



## Q-in-Q VLAN トンネルの設定

- [Q-in-Q トンネルについて \(1 ページ\)](#)
- [注意事項と制約事項 \(7 ページ\)](#)
- [複数プロバイダー VLAN を使用した選択的 Q-in-Q の注意事項と制約事項 \(9 ページ\)](#)
- [Q-in-Q トンネルおよびレイヤ 2 プロトコルのトンネリングの設定 \(10 ページ\)](#)
- [複合アクセス ポート機能セットの設定 \(20 ページ\)](#)
- [Q-in-Q 設定の確認 \(22 ページ\)](#)
- [Q-in-Q およびレイヤ 2 プロトコルのトンネリングの設定例 \(23 ページ\)](#)

### Q-in-Q トンネルについて

この章では、Cisco NX-OS デバイス上で IEEE 802.1Q-in-Q VLAN トンネルおよびレイヤ 2 プロトコルのトンネリングを設定する方法について説明します。

Q-in-Q VLAN トンネルを使用することで、サービスプロバイダーは第 2 の 802.1Q タグをすでにタグ付けされたフレームに追加して、カスタマーに内部使用の VLAN をすべて提供しながら、インフラストラクチャ内で異なるカスタマーのトラフィックを分離することができます。

### Q-in-Q トンネリング

サービスプロバイダーのビジネスカスタマーには、多くの場合、サポートする VLAN ID および VLAN の数に固有の要件があります。同一サービスプロバイダネットワークのさまざまなカスタマーが必要とする VLAN 範囲は重複し、インフラストラクチャを通るカスタマーのトラフィックは混合してしまふことがあります。カスタマーごとに一意の VLAN ID 範囲を割り当てると、カスタマーの設定が制限され、802.1Q 仕様の VLAN に関する上限 (4096 個) を容易に超えてしまいます。

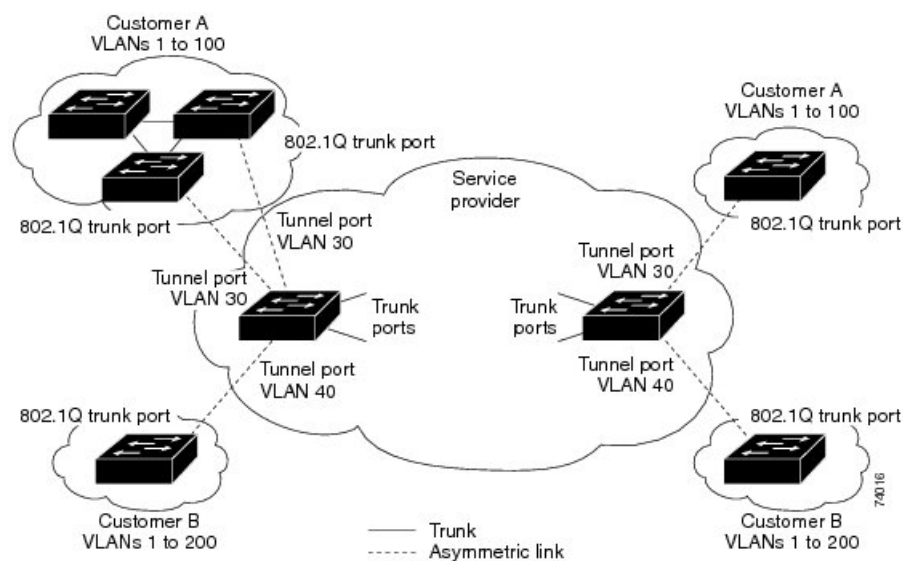


- (注) Q-in-Q は、ポートチャネルでサポートされています。非対称リンクとしてポートチャネルを設定するには、ポートチャネル内のすべてのポートが同じトンネリング設定でなければなりません。

サービスプロバイダは、802.1Q トンネリング機能を使用すると、単一の VLAN を使用して、複数の VLAN を含む顧客をサポートできます。サービスプロバイダーのインフラストラクチャ上で顧客 VLAN ID が保持され、同じ VLAN 上に存在するように見えても、異なる顧客からのトラフィックが分離されます。IEEE 802.1Q トンネリングは、VLAN-in-VLAN 階層構造およびタグ付きパケットへのタグgingによって、VLAN スペースを拡張します。802.1Q トンネリングをサポートするように設定されたポートは、トンネルポートといえます。トンネリングを設定する場合、トンネリング専用の VLAN にトンネルポートを割り当てます。顧客ごとに個別の VLAN が必要ですが、その VLAN は顧客の VLAN をすべてサポートします。

適切な VLAN ID で通常どおりにタグ付けされた顧客のトラフィックは、顧客デバイスの 802.1Q トランクポートからサービスプロバイダー側のエッジスイッチのトンネルポートに発信されます。顧客デバイスとエッジスイッチの間のリンクは、一方の端が 802.1Q トランクポート、反対側がトンネルポートとして設定されているので、非対称リンクです。それぞれの顧客に固有のアクセス VLAN ID には、トンネルポートインターフェイスを割り当てます。以下の図を参照してください。

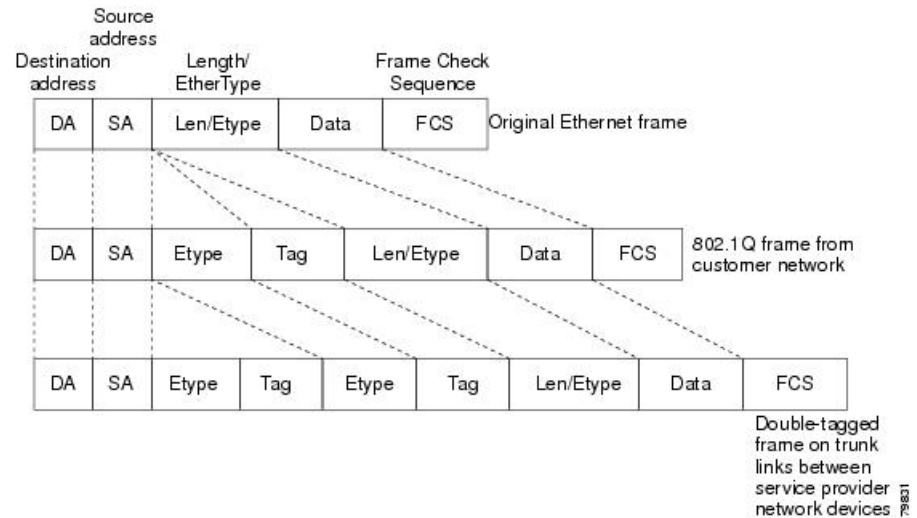
図 1: 802.1Q-in-Q トンネルポート



サービスプロバイダーエッジスイッチのトンネルポートに着信するパケット（適切な VLAN ID すでに 802.1Q タグ付けされている）は、顧客に一意である VLAN ID を含む 802.1Q タグの別のレイヤでカプセル化されます。元々の顧客の 802.1Q タグは、カプセル化されたパケットの中に維持されます。したがって、サービスプロバイダーインフラストラクチャに着信するパケットは二重にタグ付けされます。

外部タグには、顧客の（サービスプロバイダーによって割り当てられた）アクセス VLAN ID が含まれます。（顧客によって割り当てられた）内部タグの VLAN ID は、受信トラフィックの VLAN です。この二重タグgingは、以下の図に示すようにタグスタック構成 Double-Q または Q-in-Q と呼ばれます。

図 2: タグなし、802.1Q タグ付き、および二重タグ付きイーサネット フレーム



この方法で、外部タグの VLAN ID スペースは内部タグの VLAN ID スペースに依存しません。単一の外部 VLAN ID は、個々のカスタマーの全体の VLAN ID スペースを表すことができます。この方法により、カスタマーのレイヤ2 ネットワークをサービスプロバイダーネットワーク全体に拡張して、複数のサイトに仮想 LAN インフラストラクチャを作成することも可能になります。



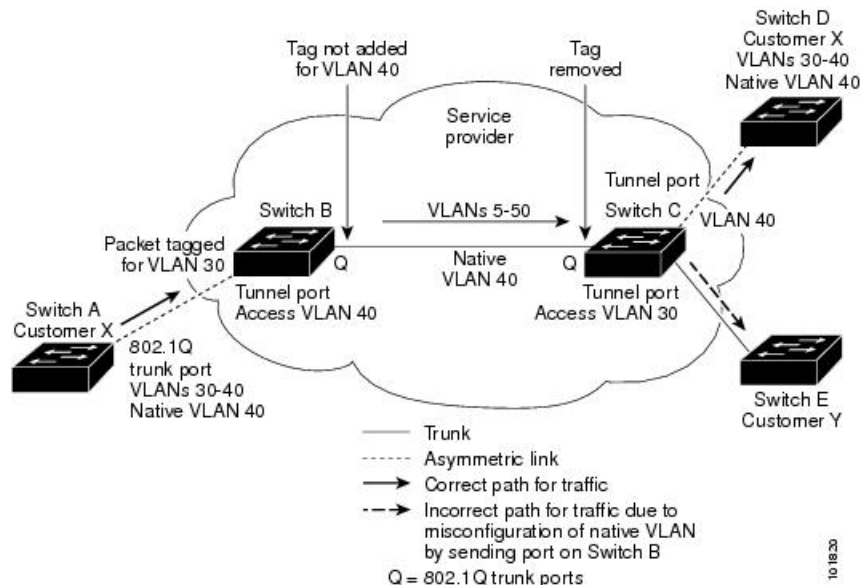
(注) 階層型タギング、すなわちマルチレベルの dot1q タギング Q-in-Q はサポートされていません。

## ネイティブ VLAN のリスク

エッジスイッチで 802.1Q トンネリングを設定する場合は、サービスプロバイダーネットワークにパケットを送信するために、802.1Q トランクポートを使用する必要があります。ただし、サービスプロバイダーネットワークのコアを通過するパケットは、802.1Q トランク、ISL トランク、または非トランッキングリンクで伝送される場合があります。802.1Q トランクをこれらのコアスイッチで使用する場合には、802.1Q トランクのネイティブ VLAN を、同じスイッチ上の dot1q トンネルポートのどのネイティブ VLAN にも一致させないでください。ネイティブ VLAN 上のトラフィックが 802.1Q 送信トランクポートでタグ付けされなくなるためです。

下の図の VLAN 40 は、サービスプロバイダーネットワークの入力エッジスイッチ（スイッチ B）において、カスタマー X からの 802.1Q トランクポートのネイティブ VLAN として設定されています。カスタマー X のスイッチ A は、VLAN 30 のタグ付きパケットを、アクセス VLAN 40 に属する、サービスプロバイダネットワークのスイッチ B の入力トンネルポートに送信します。トンネルポートのアクセス VLAN（VLAN 40）は、エッジスイッチのトランクポートのネイティブ VLAN（VLAN 40）と同じなので、トンネルポートから受信したタグ付きパケットに 802.1Q タグは追加されません。パケットには VLAN 30 タグだけが付いて、サービスプロバイダーネットワークで出力エッジスイッチ（スイッチ C）のトランクポートに送信され、出力スイッチ トンネルによってカスタマー Y に間違えて送信されます。

図 3: ネイティブ VLAN のリスク



ネイティブ VLAN の問題を解決する方法は 2 つあります。

- 802.1Q トランクから出るすべてのパケット（ネイティブ VLAN を含む）が、`vlan dot1q tag native` コマンドを使用してタグ付けされるように、エッジスイッチを設定します。すべての 802.1Q トランクでネイティブ VLAN パケットにタグを付けるようにスイッチを設定した場合、スイッチはタグなしパケットを受信しますが、タグ付きパケットだけを送信します。



(注) **vlan dot1q tag native** コマンドは、すべてのトランクポート上のタギング動作に影響を与えるグローバルコマンドです。

- エッジスイッチのトランクポートのネイティブ VLAN ID が、カスタマー VLAN 範囲に属さないようにします。たとえばトランクポートが VLAN100 ~ 200 のトラフィックを運ぶ場合は、この範囲以外の番号をネイティブ VLAN に割り当てます。

## レイヤ2 プロトコルのトンネリングについて

サービスプロバイダーネットワーク経由で接続される複数のサイトの顧客は、さまざまなレイヤ2 プロトコルを実行して、すべてのリモートサイトおよびローカルサイトを含むようにトポロジを拡大する必要があります。スパニングツリープロトコル (STP) が適切に稼働している必要があり、すべての VLAN で、ローカルサイトおよびサービスプロバイダーインフラストラクチャ経由のすべてのリモートサイトを含む、適切なスパニングツリーを構築する必要があります。Cisco Discovery Protocol (CDP) は、ローカルおよびリモートサイトから隣接するシスコデバイスを検出することができる必要があり、VLAN トランッキングプロトコル

(VTP) は、カスタマー ネットワークのすべてのサイトを通して一貫した VLAN 設定を提供する必要があります。

トンネルポートでマルチタグ付き BPDU を許可するようにスイッチを設定できます。 **l2protocol tunnel allow-double-tag** コマンドをイネーブルにすると、複数のタグが付けられたカスタマー BPDU がトンネルポートに入ると、カスタマー トラフィックからの元の 802.1Q タグが保持され、外部 VLAN タグ (サービス プロバイダーによって割り当てられたカスタマー アクセス VLANID) が追加されます。カプセル化されたパケットに含まれています。したがって、サービス プロバイダー インフラストラクチャに着信するパケットは複数のタグが付けられます。BPDU がサービス プロバイダー ネットワークを離れると、外部タグが削除され、元の複数のタグが付けられた BPDU がカスタマー ネットワークに送信されます。

プロトコルトンネリングがイネーブルになると、サービスプロバイダーインフラストラクチャの受信側にあるエッジスイッチが、レイヤ2プロトコルを特別の MAC アドレスでカプセル化し、サービスプロバイダー ネットワークの端まで送信します。ネットワークのコアスイッチでは、このパケットが処理されずに通常のパケットとして転送されます。CDP、STP、または VTP のブリッジプロトコルデータユニット (BPDU) は、サービスプロバイダー インフラストラクチャを通過し、サービスプロバイダー ネットワークの発信側にあるカスタマー スイッチまで配信されます。同一パケットは同じ VLAN のすべてのカスタマー ポートで受信されます。

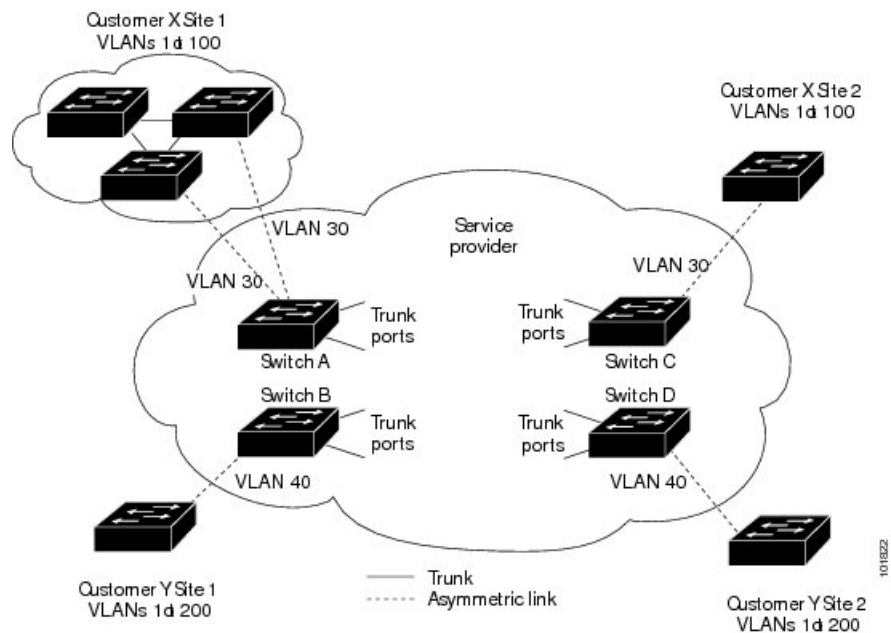
802.1Q トンネリングポートでプロトコルのトンネリングをイネーブルにしていない場合、サービスプロバイダー ネットワークの受信側のリモートスイッチでは BPDU を受信せず、STP、CDP、802.1X、および VTP を適切に実行できません。プロトコルのトンネリングがイネーブルである場合、それぞれのカスタマーネットワークのレイヤ2プロトコルは、サービスプロバイダー ネットワーク内で動作しているものから完全に区別されます。802.1Q トンネリングでサービスプロバイダーネットワークを通してトラフィックを送信する、さまざまなサイトのカスタマー スイッチでは、カスタマー VLAN が完全に認識されます。



- (注) レイヤ2プロトコルのトンネリングは、ソフトウェアでBPDUをトンネリングすることで動作します。スーパーバイザが受信する多数のBPDUによりCPUの負荷が大きくなります。スーパーバイザCPUの負荷を軽減するために、Software レートリミッタを使用する必要がある場合があります。 [レイヤ2プロトコルトンネルポートのしきい値の設定 \(19 ページ\)](#) を参照してください。

たとえば、以下の図で、カスタマー X には、サービスプロバイダー ネットワークを介して接続された同じ VLAN に 4 台のスイッチがあります。ネットワークが BPDU をトンネリングしないと、ネットワークの遠端のスイッチは STP、CDP、802.1X、および VTP プロトコルを正しく実行できません。

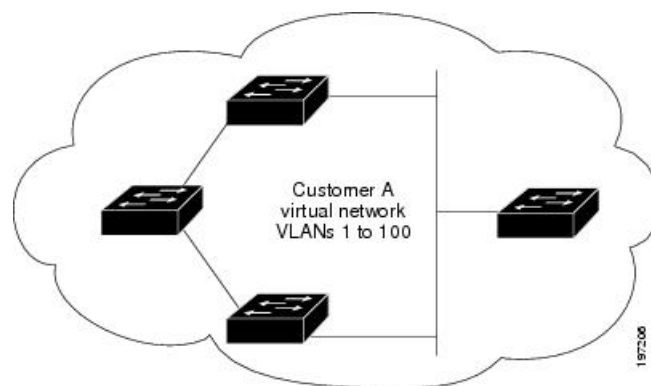
図 4: レイヤ 2 プロトコル トンネリング



前の例では、カスタマー X、サイト 1 のスイッチ上の VLAN で動作する STP は、カスタマー X、サイト 2 のスイッチに基づくコンバージェンスパラメータを考慮せずに、このサイトのスイッチのスパニングツリーを構築します。

以下の図は、BPDU トンネリングがイネーブルになっていない場合の、カスタマーのネットワークでの結果トポロジを示します。

図 5: BPDU トンネリングを使用しない仮想ネットワーク トポロジ



## 複数プロバイダー VLAN を使用した選択的 Q-in-Q

複数プロバイダー VLAN を使用する選択的 Q-in-Q は、ポート上のユーザ固有の範囲のカスタマー VLAN を 1 つの特定のプロバイダー VLAN に関連付けることができるトンネリング機能であり、ポート上で複数のカスタマー VLAN をプロバイダー VLAN にマッピングできます。ポートに設定されたカスタマー VLAN のいずれかに一致する VLAN タグが付いたパケットは、

サービス プロバイダー VLAN のプロパティを使用して VLAN ファブリック全体でトンネリングされます。カプセル化パケットは、内部パケットのレイヤ 2 ヘッダーの一部としてカスタマー VLAN タグを伝送します。

## 注意事項と制約事項

Q-in-Q トンネリングおよびレイヤ 2 トンネリングには、次の設定に関するガイドラインと制約事項があります。

- Q-in-Q は、サービス プロバイダーのエッジデバイスのカスタマー側インターフェイスで設定する必要があります。イーサネットフレームが Cisco Nexus 9000 シリーズ スイッチに入力されると、スイッチは 1 つの転送決定内で 2 つの 802.1Q ヘッダーを持つフレームをカプセル化できません。同様に、Q-in-Q カプセル化イーサネット フレームが 802.1Q ヘッダーのない Cisco Nexus 9000 シリーズ スイッチを出力する必要がある場合、スイッチは単一の転送決定内でイーサネット フレームから 2 つの 802.1Q ヘッダーをカプセル化解除できません。
- 複数の VLAN のマッピングがサポートされています。
- マルチタグ付き BPDU は、Cisco Nexus 93108TC-EX および 93180YC-EX スイッチでサポートされています。最大 3 つのタグをサポートしています。
- マルチタグ付きの BPDU では選択的 Q-in-Q トンネリングはサポートされません。
- マルチタグ付き CDP および STP BPDU のみがサポートされます。
- 最も内側のタグは常に 0x8100 である必要があります。
- 複数の選択的 Q-in-Q タグはサポートされていません。つまり、Q-in-Q は単一のインターフェイスで複数の SP タグをサポートしません。
- サービスプロバイダー ネットワーク内のスイッチは、Q-in-Q タギングによる MTU サイズの増加に対応するように設定する必要があります。
- Q-in-Q タグ付きパケットの MAC アドレス ラーニングは、外部 VLAN (サービス プロバイダー VLAN) タグに基づいています。単一の MAC アドレスが複数の内部 (カスタマー) VLAN で使用される配置においては、パケット転送の問題が発生する場合があります。
- レイヤ 3 以上のパラメータは、トンネルトラフィックでは識別できません (レイヤ 3 宛先や送信元アドレスなど)。トンネル型トラフィックはルーティングできません。
- **system dot1q-tunnel transit** コマンドを使用する場合、次の警告が適用されます。
  - **system dot1q-tunnel transit vlan provider\_vlan\_list** コマンドを設定して、モジュラーデバイスで Q in Q または選択的 Q in Q コンフィギュレーションを設定することが推奨されています。
  - トランク ポートを出力するレイヤ 2 フレームは常に、ポートでネイティブ VLAN を装備している場合でも、タグ付けされます。

- すべてのトンネルメカニズム（たとえば、Q in Q、VXLAN、MPLS）は、**system dot1q-tunnel transit** が設定されている場合は正しく機能せず、相互運用できません。
- Cisco Nexus 9000 シリーズのデバイスは、トンネルトラフィックに対する MAC レイヤ ACL/QoS（VLAN ID および送信元/宛先 MAC アドレス）のみを提供できます。
- MAC アドレスに基づくフレーム配布を使用する必要があります。
- 非対称リンクでは 1 つのポートだけがトラッキングするため、Dynamic Trunking Protocol（DTP）をサポートしません。無条件でトランクになるように、非対称リンクの 802.1Q トランクポートを設定する必要があります。
- プライベート VLAN をサポートするように設定されたポートに 802.1Q トンネリング機能を設定することはできません。プライベート VLAN は、これらの導入には必要ではありません。
- トンネル VLAN の IGMP スヌーピングをディセーブルにする必要があります。
- ネイティブ VLAN でのタグgingを維持し、タグなしトラフィックを廃棄するには、`vlan dot1q tag native` コマンドを入力する必要があります。このコマンドにより、ネイティブ VLAN の設定ミスを防止できます。
- 802.1Q インターフェイスをエッジポートにするように手動で設定する必要があります。
- IGMP スヌーピングは内部 VLAN ではサポートされません。
- Q-in-Q は、Cisco Nexus 9332PQ、9372PX、9372TX、および 93120TX スイッチのアップリンクポートと、N9K-M6PQ または N9K-M12PQ の汎用拡張モジュール（GEM）を搭載した Cisco Nexus 9396PX、9396TX、および 93128TX スイッチではサポートされていません。
- Q-in-Q トンネルは、Cisco Nexus 9300 および 9500 シリーズ デバイスのアプリケーションリーフエンジン（ALE）アップリンクポートに関する制約事項の影響を受ける可能性があります（「[ALE アップリンクポートに関する制約事項](#)」）。
- Q-in-Q トンネリングは、Application Spine Engine 2（ASE2）および Application Spine Engine 3（ASE3）ベースの Cisco Nexus スイッチではサポートされていません。
- Link Aggregation Control Protocol（LACP）での Layer 2 プロトコル トンネリングはサポートされません。
- Q-in-Q タグgingはサポートされていません。
- Layer 2 プロトコル トンネリングは、N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX ラインカードを搭載した Cisco Nexus 9500 シリーズ スイッチではサポートされません。
- N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX ラインカードを搭載した Cisco Nexus 9500 シリーズ スイッチでは、Q-in-Q はポートまたはポートチャネルのレイヤ 2 アクセス VLAN エッジデバイスでのみサポートされます。
- FEX 設定は Q-in-Q ポートではサポートされません。



- コマンド `l2potocol tunnel stp` がトンネルインターフェイスで設定されている場合、サービスプロバイダーで設定する VLAN はカスタマーネットワークの VLAN とは異なる必要があります。

## 複数プロバイダー VLAN を使用した選択的 Q-in-Q の注意事項と制約事項

- 複数のプロバイダー VLAN を使用する選択的 Q-in-Q には、選択的 Q-in-Q に関する既存の制限事項とガイドラインがすべて適用されます。
- Cisco NX-OS リリース 9.3(5) 以降、複数プロバイダー VLAN を使用した選択的 Q-in-Q 機能は、Cisco Nexus N9K-C9316D-GX、N9K-C93600CD-GX、N9K-C9364C-GX スイッチでサポートされます。
- 複数プロバイダー VLAN を使用した選択的 Q-in-Q 機能は、Nexus 9300-EX、9300-FX、および 9300-FX2 プラットフォームでサポートされます。
- vPC ポート チャンネルで複数のプロバイダー VLAN をイネーブルにする場合は、vPC ピア間で設定が一貫している必要があります。
- vPC セットアップで複数のプロバイダー VLAN 機能を使用して選択的 Q-in-Q を実行する場合は、「`system dot1q tunnel tunnel`」を有効にすることを推奨します。
- 通常のトランクではプロバイダー VLAN を許可しないことを推奨します。
- 複数のプロバイダー VLAN インターフェイスの VLAN リストを許可しているトランク インターフェイスで、ネイティブ VLAN およびプロバイダー VLAN のみを許可します。
- ポートから VLAN へのマッピング（例：`switchport vlan mapping 10 20`）は、複数のプロバイダー VLAN で選択的 Q-in-Q 用に設定されたポートではサポートされません。
- プライベート VLAN は、複数のプロバイダー VLAN で選択的 Q-in-Q 用に設定されたポートではサポートされません。
- レイヤ 2 スイッチングのみがサポートされます。
- プロバイダー VLAN でのルーティングはサポートされていません。
- FEX は、複数のプロバイダー VLAN を使用する選択的 Q-in-Q ではサポートされません。
- 複数プロバイダー VLAN を使用した選択的 Q-in-Q
- VLAN1 が複数のプロバイダー タグを使用して選択的 Q-in-VNI を使用してネイティブ VLAN として設定されている場合、ネイティブ VLAN 上のトラフィックはドロップされます。ポートが選択的 Q-in-Q で設定されている場合は、VLAN1 をネイティブ VLAN として設定しないでください。VLAN1 がカスタマー VLAN として設定されている場合、VLAN1 のトラフィックはドロップされます。

### 複合アクセス ポート機能セットに関する注意事項と制限事項

- Cisco NX-OS リリース 9.3(3) 以降では、Cisco Nexus C9348GC-FXPスイッチで複合アクセス ポート機能セットがサポートされています。
- 複合アクセス ポート機能セットは、次の機能で構成されます。
  - プライベート VLAN（セカンダリ隔離あり）
  - 選択的 Q-in-Q
  - ポートセキュリティ
- PVLANおよび選択的Q-in-Qに関するすべてのガイドラインと制限は、複合アクセス ポート機能セットにも適用されます。
- ポートモードの **private-vlan trunk secondary** は、複合アクセス ポート機能セットでサポートされます。
- vPC ポート チャンネルで複合アクセス ポート機能セットを有効にする場合は、設定が vPC ピア全体で一貫していることを確認する必要があります。
- 複合アクセス ポート機能セットを実行する場合は、**system dot1q-tunnel transit** と入力することを推奨します。
- ポート VLAN マッピング（例：**switchport vlan mapping 10 20**）はサポートされていません。
- 選択的 Q-in-Q ではレイヤ 2 スイッチングのみがサポートされます。
- 複合アクセス ポート機能のネイティブ VLAN では、ルーティングのみがサポートされます。

## Q-in-Q トンネルおよびレイヤ 2 プロトコルのトンネリングの設定

### 802.1Q トンネル ポートの作成

dot1qトンネルポートを作成するには、コマンドを使用します。**switchport mode**



(注) コマンドを使用して、802.1Qトンネルポートをエッジポートに設定する必要があります。**spanning-tree port type edge** ポートの VLAN メンバーシップは、**switchport access vlan vlan-id** を使用して変更します。

dot1q-tunnel ポートに割り当てられたアクセス VLAN の IGMP スヌーピングをディセーブルにして、マルチキャスト パケットが Q-in-Q トンネルを通過できるようにする必要があります。

次の CLI は、LSE、EX、FX、FX2 ベースの Cisco Nexus 9000 シリーズ スイッチでのみ必須です。Q-in-Q カプセル化またはカプセル化解除の要件を持たない SP クラウド内の純粋な中継ボックス上で、すべての VLAN タグのシームレスなパケット転送と保存を行うには、ネットワーク全体 CLI コマンド **system dot1q-tunnel transit** を設定します。CLI を削除するには次のコマンドを設定します。 **no system dot1q-tunnel transit**

**system dot1q-tunnel transit** コマンドを使用する場合、次の警告が適用されます。

- **system dot1q-tunnel transit vlan provider\_vlan\_list** コマンドを設定して、モジュラー デバイスで Q in Q または選択的 Q in Q コンフィギュレーションを設定することが推奨されています。
- トランク ポートを出力する L2 フレームは常に、ポートでネイティブ VLAN を装備している場合でも、タグ付けされます。
- すべてのトンネルメカニズム（たとえば、Q in Q、VXLAN、MPLS）は、**system dot1q-tunnel transit** が設定されている場合は正しく機能せず、相互運用できません。

### 始める前に

はじめに、スイッチ ポートとしてインターフェイスを設定する必要があります。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet slot/port**
3. switch(config-if)# **switchport**
4. switch(config-if)# **switchport mode dot1q-tunnel**
5. (任意) switch(config-if)# **no switchport mode dot1q-tunnel**
6. switch(config-if)# **exit**
7. (任意) switch(config)# **show dot1q-tunnel [interface if-range]**
8. (任意) switch(config)# **no shutdown**
9. (任意) switch(config)# **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>interface ethernet slot/port</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# <b>switchport</b>	インターフェイスをレイヤ 2 スイッチング ポートとして設定します。
ステップ 4	switch(config-if)# <b>switchport mode dot1q-tunnel</b>	ポートに 802.1Q トンネルを作成します。インターフェイス モードを変更すると、ポートはダウンし、

	コマンドまたはアクション	目的
		再初期化（ポートフラップ）されます。トンネルインターフェイスでは BPDU フィルタリングがイネーブルになり、CDP がディセーブルになります。
ステップ 5	(任意) switch(config-if)# <b>no switchport mode dot1q-tunnel</b>	ポートで 802.1Q トンネルをディセーブルにします。
ステップ 6	switch(config-if)# <b>exit</b>	コンフィグレーション モードを終了します。
ステップ 7	(任意) switch(config)# <b>show dot1q-tunnel [interface if-range]</b>	dot1q-tunnel モードにあるすべてのポートを表示します。必要に応じて、表示するインターフェイスまたはインターフェイスの範囲を指定できます。
ステップ 8	(任意) switch(config)# <b>no shutdown</b>	ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続き、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 9	(任意) switch(config)# <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

### 例

次に、802.1Q トンネル ポートを作成する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# exit
switch(config)# exit
switch# show dot1q-tunnel
```

## 802.1Q トンネル ポートでの選択的 Q-in-Q の VLAN マッピングの設定

802.1Q トンネル ポートで選択的 Q-in-Q の VLAN マッピングを設定するには、次の手順を実行します。



(注) 同じインターフェイスでは、1対1のマッピングと選択的 Q-in-Q を設定できません。

## 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface interface-id**
3. switch(config-if)# **switchport mode dot1q-tunnel**
4. switch(config-if)# **switchport vlan mapping vlan-id-range dot1q-tunnel outer vlan-id**
5. switch(config-if)# **exit**
6. switch# **show interfaces interface-id vlan mapping**
7. switch# **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>interface interface-id</b>	サービス プロバイダ ネットワークに接続されるインターフェイスのインターフェイス コンフィギュレーションモードを開始します。物理インターフェイスまたは EtherChannel ポートチャネルを入力できます。
ステップ 3	switch(config-if)# <b>switchport mode dot1q-tunnel</b>	トンネルポートとしてインターフェイスを設定します。
ステップ 4	switch(config-if)# <b>switchport vlan mapping vlan-id-range dot1q-tunnel outer vlan-id</b>	マッピングする VLAN ID を入力します。 <ul style="list-style-type: none"> <li>• <b>vlan-id-range1</b> : カスタマー ネットワークからスイッチに入るカスタマー VLAN ID (C-VLAN) の範囲。指定できる範囲は 1 ~ 4094 です。VLAN-ID のストリングを入力できます。</li> <li>• <b>outer vlan-id</b> : サービスプロバイダー ネットワークの外部 VLAN ID (S-VLAN) を入力します。指定できる範囲は 1 ~ 4094 です。</li> </ul>
ステップ 5	switch(config-if)# <b>exit</b>	コンフィギュレーション モードを終了します。
ステップ 6	switch# <b>show interfaces interface-id vlan mapping</b>	設定を確認します。
ステップ 7	switch# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

VLAN マッピング設定を削除するには、**no switchport vlan mapping vlan-id-range dot1q-tunnel outer vlan-id** コマンドを使用します。

次の例では、ポートに選択した QinQ マッピングを設定して、C-VLANID が 1～5 のトラフィックが、S-VLAN ID が 100 であるスイッチに入るようにする方法を示します。その他の VLAN ID のトラフィックはドロップされます。

#### 例

```
switch(config)# interface gigabitethernet0/1
switch(config-if)# switchport vlan mapping 1-5 dot1q-tunnel 100

Switch(config-if)# exit
```

## 複数プロバイダー VLAN で選択的 Q-in-Q を設定する

#### 始める前に

プロバイダー VLAN を設定する必要があります。

#### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface interface-id**
3. switch(config-if)# **switchport**
4. switch(config-if)# **switchport mode trunk**
5. switch(config-if)# **switchport trunk native vlan vlan-id**
6. switch(config-if)# **switchport vlan mapping vlan-id-range dot1q-tunnel outer vlan-id**
7. switch(config-if)# **switchport trunk allowed vlan vlan\_list**
8. switch(config-if)# **exit**
9. switch(config-if)# **show interfaces interface-id vlan mapping**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>interface interface-id</b>	サービス プロバイダ ネットワークに接続されるインターフェイスのインターフェイス コンフィギュレーションモードを開始します。物理インターフェイスまたは EtherChannel ポートチャネルを入力できます。
ステップ 3	switch(config-if)# <b>switchport</b>	インターフェイスをレイヤ2スイッチングポートとして設定します。
ステップ 4	switch(config-if)# <b>switchport mode trunk</b>	インターフェイスをレイヤ2 トランク ポートとして設定します。

	コマンドまたはアクション	目的
ステップ 5	switch(config-if)# <b>switchport trunk native vlan</b> <i>vlan-id</i>	802.1Q トランクのネイティブ VLAN を設定します。有効な値は 1 ~ 4094 です。デフォルト値は VLAN 1 です。
ステップ 6	switch(config-if)# <b>switchport vlan mapping</b> <i>vlan-id-range</i> <b>dot1q-tunnel</b> <i>outer vlan-id</i>	マッピングする VLAN ID を入力します。  <ul style="list-style-type: none"> <li>• <b>vlan-id-range</b> : カスタマーネットワークからスイッチに入るカスタマー VLAN ID (C-VLAN) の範囲。指定できる範囲は 1 ~ 4094 です。VLAN-ID のストリングを入力できます。</li> <li>• <b>outer vlan-id</b> : サービスプロバイダーネットワークの外部 VLAN ID (S-VLAN) を入力します。指定できる範囲は 1 ~ 4094 です。</li> </ul>
ステップ 7	switch(config-if)# <b>switchport trunk allowed vlan</b> <i>vlan_list</i>	トランク インターフェイスの許可 VLAN を設定します。
ステップ 8	switch(config-if)# <b>exit</b>	コンフィギュレーション モードを終了します。
ステップ 9	switch(config-if)# <b>show interfaces</b> <i>interface-id</i> <b>vlan mapping</b>	マッピングの設定の確認

次の例では、複数のプロバイダー VLAN で選択的 Q-in-Q を設定する方法を示します。

#### 例

```
switch# sh run int e1/1

interface Ethernet1/1
  switchport
  switchport mode trunk
  switchport trunk native vlan 2
  switchport vlan mapping 3-400 dot1q-tunnel 400
  switchport vlan mapping 401-800 dot1q-tunnel 401
  switchport vlan mapping 801-1200 dot1q-tunnel 10
  switchport vlan mapping 1201-1600 dot1q-tunnel 1400
  switchport vlan mapping 1601-2000 dot1q-tunnel 9
  switchport vlan mapping 2001-2400 dot1q-tunnel 3000
  switchport vlan mapping 2401-2800 dot1q-tunnel 2099
  switchport vlan mapping 2801-3200 dot1q-tunnel 2800
  switchport vlan mapping 3201-3600 dot1q-tunnel 3967
  switchport vlan mapping 3601-4000 dot1q-tunnel 600
  switchport trunk allowed vlan 2,9-10,400-401,600,1400,2099,2800,3000,3967

switch# show interface e1/1 vlan mapping
Interface Eth1/1:
Original VLAN                Translated VLAN
-----
3                            400
4                            400
5                            400
6                            400
```

```

7                               400
8                               400
9                               400
10                              400
11                              400
12                              400
13                              400
14                              400
15                              400
16                              400
17                              400
18                              400
19                              400
20                              400

```

```

switch# show consistency-checker selective-qinq interface e1/1
Fetching ingressVlanXlate entries from slice:0 HW
Fetching ingressVlanXlate entries from slice:1 HW
Performing port specific checks for intf Eth1/1
Port specific selective QinQ checks for interface   Eth1/1 : PASS

```

```
Switch#
```

## Q-in-Q 用の EtherType の変更

スイッチは、802.1Q および Q-in-Q カプセル化に 0x8100 のデフォルトの EtherType を使用します。EtherType は、スイッチポート インターフェイスで 0x9100、0x9200、および 0x88a8 に設定できません。

## レイヤ 2 プロトコル トンネルのイネーブル化

802.1Q トンネル ポートでプロトコルのトンネリングをイネーブルにできます。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet slot/port**
3. switch(config-if)# **switchport**
4. switch(config-if)# **switchport mode dot1q-tunnel**
5. switch(config-if)# **l2protocol tunnel [cdp | stp | lacp | lldp | vtp]**
6. (任意) switch(config-if)# **no l2protocol tunnel [cdp | stp | lacp | lldp | vtp]**
7. switch(config-if)# **exit**
8. (任意) switch(config)# **no shutdown**
9. (任意) switch(config)# **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。



	コマンドまたはアクション	目的
ステップ 2	switch(config)# <b>interface ethernet slot/port</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 3	switch(config-if)# <b>switchport</b>	インターフェイスをレイヤ2 スイッチングポートとして設定します。
ステップ 4	switch(config-if)# <b>switchport mode dot1q-tunnel</b>	ポートに 802.1Q トンネルを作成します。インターフェイスモードを変更すると、ポートはダウンし、再初期化（ポートフラップ）されます。トンネルインターフェイスでは BPDU フィルタリングがイネーブルになり、CDP がディセーブルになります。
ステップ 5	switch(config-if)# <b>l2protocol tunnel [cdp   stp   lacp   lldp   vtp]</b>	レイヤ2 プロトコルのトンネリングをイネーブルにします。必要に応じて、CDP、STP、LACP、LLDP または VTP トンネリングを有効にできます。
ステップ 6	(任意) switch(config-if)# <b>no l2protocol tunnel [cdp   stp   lacp   lldp   vtp]</b>	プロトコルのトンネリングをディセーブルにします。  (注) LACP および LLDP のレイヤ2 プロトコル トンネルは、Cisco Nexus N9K-X9732C-EXM モジュールでのみサポートされます。
ステップ 7	switch(config-if)# <b>exit</b>	コンフィギュレーションモードを終了します。
ステップ 8	(任意) switch(config)# <b>no shutdown</b>	ポリシーがハードウェアポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが継続でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 9	(任意) switch(config)# <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

### 例

次に、802.1Q トンネルポートでプロトコルのトンネリングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# l2protocol tunnel stp
switch(config-if)# exit
switch(config)# exit
```

## L2 プロトコル トンネル ポートに対するグローバル CoS の設定

トンネル ポートの入力 BPDU が指定されたクラスでカプセル化されるように、サービス クラス (CoS) の値をグローバルに指定できます。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **l2protocol tunnel cos value**
3. (任意) switch(config)# **no l2protocol tunnel cos**
4. switch(config)# **exit**
5. (任意) switch# **no shutdown**
6. (任意) switch# **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>l2protocol tunnel cos value</b>	すべてのレイヤ2 プロトコルのトンネリング ポートでグローバル CoS 値を指定します。デフォルト CoS 値は 5 です。
ステップ 3	(任意) switch(config)# <b>no l2protocol tunnel cos</b>	グローバル CoS 値をデフォルト値に設定します。
ステップ 4	switch(config)# <b>exit</b>	コンフィギュレーション モードを終了します。
ステップ 5	(任意) switch# <b>no shutdown</b>	ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシープログラミングが続き、ポートがアップできます。ポリシーが対応していない場合は、エラーは error-disabled ポリシー状態になります。
ステップ 6	(任意) switch# <b>copy running-config startup-config</b>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

### 例

次に、レイヤ2 プロトコルのトンネリングのためのグローバル CoS 値を指定する例を示します。

```
switch# configure terminal
switch(config)# l2protocol tunnel cos 6
switch(config)# exit
```

## レイヤ2 プロトコル トンネル ポートのしきい値の設定

レイヤ2 プロトコルのトンネリング ポートに対するポート ドロップおよびシャットダウン値を指定できます。

### 手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet slot/port**
3. switch(config-if)# **switchport**
4. switch(config-if)# **switchport mode dot1q-tunnel**
5. switch(config-if)# **l2protocol tunnel drop-threshold [cdp | stp | vtp] packets-per-sec**
6. (任意) switch(config-if)# **no l2protocol tunnel drop-threshold [cdp | stp | vtp]**
7. switch(config-if)# **l2protocol tunnel shutdown-threshold [cdp | stp | vtp] packets-per-sec**
8. (任意) switch(config-if)# **no l2protocol tunnel shutdown-threshold [cdp | stp | vtp]**
9. switch(config-if)# **exit**
10. (任意) switch(config)# **no shutdown**
11. (任意) switch(config)# **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# <b>interface ethernet slot/port</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# <b>switchport</b>	インターフェイスをレイヤ2 スイッチング ポートとして設定します。
ステップ 4	switch(config-if)# <b>switchport mode dot1q-tunnel</b>	ポートに 802.1Q トンネルを作成します。
ステップ 5	switch(config-if)# <b>l2protocol tunnel drop-threshold [cdp   stp   vtp] packets-per-sec</b>	廃棄される前にインターフェイスで処理できる最大パケット数を指定します。必要に応じて、CDP、STP、または VTP を指定できます。パケットの有効な値は 1 ~ 4096 です。
ステップ 6	(任意) switch(config-if)# <b>no l2protocol tunnel drop-threshold [cdp   stp   vtp]</b>	しきい値を 0 にリセットし、ドロップしきい値をディセーブルにします。
ステップ 7	switch(config-if)# <b>l2protocol tunnel shutdown-threshold [cdp   stp   vtp] packets-per-sec</b>	インターフェイスで処理できる最大パケット数を指定します。パケット数が超過すると、ポートは error-disabled ステートになります。必要に応じて、CDP、STP、または VTP を指定できます。パケットの有効な値は 1 ~ 4096 です。

	コマンドまたはアクション	目的
ステップ 8	(任意) <code>switch(config-if)# no l2protocol tunnel shutdown-threshold [cdp   stp   vtp]</code>	しきい値を0にリセットし、シャットダウンしきい値をディセーブルにします。
ステップ 9	<code>switch(config-if)# exit</code>	コンフィグレーションモードを終了します。
ステップ 10	(任意) <code>switch(config)# no shutdown</code>	ポリシーがハードウェア ポリシーと一致するインターフェイスおよび VLAN のエラーをクリアします。このコマンドにより、ポリシー プログラミングが続行でき、ポートがアップできます。ポリシーが対応していない場合は、エラーは <code>error-disabled</code> ポリシー状態になります。
ステップ 11	(任意) <code>switch(config)# copy running-config startup-config</code>	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

## 複合アクセス ポート機能セットの設定

混合アクセス ポートを設定するには、次の手順を実行します。

### 手順の概要

1. `interface interface [port | port-channel | vPC]`
2. `switchport mode private-vlan trunk secondary`
3. `switchport private-vlan trunk native vlan vlan_id`
4. `switchport private-vlan trunk allowed vlan vlan list`
5. `switchport private-vlan association trunk primary_vlan_ID secondary_vlan_ID`
6. `switchport vlan mapping [vlan-id-range | all] dot1q-tunnel outer vlan-id`
7. `storm-control broadcast level [high level] [ lower level ]`
8. `storm-control multicast level [high level] [ lower level ]`
9. `storm-control action [shutdown | trap ]`
10. `load-interval counter {1 | 2 | 3 }`
11. `switchport port-security maximum [max-addr ]`
12. `switchport port-security action [restrict | shutdown | protect]`
13. `switchport port-security`
14. `service-policy {input | type {qos input | queuing {input | output}} } policy-map-name`

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>interface interface [port   port-channel   vPC]</code> 例： <code>switch# interface port-channel 202</code>	指定されたポート チャネルをインターフェイス コンフィギュレーションモードにします。範囲は 1 ~ 4096 です。

	コマンドまたはアクション	目的
ステップ 2	<b>switchport mode private-vlan trunk secondary</b> 例： switch(config)# <b>switchport mode private-vlan trunk secondary</b>	プライベート VLAN のセカンダリ トランク ポートとしてポートを設定します。
ステップ 3	<b>switchport private-vlan trunk native vlan vlan_id</b> 例： switch(config)# <b>switchport private-vlan trunk native vlan 4002</b>	PVLAN トランク ポートに割り当てるネイティブ VLAN を設定します。
ステップ 4	<b>switchport private-vlan trunk allowed vlan vlan list</b> 例： switch(config)# <b>switchport private-vlan trunk allowed vlan 1002,4002</b>	PVLAN トランク ポートで許容される通常の VLAN のリストを設定します。
ステップ 5	<b>switchport private-vlan association trunk primary_vlan_ID secondary_vlan_ID</b> 例： switch(config)# <b>switchport private-vlan association trunk 4050 4049</b>	PVLAN トランク ポートでプライマリ VLAN およびセカンダリ VLAN 間の関連付けを設定します。
ステップ 6	<b>switchport vlan mapping [vlan-id-range   all] dot1q-tunnel outer_vlan-id</b> 例： switch(config-if)# <b>switchport vlan mapping all dot1q-tunnel 1002</b>	すべての 4K VLAN を含むカスタマー範囲 VLAN またはキーワード all を入力します。
ステップ 7	<b>storm-control broadcast level [high level] [ lower level ]</b> 例： switch(config-if)# <b>storm-control broadcast level 1.00</b>	ブロードキャスト ストーム制御を設定します。ブロードキャスト トラフィックの上限しきい値レベルを指定します。
ステップ 8	<b>storm-control multicast level [high level] [ lower level ]</b> 例： switch(config-if)# <b>storm-control multicast level 1.00</b>	インターフェイス上のマルチキャスト トラフィック ストーム制御をイネーブルにし、トラフィック ストーム制御レベルを設定し、そのトラフィック ストーム制御レベルを、インターフェイス上でイネーブルにされているすべてのトラフィック ストーム制御モードに適用します。
ステップ 9	<b>storm-control action [shutdown   trap ]</b> 例： switch(config-if)# <b>storm-control action shutdown</b>	トラフィック ストームの発生時にトラップを生成するか、ポートをエラー無効にするようにトラフィック ストーム制御を設定します。

	コマンドまたはアクション	目的
ステップ 10	<b>load-interval counter</b> {1   2   3 } 例： switch(config-if)# <b>load-interval counter</b> 1 5	インターフェイスで統計情報をサンプリングする間隔を指定します。
ステップ 11	<b>switchport port-security maximum</b> [max-addr ] 例： switch(config-if)# <b>switchport port-security maximum</b> 3	ポートでセキュアMACアドレスの最大数を設定します。
ステップ 12	<b>switchport port-security action</b> [restrict   shutdown   protect] 例： switch(config-if)# <b>switchport port-security violation restrict</b>	インターフェイスのセキュリティ違反モードを制限します。
ステップ 13	<b>switchport port-security</b> 例： switch(config-if)# <b>switchport port-security</b>	ポートセキュリティのコンフィギュレーション情報を表示します。
ステップ 14	<b>service-policy</b> {input   type {qos input   queuing {input   output}} } <i>policy-map-name</i> 例： switch(config-if)# <b>service-policy type qos input</b> ovh_qos	ポリシーマップをインターフェイスに付加します。

## Q-in-Q 設定の確認

コマンド	目的
<b>clear l2protocol tunnel counters</b> [interface <i>if-range</i> ]	すべての統計情報カウンタをクリアします。インターフェイスが指定されていない場合、すべてのインターフェイスのレイヤ2プロトコルトンネル統計情報がクリアされます。
<b>show dot1q-tunnel</b> [interface <i>if-range</i> ]	dot1q トンネルモードのインターフェイス範囲またはすべてのインターフェイスが表示されます。
<b>show l2protocol tunnel</b> [interface <i>if-range</i>   <b>vlan</b> <i>vlan-id</i> ]	一定範囲のインターフェイス（特定の VLAN の一部であるすべての dot1q-tunnel インターフェイスまたはすべてのインターフェイス）のレイヤ2プロトコルトンネル情報を表示します。

コマンド	目的
<code>show l2protocol tunnel summary</code>	レイヤ2 プロトコル トンネルが設定されているすべてのポートのサマリーを表示します。
<code>show running-config l2pt</code>	現在のレイヤ2 プロトコル トンネルの実行コンフィギュレーションを表示します。

## Q-in-Q およびレイヤ2 プロトコルのトンネリングの設定例

次に、イーサネット 7/1 に着信するトラフィックに対し Q-in-Q を処理するよう設定されているサービス プロバイダーのスイッチを示します。レイヤ2 プロトコル トンネルが STP BPDU に対してイネーブルにされます。このカスタマーは VLAN 10（外部 VLAN タグ）に割り当てられます。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vlan 10
switch(config-vlan)# no shutdown
switch(config-vlan)# no ip igmp snooping
switch(config-vlan)# exit
switch(config)# interface ethernet 7/1
switch(config-if)# switchport
switch(config-if)# switchport mode dot1q-tunnel
switch(config-if)# switchport access vlan 10
switch(config-if)# spanning-tree port type edge
switch(config-if)# l2protocol tunnel stp
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# exit
switch#
```

