネット SFP を除くすべての認定された光でサポートされています。

同期イーサネットの構成

リーフスイッチで SyncE を有効にするには、2 つのレベルのポリシーを作成する必要があります。

- ノード レベルのポリシーは、リーフスイッチまたはリモート リーフスイッチで SyncE プロセスを有効にします。このポリシーは、SyncE ノードのグローバル品質レベル（QL）オプション構成を指定します。
- インターフェイス レベルのポリシーは、インターフェイスの SyncE プロパティを構成します。このポリシーは、インターフェイスに固有の QL レベルの上書きを有効にすることもできます。インターフェイス ポリシーの QL オプションは、ノード レベル ポリシーの QL オプションと一致する必要があります。

同期イーサネット ノード ポリシーの作成

この手順では、SyncE のノード レベルの構成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] > [Access Policies] の順に選択します。

ステップ 2 ナビゲーションウィンドウで、**[ポリシー（Policies）] > [スイッチ（Switch）] > [同期イーサネット ノード（Synchronous Ethernet Node）]** の順に選択します。

ステップ 3 **[同期イーサネット ノード（Synchronous Ethernet Node）]** を右クリックし、**[同期イーサネット ノード ポリシーの作成（Create Synchronous Ethernet Node Policy）]** を選択します。

ステップ 4 **[同期イーサネット ノード ポリシーの作成（Create Synchronous Ethernet Node Policy）]** ダイアログボックスで、次の手順を実行します。

a) ポリシーの **[名前（Name）]** を入力します。

b) ポリシーの **[説明（Description）]** を入力します。

c) **[管理状態（Admin State）]** コントロールを **[有効（Enabled）]** に設定してポリシーをアクティブにするか、**[無効（Disabled）]**（デフォルト）に設定してポリシーを非アクティブにします。

d) **[QL オプション（QL Option）]** ドロップダウンリストで、品質レベルを選択します。

次の ITU-T 品質レベル（QL）オプションのいずれかを選択します。

- **[オプション 1（Option 1）]**：DNU、EEC1、PRC、PRTC、SEC、SSU-A、SSU-B、eEEC および ePRTC が含まれます。
- **[オプション 2 生成 1（Option 2 generation 1）]**：DUS、EEC2、PRS、PRTC、RES、SMC、ST2、ST3、ST4、STU、eEEC、ePRTC が含まれます。
- **[オプション 2 生成 2（Option 2 generation 2）]**：DUS、EEC2、PROV、PRS、PRTC、SMC、ST2、ST3、ST3E、ST4、STU、TNC、eEEC および ePRTC が含まれます。

（注）
拡張 SSM QL オプション PRTC、eEEC、および ePRTC はサポートされていません。

Stratum 4 フリーラン（ST4）は、イーサネット ラインインターフェイスではサポートされていません。

これらのオプションの QL マッピングの詳細については、ACI 構成オプションを持つ QL マッピング（84 ページ）を参照してください。

（注）
[品質レベル オプション（Quality Level Option）] は、通常、インターフェイス レベルではなく、ここで構成されます。インターフェイス レベルで構成されている場合、そこでの QL オプションは、ここで選択した QL と一致する必要があります。

e) （任意） 5.2(4) リリース以降では、**[ラグ メンバーで DNU を送信（Transmit DNU on Lag Members）]** の機能を有効にします。

このオプションがノードで有効になっていて、ポート チャネル メンバー ポートの 1 つが SyncE 送信元としてロックされている場合、他のメンバー ポートは SyncE ESMC メッセージを使用して QL-DNU（使用しない）を送信し、SyncE 入力ポートを選択する際の潜在的なタイミングの問題を防止します。この機能により、G.8264 のリンク集約を使用した 11.1.1 ESMC 操作への準拠が可能になります。

f) **[送信（Submit）]** をクリックします。

次のタスク

[ファブリック（Fabric）] > [アクセスポリシー（Access Policies）] > [スイッチ（Switches）] > [リーフスイッチ（Leaf Switches）] > [ポリシー グループ（Policy Groups）] でアクセススイッチ ポリシー グループにポリシーを追加します。

同期イーサネット インターフェイス ポリシーの作成

この手順では、同期イーサネット（SyncE）のインターフェイス レベルの構成ポリシーを作成します。

SyncE インターフェイス ポリシーを使用すると、イーサネット インターフェイスを周波数同期入出力として構成できます。インターフェイスを入力として構成すると（**[選択入力（Selection Input）]** を使用）、インターフェイスが選択アルゴリズムに渡され、周波数同期のタイミング送信元と見なされるようになります。

インターフェイスが入力にロックされている場合、インターフェイスは常に選択された周波数信号に同期して送信します。

手順

ステップ 1 メニュー バーで、[Fabric] > [Access Policies] の順に選択します。

ステップ 2 ナビゲーションウィンドウで、**[ポリシー（Policies）]>[同期イーサネット インターフェイス（Synchronous Ethernet Interface）]** の順に選択します。

ステップ 3 **[同期イーサネット インターフェイス（Synchronous Ethernet Interface）]** を右クリックし、**[同期イーサネット インターフェイス ポリシーの作成（Create Synchronous Ethernet Interface Policy）]** を選択します。

ステップ 4 **[同期イーサネット インターフェイス ポリシーの作成（Create Synchronous Ethernet Interface Policy）]** ダイアログボックスで、次の手順を実行します。

a) ポリシーの **[名前（Name）]** を入力します。

b) ポリシーの **[説明（Description）]** を入力します。

c) **[管理状態（Admin State）]** コントロールを **[有効（Enabled）]** に設定してポリシーをアクティブにするか、**[無効（Disabled）]**（デフォルト）に設定してポリシーを非アクティブにします。

d) **[同期ステータスメッセージ（Synchronization Status Message）]** チェックボックスをオンまたはオフにします。

チェックを外さない場合、ESMC パケットの送信が無効化され、受信した ESMC パケットもすべて無視されます。このチェックボックスはデフォルトでオンになります。

e) **[選択入力（Selection Input）]** チェックボックスをオンまたはオフにします。

オンにすると、選択アルゴリズムに渡すタイミング送信元としてインターフェイスを割り当てます。このチェックボックスはデフォルトでオフになります。

f) アップまたはダウン コントロールをクリックして、**[送信元の優先順位（Source Priority）]** を設定します。

インターフェイスの周波数送信元の優先順位。この値は、クロック選択アルゴリズムで同じ QL がある 2 つの送信元間から選択するために使用されます。値は、1（最高プライオリティ）から 254（最低プライオリティ）の範囲で設定できます。デフォルト値は 100 です。

（注）
この設定は、**[選択入力（Selection Input）]** がチェックされている場合にのみ有効です。

g) アップまたはダウン コントロールをクリックして、**[復元までの待機（Wait-To-Restore）]** 時間を分単位で設定します。

分単位の復元までの待機時間は、インターフェイスが起動し、周波数同期に使用されるまでの時間です。有効値の範囲は、0 ～ 12 です。デフォルト値は 5 です。

（注）
この設定は、**[選択入力（Selection Input）]** がチェックされている場合にのみ有効です。

h) **[品質レベル オプション（Quality Level Option）]** ドロップダウンリストで、品質レベル（QL）を選択します。

この設定により、インターフェイス レベルで送受信される品質レベル（QL）を指定または上書きできます。ITU-T 品質レベルのオプションは次のとおりです。

- **[品質レベルが構成されていません（No Quality Level configured）]**：（デフォルト）ESMC を介して接続された送信元から受信した QL は、周波数同期に使用されます。
- **[オプション 1（Option 1）]**：DNU、EEC1、PRC、PRTC、SEC、SSU-A、SSU-B、eEEC および ePRTC が含まれます。

- **[オプション 2 生成 1（Option 2 generation 1）]**：DUS、EEC2、PRS、PRTC、RES、SMC、ST2、ST3、ST4、STU、eEEC、ePRTC が含まれます。
- **[オプション 2 生成 2（Option 2 generation 2）]**：DUS、EEC2、PROV、PRS、PRTC、SMC、ST2、ST3、ST3E、ST4、STU、TNC、eEEC および ePRTC が含まれます。

（注）
拡張 SSM QL オプション PRTC、eEEC、および ePRTC はサポートされていません。

Stratum 4 フリーラン（ST4）は、イーサネット ラインインターフェイスではサポートされていません。

これらのオプションの QL マッピングの詳細については、ACI 構成オプションを持つ QL マッピング（84 ページ）を参照してください。

i) **[品質レベル オプション（Quality Level Option）]** を選択した場合、**[品質の受信（Quality Receive）]** および **[品質の送信（Quality Transmit）** 値のいずれかまたは両方を構成できます。

品質の受信値を使用すると、選択アルゴリズムで使用される SSM メッセージで受信した QL 値を上書きできます。次の選択肢があります。

- **[厳密値（Exact Value）]**：受信した値に関係なく、正確な QL を使用します。ただし、受信した値が Do Not Use（DNU）の場合を除きます。
- **[最高値（Highest Value）]**：受信した QL の上限を設定します。受信した値がこの指定された QL よりも大きい場合、この QL が代わりに使用されます。
- **[最低値（Lowest Value）]**：受信した QL の下限を設定します。受信した値がこの指定された QL よりも小さい場合、DNU が代わりに使用されます。

品質送信値を使用すると、SSM メッセージで送信される QL 値を上書きできます。次の選択肢があります。

- **[厳密値（Exact Value）]**：Do Not Use（DNU）が送信されない限り、正確な QL を使用します。
- **[最高値（Highest Value）]**：送信する QL の上限を設定します。選択された送信元に、ここで指定した QL より高い QL がある場合は、この QL が代わりに送信されます。
- **[最低値（Lowest Value）]**：送信する QL の下限を設定します。選択された送信元に、ここで指定した QL より低い QL がある場合は、DNU が代わりに送信されます。

（注）
これらの設定で指定された品質オプションは、スイッチの同期イーサネット ノード ポリシーで構成された QL オプションと一致する必要があります。

ステップ 5 **[送信（Submit）]** をクリックします。

次のタスク

[ファブリック（Fablic）] > [アクセスポリシー（Access Policies）] > [インターフェイス（Interfaces）] > [リーフ インターフェイス（Leaf Interfaces）] > [ポリシー グループ（Policy

Groups）] > [リーフ アクセス ポート（Leaf Access Port）] で、リーフ アクセス ポート ポリシー グループにポリシーを追加します。

ACI 構成オプションを持つ QL マッピング

次の表に、同期イーサネット ポリシー構成でのクロック ソース品質レベル（QL）値の選択を示します。

これらの QL オプションの詳細については、*ITU-T G.781*、物理層に基づく周波数同期のための同期層機能 を参照してください。

ITU-T オプション 1

品質送受信値	品質レベル
この信号は同期には使用しないでください	QL-DNU
品質共通失敗	QL-FAILED （注を参照）
品質共通無効	QL-INVx （注を参照）
品質共通なし	（注を参照）
ITU-T オプション 1：イーサネット機器のクロック	QL-SEC/QL-EEC1
ITU-T オプション 1：拡張イーサネット機器クロック	QL-eEEC はサポートされていません QL-SEC/QL-EEC1に変換 （注を参照）
ITU-T オプション 1：拡張プライマリ リファレンス タイミング クロック	QL-ePRTC はサポートされていません QL-PRC に変換 （注を参照）
ITU-T オプション 1：プライマリ リファレンス クロック	QL-PRC
ITU-T オプション 1：プライマリ リファレンス タイミング クロック	QL-PRTC はサポートされていません QL-PRC に変換 （注を参照）

品質送受信値	品質レベル
ITU-T オプション 1：SONET 機器のクロック	QL-SEC
ITU-T オプション 1：タイプ I または V スレーブ クロック	QL-SSU-A
ITU-T オプション 1：タイプ IV スレーブ クロック	QL-SSU-B

ITU-T オプション 2、第 1 世代

品質送受信値	品質レベル
この信号は同期には使用しないでください	QL-DUS
品質共通失敗	QL-FAILED （注を参照）
品質共通無効	QL-INVx （注を参照）
品質共通なし	（注を参照）
ITU-T オプション 2、第 1 世代：イーサネット機器のクロック	QL-EEC2
ITU-T オプション 2、第 1 世代：拡張イーサネット機器クロック	QL-eEEC はサポートされていません QL-ST3に変換 （注を参照）
ITU-T オプション 2、第 1 世代：拡張プライマリ リファレンス タイミング クロック	QL-ePRTC はサポートされていません QL-PRSに変換 （注を参照）
ITU-T オプション 2、第 1 世代：プライマリ リファレンス ソース	QL-PRS
ITU-T オプション 2、第 1 世代：プライマリ リファレンス タイミング クロック	QL-PRTC はサポートされていません QL-PRSに変換 （注を参照）
ITU-T オプション 2、第 1 世代：RES	QL-RES
ITU-T オプション 2、第 1 世代：SONET クロック セルフ タイム	QL-SMC
ITU-T オプション 2、第 1 世代：Stratum 2	QL-ST2

品質送受信値	品質レベル
ITU-T オプション 2、第 1 世代：Stratum 3	QL-ST3
ITU-T オプション 2、第 1 世代：Stratum 4 フリーラン	（注を参照）
ITU-T オプション 2、第 1 世代：同期 - トレーサビリティ不明	QL-STU

ITU-T オプション 2、第 2 世代

品質送受信値	ITU 品質レベル
この信号は同期には使用しないでください	QL-DUS
品質共通失敗	QL-FAILED （注を参照）
品質共通無効	QL-INVx （注を参照）
品質共通なし	（注を参照）
ITU-T オプション 2、第 2 世代：イーサネット機器のクロック	QL-EEC2
ITU-T オプション 2、第 2 世代：拡張イーサネット機器クロック	QL-eEEC はサポートされていません QL-ST3に変換 （注を参照）
ITU-T オプション 2、第 2 世代：拡張プライマリ リファレンス タイミング クロック	QL-ePRTC はサポートされていません QL-PRSに変換 （注を参照）
ITU-T オプション 2、第 2 世代：PROV	QL-PROV
ITU-T オプション 2、第 2 世代：プライマリ リファレンス ソース	QL-PRS
ITU-T オプション 2、第 2 世代：プライマリ リファレンス タイミング クロック	QL-PRTC はサポートされていません QL-PRSに変換 （注を参照）
ITU-T オプション 2、第 2 世代：SONET クロック セルフ タイム	QL-SMC
ITU-T オプション 2、第 2 世代：Stratum 2	QL-ST2

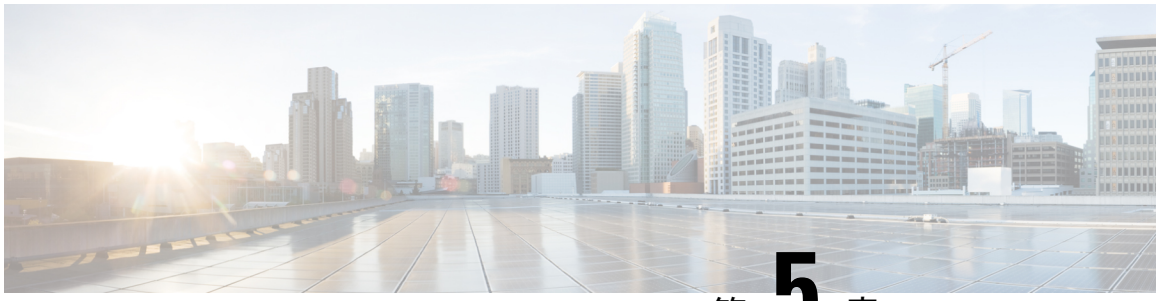
品質送受信値	ITU 品質レベル
ITU-T オプション 2、第 2 世代：Stratum 3	QL-ST3
ITU-T オプション 2、第 2 世代：Stratum 3E	QL-ST3E
ITU-T オプション 2、第 2 世代：Stratum 4 フリーラン	（注を参照）
ITU-T オプション 2、第 2 世代：同期 - トレーサビリティ不明	QL-STU
ITU-T オプション 2、第 2 世代：トランジット ノード クロック	QL-TNC

備考

- QL が構成されていない場合は、「品質共通なし」QL がデフォルトです。
- 品質レベル「品質共通無効」（QL-INVx）および「品質共通失敗」（QL-FAILED）は、リーフまたはリモート リーフスイッチ内の内部品質レベルであり、出力ポートで生成されることはありません。
- ITU-T オプション 2、第 1 世代および第 2 世代：Stratum 4 フリーラン（QL-ST4）は、イーサネット ライン インターフェイスではサポートされていません。
- 拡張 QL TLV（type-length-value）はサポートされていません。接続された周波数ソースから ESMC フレームで拡張 QL TLV を受信すると、リーフまたはリモート リーフスイッチは受信した ESMC フレームを処理しますが、指定された拡張 TLV を無視して、標準 TLV のみを重視します。
- いくつかの QL 値は、標準 QL TLV と拡張 QL TLV を組み合わせて記述されています。これらの値は、ACI リーフ ノードで、標準の QL TLV でのみ記述できる QL 値に変換されます。変換を次の表に示します。

拡張 TLV	説明	変換済み/有効な QL
ITU-T オプション 1		
QL-PRTC	ITU-T オプション 1：プライマリ リファレンス タイミング クロック	QL-PRC
QL-eEEC	ITU-T オプション 1：拡張イーサネット機器クロック	QL-SEC/QL-EEC1
QL-ePRTC	ITU-T オプション 1：拡張プライマリ リファレンス タイミング クロック	QL-PRC
ITU-T オプション 2		
QL-PRTC	ITU-T オプション 2、第 1 世代および第 2 世代：プライマリ リファレンス タイミング クロック	QL-PRS

拡張 TLV	説明	変換済み/有効な QL
QL-eEEC	ITU-T オプション 2、第 1 世代および第 2 世代：拡張イーサネット機器クロック	QL-ST3
QL-ePRTC	ITU-T オプション 2、第 1 世代および第 2 世代：拡張プライマリ リファレンス タイミング クロック	QL-PRS



第 5 章

HTTP/HTTPS プロキシ ポリシー

HTTP/HTTPS プロキシ ポリシーについて

リリース 5.2(1)以降では、インターネットアクセスを必要とする機能のために、Cisco Application Policy Infrastructure Controller（APIC）で HTTP または HTTPS プロキシ アドレスを構成できます。構成されたプロキシ アドレスを自動的に使用する Cisco APIC 機能に加えて、Cisco APIC の周囲のエコシステムも Cisco APIC のオブジェクト `proxyServer` にクエリを実行できるため、複数のプラットフォームでプロキシ情報を構成する必要なく、エコシステムが Cisco APIC と同じプロキシサーバーを使用できます。

HTTP/HTTPS プロキシ ポリシー自体は、各 Cisco APIC 機能が使用する管理ネットワーク（帯域外または帯域内）を制御または変更しません。Cisco APIC 接続設定で管理ネットワーク設定を指定できます。詳細については、*Cisco APIC* ベーシック コンフィギュレーション ガイド の「管理」の章の「管理アクセスの追加」セクションを参照してください。

HTTP/HTTPS プロキシを使用する Cisco APIC の機能

HTTP または HTTPS プロキシサーバーを構成した場合、次の Cisco Application Policy Infrastructure Controller（APIC）機能により、プロキシサーバー経由でトラフィックが送信されます。

- Cisco Intersight デバイス コネクタ
- Cisco APIC GUI内蔵のフィードバック機能

（注） リリース 5.2(1) より前の Cisco Intersight - デバイス コネクタには、組み込みのプロキシ設定がありました。この機能は、現在、Cisco APIC の HTTP/HTTPS プロキシ ポリシーに存在します。

GUI を使用した HTTP/HTTPS プロキシ ポリシーの構成

次の手順では、HTTP または HTTPS プロキシ ポリシーを構成します。初回セットアップ ウィザードを使用してプロキシ設定を構成することもできます。初回セットアップ ウィザードの詳細については、*Cisco APIC* ベーシック コンフィギュレーション ガイド の「初回セットアップ ウィザード」の章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）]** の順に選択します。

ステップ 2 ナビゲーションウィンドウで、**[Proxy Policy（プロキシ ポリシー）]** を選択します。

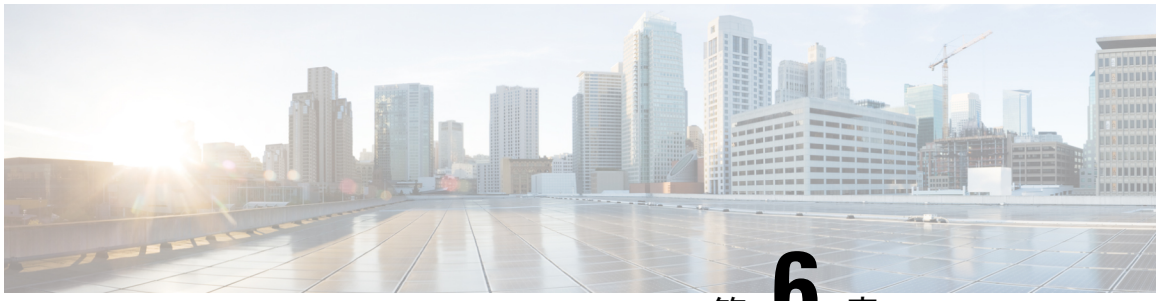
ステップ 3 [作業（Work）] ペインで、必要に応じて **[HTTP URL]** または **[HTTPS URL]** フィールドに URL を入力します。

プロキシサーバーで認証が必要な場合は、次の形式を使用します。

```
http[s]://[username:password]@proxy-server[:proxyport]
```

ステップ 4 （任意） **[ホストを無視（Ignore Hosts）]** テーブルで、**[+]** をクリックし、HTTP または HTTPS プロキシを使用しないホストのホスト名または IP アドレスを入力して、**[更新（Update）]** をクリックします。

HTTP または HTTPS プロキシを使用しないホストをさらに追加する場合は、この手順を繰り返します。



第 6 章

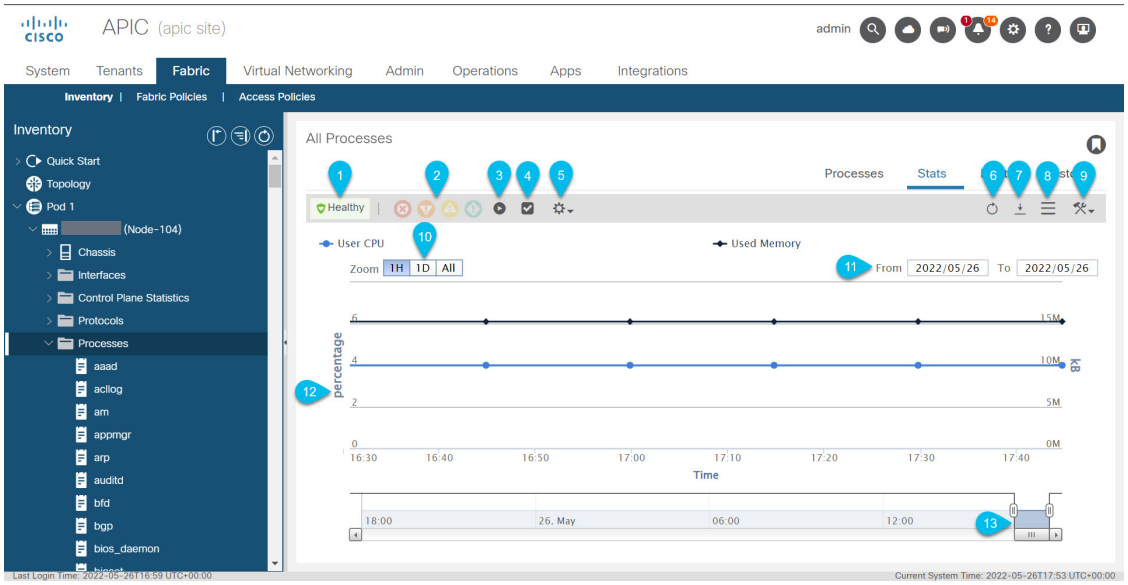
プロセス統計

GUI を使用したプロセスの統計情報の確認

プロセスの統計を表示するには、メニュー バーで**[ファブリック（Fabric）]** > **[インベントリ（Inventory）]**を選択します。 [ナビゲーション（Navigation）] ペインで、 以下のいずれかのアクションを実行します。

- すべてのプロセスの場合は、***[pod_ID]*** > ***[node_name]*** > **[Processes（プロセス）]**を選択します。
- 特定のプロセスの場合は、***[pod_ID]*** > ***[node_name]*** > **[Processes（プロセス）]** > ***[process_name]*** を選択します。

[作業（Work）]ペインで、**[Stats（統計）]** タブを選択します。次のスクリーンショットは、すべてのプロセスでの例を示していますが、特定のプロセスでのビューもほぼ同じです。



図表番号	説明
1	プロセスの全体的な正常性。カーソルを合わせると、正常性スコアが表示されます。
2	障害。カーソルを合わせると、重大度ごとの障害の数が表示されます。重大度の 1 つをクリックして **[障害（Faults）]** タブに移動し、その重大度の障害を表示します。
3	GUI で、更新された統計が表示されないようにします。このボタンをクリックした時点の統計を調べることができます。GUIのボタンを再度クリックすると、更新された統計の表示が再開されます。GUI で更新された統計を表示しないようにしても、Cisco Application Policy Infrastructure Controller（APIC）は最新の統計を収集し続けます。
4	**[統計の選択（Select Stats）]** ダイアログを開きます。このダイアログでは、サンプリング間隔を選択し、表示する統計を選択することができます。

図表番号	説明
5	表示する統計タイプを選択できます。 • **[平均（Average）]**：保持期間中のリソースの平均使用値を統計ごとに示します。 • **[最小（Min）]**：保持期間中のリソースの最小使用値を統計ごとに示します。 • **[最大（Max）]**：保持期間中のリソースの最大使用値を統計ごとに示します。 • **[傾向（Trend）]**：保持期間中のリソースの使用傾向を統計ごとに示します。 • **[使用率（Rate）]**：保持期間中のリソースの使用率を統計ごとに示します。 • **[デフォルト（default）]**：現在、このタイプは **[平均（Average）]** タイプと同じ情報を表示します。
6	統計データを更新します。
7	統計データを XML ファイルとしてローカル システムにダウンロードします。ファイルは、ブラウザのデフォルトのダウンロード場所にダウンロードされます。
8	テーブル ビューとトポロジ（グラフ）ビューを切り替えます。
9	これをクリックし、**[統計ポリシーの設定（Configure Statistics Policy）]** を選択して **[統計ターゲットの作成（Create Stats Target）]** ダイアログを開きます。このダイアログでは、1つ以上の統計ターゲットを選択し、コレクションを構成することができます。コレクションを使用すると、細分したコレクションごとに保持期間を指定し、細分ごとに有効または無効にすることができます。 詳細については、GUI を使用してポリシーの初回構成を行った後に、すべてのプロセスの統計ポリシーを構成する （96 ページ）を参照してください。

図表番号	説明
10	トポロジ ビューでのみ表示され、**15 分**と **1 時間**のサンプリング間隔でのみ表示されます。これにより、ズームがプリセット値に設定されます。ズームは、トポロジに表示する時間範囲を指定します。 • **[1H]**：ズームを過去 1 時間に設定します。 • **[1D]**：ズームを過去 1 日（過去 24 時間）に設定します。 • **[1M]**：ズームを過去 1 分に設定します。この選択肢は、**[1 時間]** のサンプリング間隔を選択した場合にのみ表示されます。 • **[すべて（All）]**：時間範囲全体を表示するようにズームを設定します。**15 分**のサンプリング間隔では 24 時間を少し超えるように、**1 時間**のサンプリング間隔では **1M** と同じ時間範囲全体を表示するようにズームが設定されます。
11	トポロジ ビューでのみ表示され、**15 分**と **1 時間**のサンプリング間隔でのみ表示されます。トポロジの日付範囲です。日付をクリックして値を変更できます。トポロジーの下部にあるタイムラインに表示されていない日付を入力することはできません。**[開始日（From）]** を **[終了日（To）]** より後にすることはできません。
12	トポロジ ビューのこの領域には、選択した統計のグラフが表示されます。いずれかの期間にカーソルを合わせると、その時点で選択したすべての統計の正確なデータが表示されます。 テーブル ビューでは、この領域に同じ統計のテーブルが表示されます。いずれかのヘッダーをクリックすると、テーブルを並べ替えることができます。ヘッダーの右側にあるドロップダウン リストの矢印をクリックし、**列**を選択して、いずれかのボックスにチェックを入れるか、チェックを外すことで、テーブルをフィルタリングできます。
13	トポロジ ビューでのみ表示されます。これは、トポロジに表示する時間範囲を指定するズームです。これにより、ズームを任意の量に設定できます。左側をドラッグしてズームの開始を指定し、右側をドラッグしてズームの終了を指定し、表示する時間の長さを決定します。開始と終了を設定した後、水平スクロール バーを使用して、タイム ラインのどの部分を表示するかを変更できます。表示される時間の長さは変わりません。

GUI を使用した初回構成のためにすべてのプロセスの統計ポリシーを構成する

この手順では、Cisco Application Policy Infrastructure Controller（APIC）を起動した後の最初の回に、すべてのプロセスの統計ポリシーを構成する方法について説明します。以前にポリシーを構成していた場合には、異なった GUI ダイアログになります。この場合は、GUI を使用してポリシーの初回構成を行った後に、すべてのプロセスの統計ポリシーを構成する （96 ページ）を参照してください。

Cisco APIC は、コレクションの最小単位（時間間隔）が経過するたびに、1 つの統計オブジェクトを作成して保存します。たとえば、15 分間のコレクションの場合、1 時間が経過すると、Cisco APIC は 4 つの統計オブジェクトを作成して保存します。Cisco APIC はコレクションごとに最大 1,000 個の統計オブジェクトを格納します。ただし、最小単位 5 分の場合は例外で、Cisco APIC は 12 個の統計オブジェクトのみを格納します。

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_ID]*** > ***[node_name]*** > **[プロセス（Processes）]** を選択します。

ステップ 3 **[作業（Work）]**ペインで、**[アクション（Action）]** > **[統計ポリシーの構成（Configure Statistics Policy）]** を選択します。

[サブネットの作成（Create Subnet）] ダイアログボックスが表示されます。

ステップ 4 **[使用可能（Available）]** 領域で、1 つまたは複数の統計タイプを選択し、**[使用可能（Available）]** 領域と **[選択済み（Selected）]** 領域の間にある上部の灰色のボタンをクリックします。

選択した統計タイプが **[選択済み（Selected）]** エリアに移動します。選択しなかったすべての統計タイプは、**[ファブリック（Fabric）]** > **[ファブリック ポリシー（Fabric Policies）]** > **[ポリシー（Policies）]** > **[監視（Monitoring）]** > **[デフォルト（default）]** > **[統計コレクション ポリシー（Stats Collection Policies）]** > **[すべて（ALL）]**からのデフォルト パラメータを使用します。

Ctrl キーを押しながら目的の統計タイプをクリックすると、複数の統計タイプを選択できます。Shift キーを押しながら最初と最後の統計タイプをクリックして、その間のすべての統計タイプを選択することもできます。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 最小単位の行をダブルクリックして、その最小単位を有効または無効にし、履歴の保持期間を変更してから、**[更新（Update）]** をクリックします。

変更する他の最小単位に対してこのステップを繰り返します。これらの値は、選択したすべての統計タイプに適用されます。

ステップ 7 **[OK]** をクリックします。

GUI を使用してポリシーの初回構成を行った後に、すべてのプロセスの統計ポリシーを構成する

この手順では、ポリシーの初回構成の後に、すべてのプロセスの統計ポリシーを構成する方法について説明します。以前にポリシーを構成していない場合には、異なった GUI ダイアログになります。この場合は、GUI を使用した初回構成のためにすべてのプロセスの統計ポリシーを構成する （95 ページ）を参照してください。

Cisco Application Policy Infrastructure Controller（APIC）は、コレクションの最小単位（時間間隔）が経過するたびに、1 つの統計オブジェクトを作成して保存します。たとえば、15 分間のコレクションの場合、1 時間が経過すると、Cisco APIC は 4 つの統計オブジェクトを作成して保存します。Cisco APIC はコレクションごとに最大 1,000 個の統計オブジェクトを格納します。ただし、最小単位 5 分の場合は例外で、Cisco APIC は 12 個の統計オブジェクトのみを格納します。

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_ID]*** > ***[node_name]*** > **[プロセス（Processes）]** を選択します。

ステップ 3 **[作業（Work）]**ペインで、**[アクション（Action）]** > **[統計ポリシーの構成（Configure Statistics Policy）]** を選択します。

[統計ポリシーのデフォルトを編集（Edit Stats Policy default）] ダイアログが表示されます。

ステップ 4 **[収集としきい値（Collections and Thresholds）]** タブで、必要に応じて **[システム CPU（System CPU）]**、**[システム負荷（System load）]** または **[システム メモリ（System memory）]** を展開します。

[システム CPU（System CPU）]、**[システム負荷（System load）]**、および **[システム メモリ（System memory）]** は以前に構成していた場合にのみ表示されます。

ステップ 5 コレクションを編集するには、目的のコレクション間隔の右側にある編集ボタン（鉛筆のアイコン）をクリックします。

その収集間隔の **[統計の収集としきい値（Stats Collection and Thresholds）]** ダイアログが表示されます。コレクションは、Cisco APIC が特定の最小単位の統計を収集するかどうか、および Cisco APIC が収集された統計を保持する期間を指定します。

a) **[ポリシー（Policy）]** タブで、必要に応じてプロパティを設定します。

プロパティ	説明
精度	編集しているコレクションの最小単位。この値は変更できません。
管理状態（Admin State）	コレクションの管理状態。表示される値は次のとおりです。 • **[無効（disabled）]**：このコレクションを無効にします。つまり、Cisco APIC はこのコレクションの最小単位の統計を収集しません。 • **[有効（enabled）]**：このコレクションを有効にします。つまり、Cisco APIC は、このコレクションの最小単位の統計を収集します。 • **[継承（inherited）**：このコレクションは、デフォルト ポリシーから管理状態を継承します。デフォルト ポリシーを表示し、編集するには、**[ファブリック（Fabric）]**>**[ファブリック ポリシー（Fabric Policies）]**に移動し、**[ポリシー（Policies）]**>**[監視（Monitoring）]**>**[デフォルト（default）]**>**[統計収集ポリシー（Stats Collection Policies）]**の順に移動します。
[履歴保持期間（History Retention Period）：	Cisco APIC が統計オブジェクトを保持する時間の長さ。

b) **[しきい値（Thresholds）]** タブで、構成済みのしきい値を編集または削除できます。
c) **[履歴（History）]** タブで、イベントと監査ログを表示できます。
d) 変更を終えたら、**[送信（Submit）]** をクリックします。

ステップ 6 しきい値を構成するには、目的の収集間隔の右側にある **[+]** ボタンをクリックして、プロパティを選択します。

[統計しきい値の作成（Create Stats Threshold）] ダイアログが表示されます。しきい値は、特定の統計値が特定の値に達するか超えたときに、Cisco APIC が障害を設定することを指定します。

a) 目的に応じてプロパティを設定します。

プロパティ	説明
正常な値	しきい値のベースライン値。
[しきい値の方向（Threshold Direction）]	統計値の上昇時、下降時、またはその両方にしきい値を設定できるかどうかを指定します。 • **[両方（Both）]**：統計値の増加と減少の両方のしきい値を構成できます。 • **[上昇（Rising）]**：統計値の増加のみにしきい値を設定できます。 • **[下降（Falling）]**：統計値の減少のみにしきい値を設定できます。

プロパティ	説明
[上昇しきい値の構成（Rising Thresholds to Config）]	これは、**[しきい値の方向（Threshold Direction）]** で **[両方（Both）]** または **[上昇（Rising）]** を選択した場合にのみ表示されます。統計値の上昇に合わせて Cisco APIC に設定させる障害の重大度ごとに、ボックスにチェックを入れます。
[下降しきい値の構成（Falling Thresholds to Config）]	これは、**[しきい値の方向（Threshold Direction）]** で **[両方（Both）]** または **[下降（Falling）]** を選択した場合にのみ表示されます。統計値の下降に合わせて Cisco APIC に設定させる障害の重大度ごとに、ボックスにチェックを入れます。
[上昇（Rising）] 領域	これは、**[しきい値の方向（Threshold Direction）]** で **[両方（Both）]** または **[上昇（Rising）]** を選択した場合にのみ表示されます。この領域では、指定した重大度の障害を設定またはリセットする統計値を指定します。 **[設定（Set）]** 値と **[リセット（Reset）]** 値は同じにすることができます。**[リセット（Reset）]** 値を **[設定（Set）]** 値より大きくすることはできません。異なる重大度の値を同じにすることはできますが、低い重大度の値を高い重大度の値より大きくすることはできません。たとえば、**[重大（Critical）]** の **[設定（Set）]** 値が 70 の場合、**[メジャー（Major）]** の **[設定（Set）]** 値として指定できるのは 70 以下です。
[下降（Faliing）] 領域	これは、**[しきい値の方向（Threshold Direction）]** で **[両方（Both）]** または **[下降（Falling）]** を選択した場合にのみ表示されます。この領域では、指定した重大度の障害を設定またはリセットする統計値を指定します。 **[設定（Set）]** 値と **[リセット（Reset）]** 値は同じにすることができます。**[設定（Set）]** 値を **[リセット（Reset）]** 値より大きくすることはできません。異なる重大度の値を同じにすることはできますが、高い重大度の値を低い重大度の値より大きくすることはできません。たとえば、**[マイナー（Minor）]** の **[設定（Set）]** 値が 50 の場合、**[メジャー（Major）]** の **[設定（Set）]** 値として指定できるのは 50 以下です。

b) [送信（Submit）] をクリックします。

ステップ 7 （任意）**[レポート可能項目（Reportables）]** タブでは、コレクションとしきい値の専用パラメータを構成する統計タイプを指定できます。

専用パラメータを設定していない統計タイプはすべて、**[ファブリック（Fabric）]**>**[ファブリック ポリシー（Fabric Policies）]** > **[ポリシー（Policies）]** > **[監視（Monitoring）]** > **[デフォルト（default）]** > **[統計コレクション ポリシー（Stats Collection Policies）]**> **[すべて（ALL）]**のデフォルト パラメータを使用します。

レポート可能項目（Reportable） は、GUI の他の部分では「監視オブジェクト」と呼ばれます。

a) **[レポート可能項目の追加/削除（Add/Remove Reportables）]** 領域で、その統計タイプ専用のコレクションおよびしきい値パラメータを構成する統計タイプのボックスにチェックを入れます。

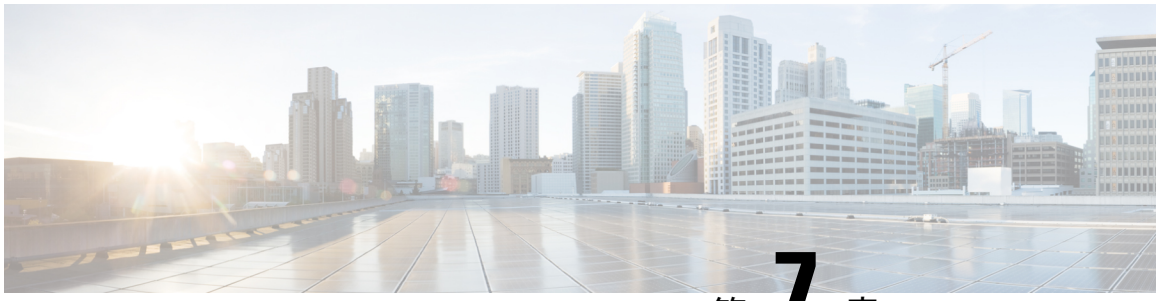
ここから統計タイプを追加すると、その統計タイプが **[コレクションとしきい値（Collections and Thresholds）]** タブに表示され、そこから専用パラメータを変更できます。統計タイプがデフォルトの統計ポリシーのパラメータを使用する必要がある場合は、ボックスからチェックを外します。

b) **[新しいレポート可能項目のコレクションの構成（Configure Collections for New Reportables）]** テーブルで、統計タイプ専用の初期コレクション パラメーターを設定できます。

ただし、この表のパラメータは、専用のパラメータ セットですでに構成されている統計タイプには有効になりません。統計タイプでは、**[レポート可能項目の追加/削除（Add/Remove Reportables）]** 領域のボックスがすでにオンになっているためです。これらの統計タイプについては、**[コレクションとしきい値（Collections and Thresholds）]** タブに移動し、そこから専用パラメータを変更します。

ステップ 8 [送信（Submit）] をクリックします。

GUI を使用してポリシーの初回構成を行った後に、すべてのプロセスの統計ポリシーを構成する



第 7 章

基本操作

APIC クラッシュ シナリオのトラブルシューティング

クラスタのトラブルシューティング シナリオ

次の表は、Cisco APIC に共通するクラスタのトラブルシューティングのシナリオを示します。

問題	ソリューション
APIC ノードはクラスタ内でエラーが発生します。たとえば、5 つの APIC のクラスタのノード 2 がエラーを起こすとします。	2 つの解決策があります。 • 目標サイズはそのままにし、APIC を交換します。 • クラスタ サイズを 4 に減らし、コントローラ 5 をデコミッションし、APIC 2 として再コミッションします。ターゲット サイズは 4 のままで、再構成された APIC がアクティブになったときの運用サイズは 4 です。 （注） クラスタに交換する APIC を追加し、目標サイズと動作サイズを増大することができます。新しい APIC を追加する方法については、『*Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*』を参照してください。

問題	ソリューション
新しい APIC はファブリックに接続し、リーフ スイッチへの接続は失われます。	インフラ（インフラストラクチャ）VLAN の不一致があるかを確認するには、次のコマンドを使用します。 • cat /mit/sys/lldp/inst/if-\[eth1--1\]/ctrlradj/summary：リーフ スイッチ上で構成された VLAN を表示します。 • cat /mit/sys/lldp/inst/if-\[eth1--1\]/ctrlradj/summary：接続された APIC によってアドバタイズされるインフラ（インフラストラクチャ）VLAN を表示します。 これらのコマンドの出力が異なる VLAN を表示する場合、新しい APIC は正しいインフラ（インフラストラクチャ）VLAN で設定されていません。この問題を解決するには、次の手順に従います。 • レスキューユーザーを使用して APIC にログインします。 （注） APIC はファブリックの一部ではないため、管理者のログイン情報は機能しません。 • 構成を消去し、 **acidiag touch setup** コマンドを使用して APIC を再起動します。 • APIC を再構成します。ファブリック名、TEP アドレス、およびクラスタの APIC にマッチするインフラ（インフラストラクチャ）VLAN を確認します。 • リーフ ノードをリロードします。25-03-2015 22:13
2 つの APIC は、再起動後に通信できません。	この問題は次の一連のイベントの後に発生することがあります。 • APIC1 と APIC2 が相互に検出します。 • APIC1 がリブートし、新しいシャーシ ID （APIC1a）でアクティブになる。 • 2 つの APIC が通信しなくなる。 このシナリオでは、APIC1a が APIC2 を検出しますが、APIC2 はオフラインと見なされる APIC1 があるクラスタ内に存在するので使用できません。その結果、APIC1a は APIC2 からのメッセージを受け入れません。 この問題を解決するには、APIC2 上の APIC1 をデコミッションし、再度 APIC1 を稼働させます。

問題	ソリューション
デコミッションされた APIC がクラスタに参加します。	この問題は次の一連のイベントの後に発生することがあります。 • クラスタのメンバーが使用できなくなるか、クラスタが分割されます。 • APIC はデコミッションされます。 • クラスターが回復すると、デコミッションされた APIC が自動的に試運転されます。 この問題を解決するには、クラスタの回復後に APIC をデコミッションします。
再起動後の ChassisID が一致しません。	この問題は、APICがクラスタで登録されたシャーシIDと異なるシャーシIDで起動したときに起こります。その結果、このAPICからのメッセージが廃棄されます。 この問題を解決するには、リブートの前に APIC が解放されていることを確認してください。
APIC はクラスタ サイズの変更時のエラーを表示します。	さまざまな条件が、AdminstrativeClusterSize に合わせたクラスタによる OperationalClusterSize の拡張の妨げになる可能性があります。詳細については、障害を調べて、*Cisco APIC* ベーシック コンフィギュレーション ガイド の「クラスタ障害」セクションを確認してください。
APIC がクラスタに参加できない	この問題は、クラスタを拡大するときに 2 つの APIC が同じクラスタ ID で設定されると起こります。その結果、2 つのうち 1 つの APIC がクラスタに参加できず、拡張競合シャーシ ID 不一致のエラーが表示されます。 この問題を解決するには、新しいクラスタ ID でクラスタの外側に APIC を設定します。

問題	ソリューション
APIC がクラスタで到達不能です。	この問題を診断するには、次の設定を確認してください。 • ファブリック検出が完了していることを確認します。 • ファブリックから欠落しているスイッチを特定します。 • スイッチが APIC からの IP アドレスを要求し、受信したかどうかを確認します。 • スイッチがソフトウェア イメージをロードしたことを確認します。 • スイッチがアクティブになっている時間を確認します。 • すべてのプロセスがスイッチ上で動作していることを確認します。詳細については、*Cisco APIC* ベーシック コンフィギュレーション ガイド の「acidiag コマンド」セクションを参照してください。 • 欠落しているスイッチに正しい日付と時刻が設定されていることを確認します。 • スイッチが他の APIC と通信できることを確認します。
クラスタは拡張しません。	この問題は、次の状況で発生します。 • OperationalClusterSize が APIC の数より少ない。 • 拡張候補はありません (たとえば、管理サイズが 5 であり、clusterID が 4 の APIC がありません。 • クラスタと新しい APIC の間に接続がない • 新しい APIC によってハートビート メッセージが拒否される • システムが正常ではありません。 • 使用できないアプライアンスは、再配置に関連するデータ サブセットを保持しています。 • 再配置に関連するデータ サブセットを持つアプライアンスでサービスがダウンしています。 • 再配置に関する不健全なデータ サブネット

問題	ソリューション
APIC がダウンしています。	次の点を確認します。 • 接続の問題：ping を使用して接続を確認します。 • インターフェイス タイプの不一致：すべての APIC がインバンド通信になっていることを確認します。 • ファブリック接続：ファブリック接続が正常であること、およびファブリック検出が完了していることを確認します。 • 拒否されたハートビート：fltInfraIICIMsgSrcOutsider エラーを確認します。一般的なエラーには、動作クラスタ サイズ、シャーシ ID の不一致、動作クラスタ サイズの外の送信元 ID 、承認されていない送信元、およびファブリック ドメインの不一致が含まれます。

クラスタの障害

APIC は、クラスタの問題の診断に役立つさまざまなエラーをサポートします。ここでは、2 つの主要なクラスタのエラーの種類について説明します。

エラーの破棄

APIC は現在のクラスタのピアまたはクラスタ拡大候補以外からのクラスタ メッセージを破棄します。APIC によりメッセージを破棄した場合、発信元の APIC のシリアル番号、クラスタ ID、タイムスタンプを含むエラーが発生します。次の表で、破棄されるメッセージのエラーを要約します。

Fault	意味
expansion-contender-chassis-id-mismatch	送信側 APIC のシャーシ ID が拡大のためにクラスタが認識するシャーシ ID と一致しません。
expansion-contender-fabric-domain-mismatch	送信側 APIC のファブリック ID が拡大のためにクラスタが認識するファブリック ID と一致しません。
expansion-contender-id-is-not-next-to-oper-cluster-size	送信側 APIC に拡大に不適切なクラスタ ID があります。値は、現在の OperationalClusterSize よりも 1 大きい必要があります。
expansion-contender-message-is-not-heartbeat	送信側 APIC が継続的ハートビート メッセージを送信しません。
fabric-domain-mismatch	送信側 APIC のファブリック ID がクラスタのファブリック ID と一致しません。
operational-cluster-size-distance-cannot-be-bridged	送信側 APIC に、受信側 APIC のものとは 1 以上違う OperationalClusterSize があります。受信側 APIC は要求を拒否します。

Fault	意味
source-chassis-id-mismatch	送信側 APIC のシャーシ ID がクラスタに登録されたシャーシ ID と一致しません。
source-cluster-id-illegal	送信側 APIC に許可されていないクラスタ ID 値があります。
source-has-mismatched-target-chassis-id	送信側 APIC の目標シャーシ ID が受信側 APIC のシャーシ ID に一致しません。
source-id-is-outside-operational-cluster-size	送信側 APIC に、クラスタの OperationalClusterSize 外のクラスタ ID があります。
source-is-not-commissioned	送信側 APIC にクラスタで現在解放されている ID があります。

クラスタ変更時エラー

次のエラーは、APIC のクラスタ サイズの変更時のエラーがある場合に適用されます。

Fault	意味
cluster-is-stuck-at-size-2	このエラーは、OperationalClusterSize が拡張期間にわたり 2 のままになると発行されます。問題を解決するには、クラスタの目標サイズをリストアします。
most-right-appliance-remains-commissioned	クラスタ内の最後の APIC が稼働中で、クラスタの縮小を妨げています。
no-expansion-contender	クラスタがより大きいクラスタ ID を持つ APIC を検出できず、クラスタの拡張を行えません。
service-down-on-appliance-carrying-replica-related-to-relocation	移動するデータのサブセットは、障害が起きているサービス上にコピーがあります。APIC に複数のこのような障害があることを示します。
unavailable-appliance-carrying-replica-related-to-relocation	移動するデータのサブセットは、使用できない APIC 上にコピーがあります。このエラーを解決するには、使用できない APIC を復元します。
unhealthy-replica-related-to-relocation	移動するデータのサブセットは、正常でない APIC 上にコピーがあります。このエラーを解決するには、障害の根本原因を特定します。

APIC 使用不可

次のクラスタのエラーは、APIC が使用できない場合に適用できます。

Fault	意味
fltInfraReplicaReplicaState	クラスタがデータのサブセットを起動できません。
fltInfraReplicaDatabaseState	データ ストア サービスの破損を示します。

Fault	意味
fltInfraServiceHealth	データのサブセットが完全には機能していないことを示します。
fltInfraWiNodeHealth	APIC が完全には機能していないことを示します。

ファブリック ノードとプロセス クラッシュのトラブルシューティング

ACI スイッチ ノードには、システムのさまざまな機能面を制御する多数のプロセスがあります。システムの特定のプロセスでソフトウェア障害が発生した場合、コア ファイルが生成され、プロセスがリロードされます。

プロセスが Data Management Engine（DME）プロセスの場合、DME プロセスは自動的に再起動します。プロセスが非 DME プロセスの場合、プロセスは自動的に再起動せず、スイッチが再起動して回復します。

このセクションでは、さまざまなプロセスの概要、プロセスがコア化したことを検出する方法、およびこれが発生したときに取るべきアクションについて説明します。

DME プロセス

APIC で実行されている重要なプロセスは、CLI で見つけることができます。APIC とは異なり、 **FABRIC** > **INVENTORY** > **Pod 1** > ***node*** の GUI を介して表示できるプロセスには、リーフで実行されているすべてのプロセスが表示されます。

ps-ef | grep svc_ifc を経由：

```
rtp_leaf1# ps -ef |grep svc_ifc
root 3990 3087 1 Oct13 ? 00:43:36 /isan/bin/svc_ifc_policyelem --x
root 4039 3087 1 Oct13 ? 00:42:00 /isan/bin/svc_ifc_eventmgr --x
root 4261 3087 1 Oct13 ? 00:40:05 /isan/bin/svc_ifc_opflexelem --x -v
dptcp:8000
root 4271 3087 1 Oct13 ? 00:44:21 /isan/bin/svc_ifc_observerelem --x
root 4277 3087 1 Oct13 ? 00:40:42 /isan/bin/svc_ifc_dbgrelem --x
root 4279 3087 1 Oct13 ? 00:41:02 /isan/bin/svc_ifc_confelem --x
rtp_leaf1#
```

スイッチで実行されている各プロセスは、システムのログファイルにアクティビティを書き込みます。これらのログ ファイルは、techsupport ファイルの一部として処理されていますが、CLI アクセスを介して /tmp/logs/ ディレクトリにあります。たとえば、ポリシー エレメントのプロセス ログ出力は、/tmp/logs/svc_ifc_policyelem.log に書き込まれます。

以下は、システムで実行されている DME プロセスの簡単な説明です。これは、特定のプロセスのトラブルシューティング時にどのログ ファイルを参照するかを理解したり、プロセスがクラッシュした場合のシステムへの影響を理解したりするのに役立ちます。

プロセス	機能
ポリシー要素	ポリシー要素: APIC からの論理 MO を処理し、具体的なモデルをスイッチにプッシュします

プロセス	機能
eventmgr	イベント マネージャ：ローカルの障害、イベント、ヘルス スコアを処理します
opflexelem	Opflex 要素: スイッチ上の Opflex サーバ
observerelem	オブザーバ要素: APIC に送信されたローカル統計を処理します
dbgrelem	デバッガー要素：コア ハンドラ
nginx	スイッチと APIC 間のトラフィックを処理する Web サーバ

プロセスがいつクラッシュしたかを特定する

プロセスがクラッシュしてコア ファイルが生成されると、イベントだけでなく障害も生成されます。APIC からの次の syslog 出力に示されているように、特定のプロセスの障害は「プロセス クラッシュ」として表示されます。

```
Oct 16 03:54:35 apic3 %LOG_LOCAL7-3-SYSTEM_MSG [E4208395][process-crash][major]
[subj-[dbgs/cores/node-102-card-1-svc-policyelem-ts-2014-10-16T03:54:55.000+00:00]/
rec-12884905092]Process policyelem cored
```

スイッチのプロセスがクラッシュすると、コア ファイルが圧縮され、APIC にコピーされます。syslog メッセージ通知は APIC から送信されます。

プロセスがクラッシュしたときに生成される障害は、プロセスが再起動された Cisco Application Centric Infrastructure 275 のトラブルシューティングでクリアされます。障害は、**[ファブリック（FABRIC）]** > **[インベントリ（INVENTORY）]** > **[ポッド 1 （Pod 1）]** でファブリック履歴タブの GUI を介して表示できます。

コア ファイルの収集

APIC GUI は、ファブリック ノードのコア ファイルを収集するための中心的な場所を提供します。

エクスポート ポリシーは、**ADMIN** > **IMPORT/EXPORT** > **Export Policies** > **Core** から作成されます。ただし、ファイルを直接ダウンロードできるデフォルトのコア ポリシーがあります。

コア ファイルには、コア ファイルが配置されている APIC の /data/techsupport にある APIC を介して SSH/SCP 経由でアクセスできます。コア ファイルは、クラスタ内の 1 つの APIC の /data/techsupport で入手できることに注意してください。コア ファイルが存在する正確な APIC は、GUI に表示されるエクスポート ロケーション パスで見つけることができます。たとえば、エクスポート先が「files/3/」で始まる場合、ファイルはノード 3（APIC3）にあります。

APIC プロセスのクラッシュの検証と再起動

症状 1

スイッチファブリックのプロセスがクラッシュします。プロセスが自動的に再起動するか、スイッチがリロードして復元します。

- **検証**：

  概要セクションに示されているように、DME プロセスがクラッシュした場合、スイッチを再起動せずに自動的に再起動する必要があります。非 DME プロセスがクラッシュした場合、プロセスは自動的に再起動せず、スイッチが再起動して回復します。

  どのプロセスがクラッシュするかによって、プロセス コアの影響は異なります。

  非DMEプロセスがクラッシュすると、通常コンソールに表示されるようにHAPリセットが発生します。

```
[ 1130.593388] nvram_klm wrote rr=16 rr_str=ntp hap reset to nvram
[ 1130.599990] obfl_klm writing reset reason 16, ntp hap reset
[ 1130.612558] Collected 8 ext4 filesystems
```

- **プロセス ログの確認**：

  クラッシュするプロセスには、クラッシュ前に何らかのレベルのログ出力が必要です。スイッチのログの出力は、/tmp/logsディレクトリに書き込まれます。プロセス名はファイル名の一部になります。たとえば、ポリシー エレメント プロセスの場合、ファイルは svc_ifc_policyelem.log です。

```
rtp_leaf2# ls -l |grep policyelem
-rw-r--r-- 2 root root 13767569 Oct 16 00:37 svc_ifc_policyelem.log
-rw-r--r-- 1 root root 1413246 Oct 14 22:10 svc_ifc_policyelem.log.1.gz
-rw-r--r-- 1 root root 1276434 Oct 14 22:15 svc_ifc_policyelem.log.2.gz
-rw-r--r-- 1 root root 1588816 Oct 14 23:12 svc_ifc_policyelem.log.3.gz
-rw-r--r-- 1 root root 2124876 Oct 15 14:34 svc_ifc_policyelem.log.4.gz
-rw-r--r-- 1 root root 1354160 Oct 15 22:30 svc_ifc_policyelem.log.5.gz
-rw-r--r-- 2 root root 13767569 Oct 16 00:37 svc_ifc_policyelem.log.6
-rw-rw-rw- 1 root root 2 Oct 14 22:06 svc_ifc_policyelem.log.PRESERVED
-rw-rw-rw- 1 root root 209 Oct 14 22:06 svc_ifc_policyelem.log.stderr
rtp_leaf2#
```

  /tmp/logsにあるプロセスごとにいくつかのファイルがあります。ログ ファイルのサイズが大きくなるにつれて、ログ ファイルは圧縮され、古いログ ファイルはローテーションされなくなります。コア ファイルの作成時刻（GUI とコア ファイル名に表示される）を確認して、ファイルのどこを確認すればよいかを理解します。また、プロセスが最初に起動しようとすると、ログファイルに「クラッシュ後にプロセスが再起動しています」というエントリが記録されます。このエントリを使用して、クラッシュの前に何が起こったかを遡って検索できます。

- **アクティビティをチェック**：

  実行中のプロセスに変更が加えられたため、クラッシュが発生しました。多くの場合、変更はシステムの構成アクティビティによるものである可能性があります。システムで発生したアクティビティは、システムの監査ログ履歴で確認できます。

- **TAC に連絡する**：

  通常、プロセスのクラッシュは発生しません。上記の手順を超える理由をよりよく理解するには、コア ファイルをデコードする必要があります。この時点で、ファイルを収集して、さらに処理するために TAC に提供する必要があります。

  上記の方法でコア ファイルを収集し、TAC でケースをオープンします。

症状 2

ファブリック スイッチが継続的にリロードするか、BIOS ローダー プロンプトでスタックします。

- **検証**：

  DME プロセスがクラッシュした場合、スイッチの再起動をせずに自動的に再起動する必要があります。非DMEプロセスがクラッシュした場合、プロセスは自動的に再起動せず、スイッチが再起動して回復します。ただし、いずれの場合でもプロセスが継続的にクラッシュすると、スイッチは継続的なリロードループに入るか、BIOS ローダー プロンプトで終了する可能性があります。

```
[ 1130.593388] nvram_klm wrote rr=16 rr_str=policyelem hap reset to nvram
[ 1130.599990] obfl_klm writing reset reason 16, policyelem hap reset
[ 1130.612558] Collected 8 ext4 filesystems
```

- **HAP リセット ループを破る**：

  最初のステップは、スイッチをさらに情報を収集できる状態に戻すことです。

  スイッチが継続的に再起動している場合、スイッチの起動時に、スイッチが起動サイクルの最初の部分である場合 CTRL C を入力して、コンソールから BIOS ローダー プロンプトに侵入します。

  スイッチがローダー プロンプトに表示されたら、次のコマンドを入力します。

  - cmdline no_hap_reset
  - ブート

  cmdline コマンドは、hap リセットが呼び出されたときにスイッチがリロードするのを防ぎます。2番目のコマンドでは、システムを起動します。リロードによって入力されたcmdlineオプションが削除されるため、ローダーでのリロードの代わりに boot コマンドが必要であることに注意してください。

  これで、システムはデータを収集するためのより適切なアクセスを許可するようになったはずですが、プロセスがクラッシュするとスイッチの機能に影響を与えます。

前の表のように、プロセスログ、アクティビティを確認し、TACの手順に連絡してください。

APIC プロセス クラッシュのトラブルシューティング

APIC には、システムのさまざまな機能的側面を制御する一連のデータ管理エンジン（DME）プロセスがあります。システムの特定のプロセスでソフトウェア障害が発生すると、コア ファイルが生成され、プロセスが再ロードされます。

次のセクションでは、システム プロセスのクラッシュやソフトウェアの障害に関連する潜在的な問題について説明します。まず、さまざまなシステム プロセスの概要、プロセスがコア化されたことを検出する方法、およびこれが発生したときに取るべきアクションについて説明します。正常に動作しているシステムの表示は、突然終了した可能性のあるプロセスを特定するために使用できます。

DME プロセス

APIC で実行されている重要なプロセスは、GUI または CLI のいずれかで見つけることができます。GUI を使用すると、実行中のプロセスとプロセス ID が **[システム（System）] > [コントローラ（Controllers）] > [プロセス（Processes）]** に表示されます。

CLI を使用すると、プロセスとプロセス ID は、/aci/system/controllers/1/processes（APIC1 の場合）のサマリ ファイルにあります。

```
admin@RTP_Apic1:processes> cat summary
processes:
process-id process-name max-memory-allocated state
---------- ---------------- ------------------- -------------------
0 KERNEL 0 interruptible-sleep
331 dhcpd 108920832 interruptible-sleep
336 vmmmgr 334442496 interruptible-sleep
554 neo 398274560 interruptible-sleep
1034 ae 153690112 interruptible-sleep
1214 eventmgr 514793472 interruptible-sleep
2541 bootmgr 292020224 interruptible-sleep
4390 snoopy 28499968 interruptible-sleep
5832 scripthandler 254308352 interruptible-sleep
19204 dbgr 648941568 interruptible-sleep
21863 nginx 4312199168 interruptible-sleep
32192 appliancedirector 136732672 interruptible-sleep
32197 sshd 1228800 interruptible-sleep
32202 perfwatch 19345408 interruptible-sleep
32203 observer 724484096 interruptible-sleep
32205 lldpad 1200128 interruptible-sleep
32209 topomgr 280576000 interruptible-sleep
32210 xinetd 99258368 interruptible-sleep
32213 policymgr 673251328 interruptible-sleep
32215 reader 258940928 interruptible-sleep
32216 logwatch 266596352 interruptible-sleep
32218 idmgr 246824960 interruptible-sleep
32416 keyhole 15233024 interruptible-sleep
admin@apic1:processes>
```

APIC で実行されている各プロセスは、システムのログ ファイルに書き込みます。これらのログ ファイルは、APIC techsupport ファイルの一部としてバンドルできますが、/var/log/dme/log の SSH シェル アクセスを介して確認することもできます。たとえば、Policy Manager プロセス ログ出力は /var/log/dme/log/svc_ifc_policymgr.bin.log に書き込まれます。

以下は、システムで実行されているプロセスの簡単な説明です。これは、特定のプロセスのトラブルシューティング時にどのログ ファイルを参照するかを理解したり、プロセスがクラッシュした場合のシステムへの影響を理解したりするのに役立ちます。

プロセス	機能
カーネル	Linux カーネル
dhcpd	APICがインフラアドレスを割り当てるために実行されている DHCP プロセス
vmmmgr	APIC とハイパーバイザ間のプロセスを処理します
neo	Shell CLI インタープリタ
ae	ローカルAPICアプライアンスの状態とインベントリを処理します
eventmgr	システム上のすべてのイベントと障害を処理します
bootmgr	ファブリック ノードでの起動とファームウェアの更新を制御します
snoopy	Shell CLI ヘルプ、タブ コマンド補完
scripthandler	L4-L7 デバイスのスクリプトと通信を処理します
dbgr	プロセスがクラッシュしたときにコア ファイルを生成します
nginx	Web サービス処理 GUI および REST API アクセス
appliancedirector	APIC クラスタの形成と制御を処理します
sshd	APIC への SSH アクセスを有効化
perfwatch	Linux cgroup 技術情報の使用法を監視します
observer	ファブリック システムと状態、統計、正常性のデータ処理を監視します
lldpad	LLDP エージェント
topomgr	ファブリックのトポロジとインベントリを維持します

Cisco APIC トラブルシューティング オペレーション

Cisco APIC システムのシャットダウン

この手順では、Cisco Application Policy Infrastructure Controller（APIC）システムをシャットダウンします。システムをシャットダウンした後、ファブリック全体を再配置してから電源を入れ、それに応じてタイム ゾーンおよび/または NTP サーバーを更新します。

始める前に

クラスタの健全性が完全に適合し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、**[システム（System）] > [コントローラ（Controllers）]** を選択します。
ステップ 2 ナビゲーション ウィンドウで、**[コントローラ（Controllers）] > *apic_name*** を選択します。
ステップ 3 Cisco APIC を右クリックし、**[シャットダウン（Shutdown）]** を選択します。
ステップ 4 Cisco APIC を再配置してから、電源を入れます。
ステップ 5 クラスタが完全に収束したことを確認します。
ステップ 6 次の Cisco APIC についてこの手順を繰り返します。

GUI を使用した Cisco APIC のシャットダウン

この手順では、Cisco Application Policy Infrastructure Controller（APIC）をシャットダウンします。この手順では、Cisco APIC システム全体ではなく、1 つの Cisco APIC システムのみがシャットダウンされます。この手順に従うと、コントローラはすぐにシャットダウンします。コントローラを元に戻すには、実際のマシンから実行するしかないため、シャットダウンの実行には注意が必要です。マシンにアクセスする必要がある場合は、「GUI を使用した LED ロケータの制御 （114 ページ）」を参照してください。

（注） 可能であれば、Cisco APIC を 1 つずつ移動します。クラスタ内にオンラインの Cisco APIC が少なくとも 2 つある限り、読み取り/書き込みアクセスが可能です。一度に複数の Cisco APIC を再配置する必要がある場合、これにより、1 つまたはすべてのコントローラがオンラインになり、ファブリックはシャットダウン時に読み取り専用モードになります。この間、エンドポイントの移動（仮想マシンの移動を含む）を含むポリシーの変更はできません。

手順

ステップ 1 メニュー バーで、**[システム（System）]** > **[コントローラ（Controllers）]** を選択します。
ステップ 2 ナビゲーション ウィンドウで、**[コントローラ（Controllers）]** > ***apic_name*** を選択します。
ステップ 3 Cisco APIC を右クリックし、**[シャットダウン（Shutdown）]** を選択します。
ステップ 4 Cisco APIC を再配置してから、電源を入れます。
ステップ 5 クラスタが完全に収束したことを確認します。

GUI を使用した APIC リロード オプションの使用

この手順では、GUI を使用して、Cisco APIC システム全体ではなく Cisco Application Policy Infrastructure Controller（APIC）をリロードします。

手順

ステップ 1 メニュー バーで、**[システム（System）]** > **[コントローラ（Controllers）]** を選択します。
ステップ 2 ナビゲーション ウィンドウで、**[コントローラ（Controllers）]** > ***apic_name*** を選択します。
ステップ 3 Cisco APIC を右クリックし、**[リロード（Reload）]** を選択します。

GUI を使用した LED ロケータの制御

この手順では、GUI を使用して Cisco Application Policy Infrastructure Controller（APIC）の LED ロケータをオンまたはオフにします。

手順

ステップ 1 メニュー バーで、**[システム（System）]** > **[コントローラ（Controllers）]** を選択します。
ステップ 2 ナビゲーション ウィンドウで、**[コントローラ（Controllers）]** > ***apic_name*** を選択します。
ステップ 3 Cisco APIC を右クリックし、必要に応じて **[ロケータ LED をオンにする（Turn On Locator LED）]** または **[ロケータ LED をオンにする（Turn On Locator LED）]** を選択します。

GUI を使用したファブリックの電源切断

この手順では、電源メンテナンスのため、Cisco Application Policy Infrastructure Controller（APIC）GUI および Cisco 統合管理コントローラ （IMC）GUI を使用してファブリックの電源を切断します。

手順

ステップ 1 Cisco APIC GUI を使用して、最後の 1 台を残し、すべての Cisco APIC をシャットダウンします。

a) Cisco APIC にログインします。
b) メニュー バーで、**[システム（System）]** > **[コントローラ（Controllers）]** を選択します。
c) Cisco APIC のいずれかのナビゲーションウィンドウで、**[コントローラ（Controllers）]** > ***apic_name***を選択します。
d) Cisco APIC を右クリックし、**[シャットダウン（Shutdown）]** を選択します。
e) 最後の 1 台を除く他のすべての Cisco APIC について、手順 1.c （115 ページ） と 1.d （115 ページ） を繰り返します。

ステップ 2 Cisco IMC GUI を使用して、最後の Cisco APIC をシャットダウンします。

a) 最後の Cisco APIC の Cisco IMC GUI にログインします。
b) [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。
c) **[シャーシ（Chassis）]** メニューで **[サマリー（Summary）]** を選択します。
d) 作業ペイン上部のツールバーで、**[ホストの電源（Host Power）]** > **[シャットダウン（Shut Down）]**を選択します。

最後の Cisco APIC では、サーバが読み取り専用モードになり、Cisco APIC GUI を使用してシャットダウンリクエストを処理することができなくなるため、Cisco IMC GUI を使用してシャットダウンする必要があります。

ステップ 3 すべての Cisco APIC をシャットダウンした後、各電源装置をオフにしてスイッチの電源をオフにします。

GUI を使用したファブリックの電源投入

この手順では、Cisco 統合管理コントローラ （IMC）GUI を使用してファブリックに電源を入れます。

手順

ステップ 1 Cisco IMC GUI を使用して Cisco APIC の電源をオンにします。

a) Cisco APIC の Cisco IMC GUI にログインします。
b) [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

c) **[シャーシ（Chassis）]** メニューで **[サマリー（Summary）]** を選択します。
d) 作業ペイン上部のツールバーで、**[ホストの電源（Host Power）]** > **[電源オン（Power On）]**を選択します。
e) すべての Cisco APIC に対し、これらのサブステップを繰り返します。

ステップ 2 Cisco APIC に直接接続されているリーフ スイッチの電源をオンにします。

ステップ 3 リーフ スイッチの電源をオンにしてから約 1 分後に、スパイン スイッチの電源をオンにします。

ステップ 4 ファブリックの残りのリーフ スイッチで電源をオンにします。

Cisco APIC は LLDP により、直接接続されているリーフ スイッチを検出し、その後スパイン スイッチと残りのリーフ スイッチを検出します。Cisco APIC はリロードとシャットダウン後も構成とファブリック メンバーシップを保持するので、検出は自動的に行われます。Cisco APIC が接続されているすべてのリーフ スイッチを検出し、スパインスイッチを検出した後、クラスタは完全に適合した状態で起動します。

スイッチ操作

GUI からの無効なインターフェイスおよび廃止されたスイッチの手動での削除

ファブリック ポートがシャットダウンされてから再びアップされるシナリオでは、ポート エントリが GUI で無効のままになる可能性があります。これが発生した場合、ポートで操作を実行できません。これを解決するには、ポートを GUI から手動で削除する必要があります。

手順

ステップ 1 **[ファブリック（Fabric）]** タブで、**[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、**[インターフェイスと廃止されたスイッチを無効にする（Disabled Interfaces and Decommissioned Switches）]** をクリックします。
無効になっているインターフェイスと廃止されたスイッチのリストが、**[作業（Work）]**ペインの要約テーブルに表示されます。

ステップ 3 **[作業（Work）]** ペインで、削除するインターフェイスまたはスイッチを右クリックし、**[削除（Delete）]** を選択します。

スイッチのデコミッションおよび再コミッション

ポッドのすべてのノードをデコミッションし、再コミッションするには、この手順を実行します。この使用例の 1 つは、ノード ID をより論理的でスケーラブルな番号付け規則に変更することです。

手順

ステップ 1 ノードごとに次の手順に従って、ポッド内のノードをデコミッションします。

a) **[ファブリック（Fabric）]** > **[インベントリ（Inventory）]** に移動し、**Pod** を展開します。

b) スイッチを選択して右クリックし、**[コントローラから削除（Remove from Controller）]** を選択します。

c) アクションを確認し、**[OK]** をクリックします。

プロセスにはおよそ 10 分ほどかかります。ノードは自動的にワイプされ、リロードされます。さらに、ノード構成がコントローラから削除されます。

d) 廃止されたノードにポート プロファイル機能が展開されている場合、一部のポート構成は残りの構成とともに削除されません。ポートをデフォルト状態に戻すには、デコミッション後に手動で構成を削除する必要があります。これを行うにはスイッチにログインし、**setup-clean-config.sh** スクリプトを実行し、実行されるまで待ちます。それから、**リロード** コマンドを入力します。

ステップ 2 すべてのスイッチがポッドから廃止されたら、それらがすべて物理的に接続され、目的の構成で起動されていることを確認します。

ステップ 3 次のアクションを実行して、各ノードを再稼働させます。

（注）
ポート プロファイルが構成されたノードを新しいノードとして再コミッショ二ングさせる前に、6.0（7）以前のリリースでは、ポート構成をデフォルト設定に復元するために**setup-clean-config.sh script** を実行する必要があります。または、ポート構成をデフォルト設定に復元するために 6.0（8）以降の場合、**setup-clean-config.sh -d** スクリプトを実行する必要があります。

a) **[ファブリック（Fabric）]**>**[インベントリ（Inventory）]**に移動し、**[クイック スタート（Quick Start）]** を展開し、**[ノードまたはポッドのセットアップ（Node or Pod Setup）** をクリックします。

b) **[セットアップ ノード（Setup Node）]** をクリックします。

c) **[ポッド ID（Pod ID）]** フィールドで、ポッド ID を選択します。

d) [+] をクリックして、**[ノード（Nodes）]** テーブルを開きます。

e) スイッチのノード ID、シリアル番号、スイッチ名、TEP プール ID、およびロール（**リーフ**または**スパイン**）を入力します。

f) [Update] をクリックします。

ステップ 4 **[ファブリック（Fabric）]** > **[インベントリ（Inventory）]** > **[ファブリック メンバーシップ（ Fabric Membership）]** に移動して、ノードがすべて設定されていることを確認します。

次のタスク

ポッドがマルチポッドトポロジ内のポッドの1つである場合は、このポッドとノード用にマルチポッドを再構成します。詳細については、『*Cisco APIC Layer 3 Networking* 構成ガイド』「マルチポッド」を参照してください。

Cisco ACI モード スイッチのクリーンリロード

この手順では、Cisco ACI モード スイッチのクリーン リロードを実行します。クリーン リロードでは、スイッチのすべての構成が消去されます。スイッチが起動すると、スイッチは Cisco Application Policy Infrastructure Controller（APIC）から構成を取得します。

手順

ステップ 1 クリーン リロードするスイッチにログインします。

ステップ 2 **setup-clean-config.sh** スクリプトに **-k** 引数を指定して実行します。

例：

```
switch1# setup-clean-config.sh -k
```

ステップ 3 スイッチをリロードします。

例：

```
switch1# reload
```

切断されたリーフの復元

リーフにプッシュされた構成が原因で、リーフ上のすべてのファブリック インターフェイス（リーフをスパインに接続するインターフェイス）が無効になっている場合、リーフへの接続は永久に失われ、リーフはファブリック内で非アクティブになります。接続が失われたため、構成をリーフにプッシュしようとしても機能しません。この章では、切断されたリーフを回復する方法について説明します。

NX-OS-Style CLI を使用した切断されたリーフの復元

この手順では、Cisco Application Policy Infrastructure Controller（APIC）NX-OS スタイルの CLI を使用してファブリック インターフェイスを有効にします。REST API コールを実行できる外部ツールがない場合は、この手順を使用します。

（注） この手順では、1/31 がスパイン スイッチに接続するリーフ スイッチ ポートの 1 つであることを前提としています。

手順

ステップ 1 Cisco APIC NX-OS-style CLI を使用して、ブロック リスト ポリシーを削除します。

例：

```
apic1# podId='1'
apic1# nodeId='103'
apic1# interface='eth1/31'
apic1# icurl -sX POST 'http://127.0.0.1:7777/api/mo/.json' -d '{"fabricRsOosPath":{"attributes":

{"dn":"uni/fabric/outofsvc/rsoosPath-[topology/pod-'$podId'/paths-'$nodeId'/pathep-['$interface']]","status":"deleted"}}}'
```

ステップ 2 リーフ スイッチまたはスパイン スイッチの CLI を使用して、サービス中のポートを設定して、リーフ スイッチのポートを起動します。

例：

```
switch1# podId='1'
switch1# nodeId='103'
switch1# interface='eth1/31'
switch1# icurl -X POST
'http://127.0.0.1:7777/api/node/mo/topology/pod-'$podId'/node-'$nodeId'/sys/action.json'
  -d
'{"actionLSubj":{"attributes":{"oDn":"sys/phys-['$interface']"},"children":[{"l1EthIfSetInServiceLTask":

  {"attributes":{"adminSt":"start"}}}]}}'
```

REST API を使用した切断されたリーフの復元

切断されたリーフ スイッチを復元するには、次のプロセスを使用して、ファブリック インターフェイスの少なくとも 1 つを有効にする必要があります。残りのインターフェイスは、GUI、REST API、または CLI を使用して有効にできます。

最初のインターフェイスを有効にするには、REST API を使用してポリシーを投稿し、投稿されたポリシーを削除し、ファブリック ポートをアウト オブ サービスにします。次のように、ポリシーをリーフ スイッチにポストして、アウト オブ サービスのポートをインサービスにすることができます。

（注） この手順では、1/49 がスパイン スイッチに接続するリーフ スイッチ ポートの 1 つであることを前提としています。

手順

ステップ 1 REST API を使用して、Cisco APIC からブロック リスト ポリシーをクリアします。

例：

```
$APIC_Address/api/policymgr/mo/.xml
<polUni>
    <fabricInst>
        <fabricOOServicePol>
            <fabricRsOosPath tDn="topology/pod-1/paths-$LEAF_Id/pathep-[eth1/49]" lc="blacklist"
status ="deleted"/>
        </fabricOOServicePol>
    </fabricInst>
</polUni>
```

ステップ 2 ローカル タスクをノード自体にポストし、**l1EthIfSetInServiceLTask** を使用して必要なインターフェイスを起動します。

例：

```
$LEAF_Address/api/node/mo/topology/pod-1/node-$LEAF_Id/sys/action.xml
<actionLSubj oDn="sys/phys-[eth1/49]">
    <l1EthIfSetInServiceLTask adminSt='start'/>
</actionLSubj>
```

ファブリックの再構築の実行

ファブリックの再構築

⚠

注意 この手順は非常に混乱を招きます。既存のファブリックを取り除き、新しいファブリックを作り直します。

この手順により、ファブリックを再構築（再初期化）できます。これは、次のいずれかの理由で必要になる場合があります。

- TEP IP を変更するには
- インフラ VLAN を変更するには
- ファブリック名を変更するには
- TAC トラブルシューティング タスクを実行するには

APIC を削除すると、それらの構成が消去され、スタートアップ スクリプトでそれらが表示されます。APIC でこれを実行する順序は任意ですが、すべて（ファブリック内のすべてのリーフとスパイン）で手順を実行するようにしてください。

始める前に

以下が所定の場所に準備されていることを確認します。

- 定期的にスケジュールされた構成のバックアップ
- リーフとスパインへのコンソールアクセス

- KVM コンソール アクセスに必要な構成済みの到達可能な CIMC
- Java の問題なし

手順

ステップ 1 現在の構成を保持したい場合は、構成のエクスポートを実行できます。詳細については、『*Cisco ACI Configuration Files：Import and Export*』の文書 https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html を参照してください。

ステップ 2 KVM コンソールに接続し、次のコマンドを入力して、APIC の設定を消去します。

a) **>acidiag touch clean**
b) **>acidiag touch setup**
c) **>acidiag reboot**

各ノードがファブリック検出モードで起動し、以前に構成されたファブリックの一部ではないことを確認します。

（注）
スタートアップ スクリプトで APIC を起動しないため、 **acidiag touch** コマンドだけはこの手順では役に立ちません。

注意
以前のすべてのファブリック構成が削除されていることを確認することが非常に重要です。単一のノードに以前のファブリック構成が存在する場合でも、ファブリックを再構築することはできません。

ステップ 3 以前の構成がすべて削除されたら、すべての APIC のスタートアップ スクリプトを実行します。この時点で、上記の値、TEP、TEP Vlan、および/またはファブリック名のいずれかを変更できます。これらがすべての APIC で一貫していることを確認してください。詳細については、『*Cisco APIC Getting Started Guide*』の https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html を参照してください。

ステップ 4 ファブリック ノードをクリーン リブートするには、各ファブリック ノードにログインし、次を実行します。

a) **>setup-clean-config.sh**
b) **>reload**

ステップ 5 apic1 にログインし、構成のインポートを実行します。詳細については、『*Cisco ACI Configuration Files：Import and Export*』の文書 https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html を参照してください。

ステップ 6 ファブリックが以前のファブリック登録ポリシーを使用してノード上でファブリックを再構築するようになったため、数分間待ちます。（ファブリックのサイズによっては、この作業に時間がかかる場合があります。）

ループバック障害のトラブルシューティング

障害の発生したライン カードの識別

このセクションでは、ループバック障害が発生したときに、障害が発生したラインカードを特定する方法について説明します。

始める前に

ファブリック ノードのオンデマンド TechSupport ポリシーを作成しておく必要があります。オンデマンド TechSupport ポリシーをまだ作成していない場合は、*Cisco APIC* ベーシック コンフィギュレーション ガイド の「GUI を使用したオンデマンド テクニカル サポート ファイルの送信」セクションを参照してください。

手順

ステップ 1 ファブリック ノードのオンデマンド TechSupport ポリシーのログの場所ファイルを収集します。収集を開始するには：

a) メニュー バーで、[Admin] をクリックします。
b) サブメニュー バーで、[Import/Export] をクリックします。
c) **[ナビゲーション（Navigation）]** ペインで、**[ポリシーのエクスポート（Export Policies）]** を展開し、ファブリック ノードのオンデマンド TechSupport ポリシーを右クリックします。
オプションのリストが表示されます。
d) **[Tech サポートの収集（Collect Tech Supports）]** を選択します。
[Tech サポートの収集（Collect Tech Supports）] ダイアログ ボックスが表示されます。
e) **[Tech サポートの収集（Collect Tech Supports）]** ダイアログ ボックスで、**[はい（Yes）]** をクリックして、テクニカル サポート情報の収集を開始します。

ステップ 2 ファブリック ノードのオンデマンド TechSupport ポリシーのログの場所ファイルをダウンロードします。ログの場所ファイルをダウンロードするには：

a) **[作業（Work）]** ペインの [オンデマンド TechSupport ポリシー（On-Demand TechSupport policy）] ウィンドウから、**[操作性（Operational）]** タブをクリックします。
[オンデマンド TechSupport ポリシー（On-Demand TechSupport policy）] ウィンドウに、**[ログの場所（Logs Location）]** 列を含むいくつかの列とともに概要テーブルが表示されます。
b) **[ログの場所（Logs Location）]** 列の URL をクリックします。

ステップ 3 ログの場所ファイル内で、/var/sysmgr/tmp_logs/ ディレクトリに移動し、svc_ifc_techsup_nxos.tar ファイルを解凍します。

```
-bash-4.1$ tar xopf svc_ifc_techsup_nxos.tar
```

show_tech_info ディレクトリが作成されます。

ステップ 4 **zgrep "fclc-conn failed" show-tech-sup-output.gz | less** を実行します。

```
-bash-4.1$ zgrep "fclc-conn failed" show-tech-sup-output.gz | less
[103] diag_port_lb_fail_module: Bringing down the module 25 for Loopback test failed. Packets possibly
 lost on the switch SPINE or LC fabric (fclc-conn failed)
[103] diag_port_lb_fail_module: Bringing down the module 24 for Loopback test failed. Packets possibly
 lost on the switch SPINE or LC fabric (fclc-conn failed)
```

（注）
fclc-conn failed メッセージは、ラインカードの障害を示しています。

ステップ 5 現在障害が発生しているファブリック カードの電源を入れ直し、ファブリック カードがオンラインになることを確認します。

ステップ 6 ファブリック カードがオンラインにならない場合、またはファブリック カードが再びオフラインになった後、すぐに diag_port_lb.log ファイルを収集して、そのファイルを TAC チームに送信します。diag_port_lb.log ファイルは、ログの場所ファイルの /var/sysmgr/tmp_logs/ ディレクトリにあります。

不要な _ui_ オブジェクトの削除

注意 APIC の基本 GUI を使用して行われた変更を拡張 GUI で表示することはできますが、変更を加えることはできません。また、拡張 GUI で行われた変更を基本 GUI で表示することはできません。基本 GUI と NX-OS スタイルの CLI は常に同期されるため、NX-OS スタイルの CLI から行った変更は基本 GUI に表示され、基本 GUI で行った変更は NX-OS スタイルの CLI に表示されます。ただし拡張 GUI と NX-OS スタイルの CLI の間ではこのような同期が行われません。次の例を参照してください。

- 基本 GUI モードと拡張 GUI モードを混在させないでください。拡張モードを使用して 2 つのポートにインターフェイス ポリシーを適用し、次に基本モードを使用していずれかのポートの設定を変更すると、変更内容が両方のポートに適用される可能性があります。
- APIC でインターフェイスごとの設定を行う際に、拡張 GUI と CLI を混在させないでください。GUI で行われた設定が、NX-OS CLI では部分的にしか機能しない可能性があります。

  たとえば、GUI の **[Tenants]** > ***[tenant-name]*** > **[Application Profiles]** > ***[application-profile-name]*** > **[Application EPGs]** > ***[EPG-name]*** > **[Static Ports]** > **[Deploy Static EPG on PC, VPC, or Interface]** でスイッチ ポートを設定したと仮定します。

  次に NX-OS スタイルの CLI で show running-config コマンドを使用すると、以下のような出力を受信します。

```
leaf 102
interface ethernet 1/15
switchport trunk allowed vlan 201 tenant t1 application ap1 epg ep1
 exit
 exit
```

  NX-OS スタイルの CLI でこれらのコマンドを使用してスタティック ポートを設定すると、次のエラーが発生します。

```
apic1(config)# leaf 102
apic1(config-leaf)# interface ethernet 1/15
apic1(config-leaf-if)# switchport trunk allowed vlan 201 tenant t1 application ap1
epg ep1
No vlan-domain associated to node 102 interface ethernet1/15 encap vlan-201
```

  これは、CLI に APIC GUI では実行されない検証があることが原因です。show running-config コマンドによって出力されたコマンドが NX-OS CLI で機能するためには、VLAN ドメインが事前に設定されている必要があります。設定の順序は GUI に適用されません。

- 拡張 GUI を使用する前に、基本 GUI または NX-OS CLI によって変更を加えないでください。変更を加えてしまうと、名前の先頭に `_ui_` が付加されたオブジェクトが意図せず作成される場合があります。このオブジェクトは拡張 GUI で変更または削除できません。

高度な GUI を使用する前に、基本 GUI または NX-OS CLI を変更する場合、これは意図せずにオブジェクトが作成され（名前に_ui_ が付加される）、高度な GUI で変更または削除できなくなる場合があります。

このようなオブジェクトを削除する手順については、REST API を使用した不要な _ui_ オブジェクトの削除 （125 ページ）を参照してください。

REST API を使用した不要な _ui_ オブジェクトの削除

Cisco APIC GUI を使用する前に Cisco NX OS スタイル CLI で変更を行い、名前の先頭に _ui_ が付加されたオブジェクトが表示された場合は、API に対して次を含む REST API 要求を実行することでこれらのオブジェクトを削除できます。

- クラス名（例：**infraAccPortGrp**）
- Dn 属性（例：**dn="uni/infra/funcprof/accportgrp-__ui_l101_eth1--31"**
- **status="deleted"** に設定したステータス属性

次の手順で API に POST を実行します。

手順

ステップ 1 削除するオブジェクトへの書き込みアクセス権を持つユーザ アカウントにログインします。

ステップ 2 API に次の例のような POST を送信します。

```
POST https://192.168.20.123/api/mo/uni.xml
Payload:<infraAccPortGrp dn="uni/infra/funcprof/accportgrp-__ui_l101_eth1--31" status="deleted"/>
```

Cisco APIC SSD の交換

この手順を使用して、Cisco APIC のソリッド ステート ドライブ（SSD）を交換します。

（注） この手順は、クラスタに正常な SSD を備えた APIC が少なくとも 1 つあり、完全に適合している場合にのみ実行する必要があります。クラスタ内のすべての APIC コントローラに障害が発生した SSD がある場合は、Cisco Technical Assistance Center（TAC）でケースをオープンしてください。

Cisco APIC のソリッド ステート ドライブ（SSD）の交換

始める前に

- Cisco IMC リリースが 2.0(9c) より前の場合は、ソリッド ステート ドライブ (SSD) を交換する前に Cisco IMC ソフトウェアをアップグレードする必要があります。対象の Cisco IMC リリースのリリース ノートを参照して、現在のリリースから対象のリリースへの推奨されるアップグレードパスを確認してください。このリンクにある『*Cisco Host Upgrade Utility（HUU）User Guide*』の現在のバージョンの指示に従って、アップグレードを実行します。
- Cisco IMC BIOS で、トラステッドプラットフォーム モジュール（TPM）の状態が「有効」に設定されていることを確認します。KVM コンソールを使用して BIOS 設定にアクセスすると、**[高度（Advanced）] > [トラステッド コンピューティング（Trusted Computing）] > [TPM ステート（TPM State）]** で TPM の状態を表示および構成できます。

（注） TPM ステートが「無効」の場合、APIC は起動に失敗します。

- シスコ ソフトウェア ダウンロード サイトから APIC `.iso` イメージを取得します。

（注） APIC `.iso` イメージのリリース バージョンは、クラスタ内の他の APIC コントローラと同じバージョンである必要があります。

手順

ステップ 1 クラスタ内の別の APIC から、SSD を交換する APIC を廃止します。

a) メニューバーで、 **System** > **Controllers** を選択します。
b) **Navigation** ウィンドウで、 **Controllers** > **apic_controller_name** > **Cluster as Seen by Node** を展開します。**apic_controller_name** には、廃止されていない APIC コントローラを指定します。
c) 継続する前に、**Work** ウィンドウで、クラスタの **Health State** (**Active Controllers** サマリ テーブルに示されているもの) が **Fully Fit** になっていることを確認します。
d) 同じ **[作業（Work）]** ペインで、廃止するコントローラを選択し、**[アクション（Actions）] > [廃止（Decommission）]** をクリックします。
e) **Yes** をクリックします。
解放されたコントローラは [Operational State] 列に [Unregistered] と表示されます。コントローラは稼動対象外になり、**[作業（Work）]** ウィンドウには表示されなくなります。

ステップ 2 古い SSD があればそれを物理的に取り外し、新しい SSD を追加します。

ステップ 3 Cisco IMC で、新しく取り付けた SSD を使用して RAID ボリュームを作成します。

Cisco IMC については、『*Cisco UCS C* シリーズ統合管理コントローラ *GUI* 構成ガイド』を参照してください。「ストレージアダプタの管理」の章の「未使用の物理ドライブからの仮想ドライブの作成」の手順に従って、RAID 0 仮想ドライブを作成および初期化します。

ステップ 4 Cisco IMC で、仮想メディアを使用して APIC イメージをインストールします。この手順では、SSD がパーティション分割され、APIC ソフトウェアが HDD にインストールされます。

（注）
Cisco APIC リリース 4.x 以降の新規インストールについては、『*Cisco APIC* のインストール、アップグレード、およびダウングレード ガイド』を参照してください。

a) Cisco IMC vMedia 機能を使用して、APIC `.iso` イメージをマウントします。
b) コントローラを起動し電源を再投入します。
c) 起動プロセス中を押して **F6** を選択、 **Cisco vKVM マッピング vDVD** ワンタイム ブート デバイスとして。BIOS パスワードを入力する必要があります。デフォルトのパスワードは「password」です。
d) 最初の起動時に、構成スクリプトが実行されます。画面の指示に従って、APIC ソフトウェアの初期設定を構成します。
e) インストールが完了したら、仮想メディア マウントのマッピングを解除します。

ステップ 5 クラスタ内の APIC から、廃止された APIC を起動します。

a) クラスタの一部である他の APIC を選択します。メニュー バーで、 **[システム (System)]** > **[コントローラ (Controllers)]** を選択します。
b) **Navigation** ウィンドウで、 **Controllers** > **apic_controller_name** > **Cluster as Seen by Node** を展開します。 **apic_controller_name** には、クラスタの一部であるアクティブなコントローラーを指定します。
c) **[作業（Work）]** ウィンドウで、**未登録（Unregistered）** と **稼働状態（Operational State）** 列に表示されている廃止されているコントローラをクリックします。
d) **Work** ウィンドウで、**Actions** > **Commission** をクリックします。
e) **Confirmation** ダイアログボックスで **Yes** をクリックします。

稼働済みコントローラには、正常性状態が**完全適合**と表示され、動作状態が**使用可**能と表示されます。これで、コントローラが **[作業（Work）]** ペインに表示されます。

CRC エラー カウンターの表示

CRC およびストンプ CRC エラー カウンターの表示

Cisco APIC リリース 4.2(3) 以降、CRC エラーは、CRC エラーとストンプ CRC エラーの 2 つのカテゴリに分けられています。CRCエラーはローカルでドロップされた破損フレームであり、ストンプCRCエラーはカットスルー スイッチによる破損フレームです。この区別により、CRC エラーの影響を受ける実際のインターフェイスを識別し、ファブリック内の物理層の問題のトラブルシューティングを行うことが容易になります。

このセクションでは、CRC およびストンプ CRC エラーを表示する方法を示します。

GUI を使用した CRC エラーの表示

このセクションでは、GUI を使用して CRC エラーおよびストンプ CRC エラー カウンターを表示する方法を示します。

手順の概要

1. メニュー バーで **[ファブリック（Fabric）] > [インベントリ（Inventory）]** を選択します。
2. **[ナビゲーション（Navigation）]** ペインで、ポッドをクリックして展開します。
3. **[インターフェイス（Interfaces）]** をクリックして展開します。
4. インターフェイスをクリックして、選択します。
5. **[作業（Work）]** ペインで、**[エラー カウンター（Error Counters）]** タブをクリックします。

手順の詳細

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、ポッドをクリックして展開します。

ステップ 3 **[インターフェイス（Interfaces）]** をクリックして展開します。
[ナビゲーション（Navigation）] ペインに、インターフェイスのリストが表示されます。

ステップ 4 インターフェイスをクリックして、選択します。
[作業（Work）] ペインに、ウィンドウの上部にタブのリストが表示されます。

ステップ 5 **[作業（Work）]** ペインで、**[エラー カウンター（Error Counters）]** タブをクリックします。
CRC エラー（FCS エラー）および**ストンプCRC エラー（パケット）**を含む、エラー カテゴリのリストが表示されます。

CLI を使用した CRC エラーの表示

このセクションでは、CLI を使用して CRC エラーおよびストンプ CRC エラー カウンターを表示する方法を示します。

手順

CRC エラーおよびストンプ CRC エラーを表示するには:

例：

```
Switch# show interface ethernet 1/1
Ethernet1/1 is up
admin state is up, Dedicated Interface
```

```
  Belongs to po4
  Hardware: 100/1000/10000/25000/auto Ethernet, address: 00a6.cab6.bda5 (bia 00a6.cab6.bda5)
  MTU 9000 bytes, BW 10000000 Kbit, DLY 1 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, medium is broadcast
  Port mode is trunk
  full-duplex, 10 Gb/s, media type is 10G
  FEC (forward-error-correction) : disable-fec
^[[B  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned off
  Rate mode is dedicated
  Switchport monitor is off
  EtherType is 0x8100
  EEE (efficient-ethernet) : n/a
  Last link flapped 3d02h
  Last clearing of "show interface" counters never
  1 interface resets
  30 seconds input rate 0 bits/sec, 0 packets/sec
  30 seconds output rate 4992 bits/sec, 8 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 0 bps, 0 pps; output rate 4536 bps, 8 pps
  RX
    0 unicast packets  200563 multicast packets  0 broadcast packets
    200563 input packets  27949761 bytes
    0 jumbo packets  0 storm suppression bytes
    0 runts  0 giants  0 CRC  0 Stomped CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  0 input discard
    0 input buffer drop  0 input total drop
    0 Rx pause
  TX
    0 unicast packets  2156812 multicast packets  0 broadcast packets
    2156812 output packets  151413837 bytes
    0 jumbo packets
    0 output error  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble  0 output discard
    0 output buffer drops  0 output total drops
    0 Tx pause
```

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。