



# CHAPTER 17

## IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングの設定

Virtual Private Network (VPN; バーチャル プライベート ネットワーク) では、多くの場合にイーサネットベースの共有インフラストラクチャである企業規模の接続に、プライベート ネットワークと同じセキュリティ、プライオリティ、信頼性、管理の容易さが提供されます。トンネリングは、サービスプロバイダーのネットワークを越えて複数のカスタマーのトラフィックを運び、その他のカスタマーのトラフィックに影響を与えずに、それぞれのカスタマーの VLAN およびレイヤ 2 プロトコルの設定を維持する必要があるサービス プロバイダー用に設計された機能です。Catalyst 3560 スイッチでは、IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングがサポートされています。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

この章で説明する内容は、次のとおりです。

- 「IEEE 802.1Q トンネリングの概要」 (P.17-1)
- 「IEEE 802.1Q トンネリングの設定」 (P.17-3)
- 「レイヤ 2 プロトコル トンネリングの概要」 (P.17-7)
- 「レイヤ 2 プロトコル トンネリングの設定」 (P.17-10)
- 「トンネリング ステータスのモニタおよびメンテナンス」 (P.17-18)

## IEEE 802.1Q トンネリングの概要

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 プロバイダー 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在することがあります。それぞれのカスタマーに VLAN ID の固有の範囲を割り当てると、カスタマーの設定が制限され、IEEE 802.1Q 仕様の VLAN 制限 (4096) を簡単に越えてしまうことがあります。

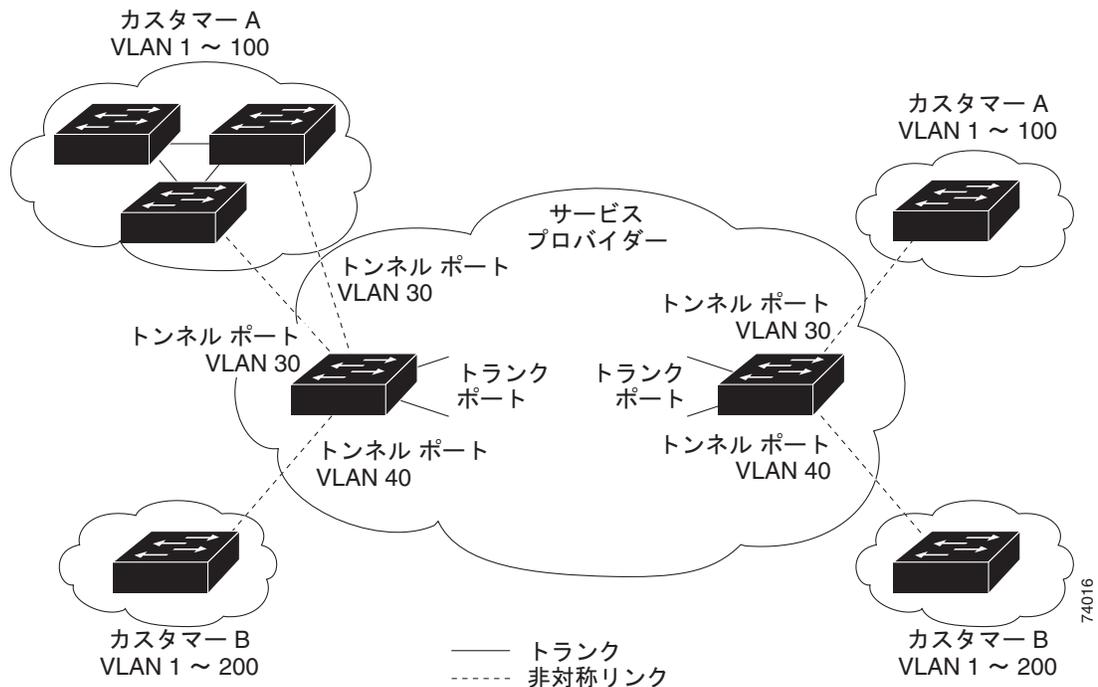
サービス プロバイダーは、IEEE 802.1Q トンネリング機能を使用すると、単一の VLAN を使用して、複数の VLAN を含むカスタマーをサポートできます。カスタマーの VLAN ID は、同一 VLAN に見えても保護され、さまざまなカスタマーのトラフィックは、サービス プロバイダー ネットワーク内で区別されます。IEEE 802.1Q トンネリングを使用すると、VLAN 内の VLAN 階層を使用してタグ付きパケットにタグを再び付けることで、VLAN 容量が拡大します。IEEE 802.1Q トンネリングをサポートするように設定したポートは、トンネル ポートと呼ばれます。トンネリングを設定する

場合は、トンネリング専用の VLAN ID にトンネル ポートを割り当てます。それぞれの顧客には個別のサービス プロバイダー VLAN ID が必要ですが、その VLAN ID ではすべての顧客の VLAN がサポートされます。

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 IEEE 802.1Q トランク ポートからサービス プロバイダー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間のリンクは、片方が IEEE 802.1Q トランク ポートとして設定され、もう一方がトンネル ポートとして設定されているので非対称です。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。

図 17-1 を参照してください。

図 17-1 サービス プロバイダー ネットワークの IEEE 802.1Q トンネル ポート



顧客のトランク ポートからサービス プロバイダーのエッジスイッチのトンネル ポートに発信されるパケットには、通常、適切な VLAN ID とともに IEEE 802.1Q タグが付いています。タグ付きパケットはスイッチ内でそのまま残り、トランク ポートからサービス プロバイダー ネットワークに発信されると、顧客に固有の VLAN ID を含む IEEE 802.1Q タグの別のレイヤ（メトロ タグと呼ばれる）でカプセル化されます。顧客の元の IEEE 802.1Q タグは、カプセル化されたパケット内で保護されます。このため、サービス プロバイダー ネットワークに入るパケットには、顧客のアクセス VLAN ID を含む外部（メトロ）タグ、および着信トラフィックのものである内部 VLAN ID という、二重のタグが付いています。

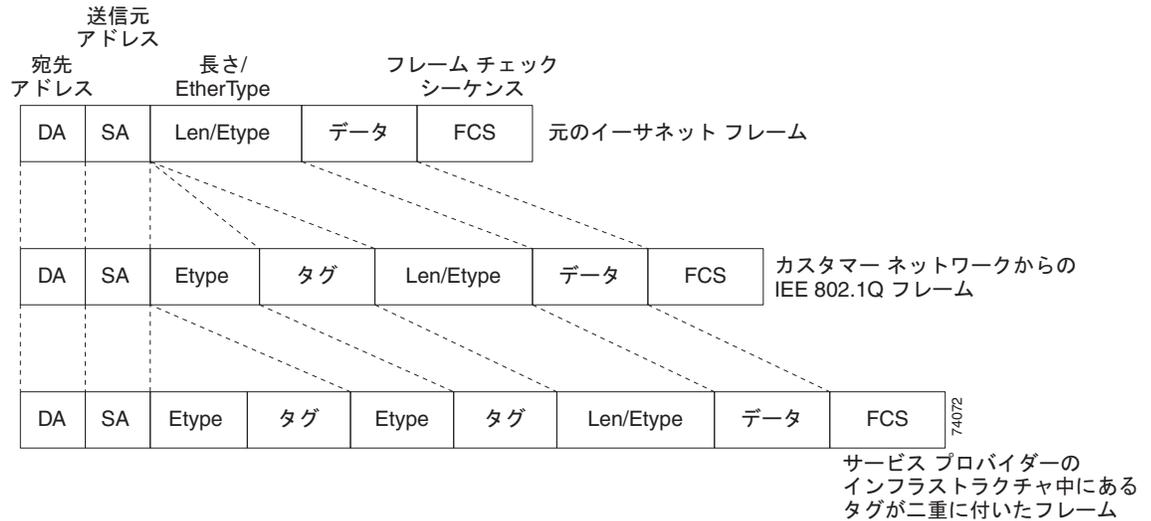
二重タグ パケットがサービス プロバイダー コア スイッチの別のトランク ポートに入ると、スイッチがパケットを処理する間に外部タグが外されます。パケットが、そのコア スイッチの別のトランク ポートを出るとき、同じメトロ タグがパケットに再び追加されます。図 17-2 に、二重タグ パケットのタグ構造を示します。



(注)

カプセル化された着信パケットによってそのトランク ポートが `errdisable` に変更されたため、トランク ポートからレイヤ 2 プロトコル設定を削除します。カプセル化された発信 VTP (CDP および STP) パケットが、そのトランクから廃棄されます。

図 17-2 元の（通常）イーサネット パケット、IEEE 802.1Q イーサネット パケット、二重タグ イーサネット パケットの形式



パケットがサービス プロバイダー出力スイッチのトランク ポートに入ると、スイッチがパケットを内部処理する間に外部タグは再び外されます。しかし、パケットがエッジスイッチのトンネルポートからカスタマー ネットワークに送信される時、メトロ タグは追加されません。パケットは通常の IEEE 802.1Q タグ フレームとして送信され、カスタマー ネットワーク内で元の VLAN 番号は保護されます。

図 17-1 では、カスタマー A に VLAN 30 が、カスタマー B に VLAN 40 が割り当てられています。エッジスイッチのトンネルポートに入る、IEEE 802.1Q タグが付いたパケットには、サービス プロバイダー ネットワークに入るとき、VLAN ID 30 または 40 を適切に含む外部タグ、および VLAN 100 などの元の VLAN 番号を含む内部タグが付いて二重タグになります。カスタマー A とカスタマー B の両方が、それぞれのネットワーク内で VLAN 100 を含んでいても、外部タグが異なるので、サービス プロバイダー ネットワーク内で区別されます。それぞれのカスタマーは、その他のカスタマーが使用する VLAN 番号スペース、およびサービス プロバイダー ネットワークが使用する VLAN 番号スペースから独立した、独自の VLAN 番号スペースを制御します。

発信トンネルポートでは、カスタマーのネットワーク上の元の VLAN 番号が回復されます。トンネリングおよびタグ付けを複数のレベルにすることもできますが、このリリースのスイッチでは 1 レベルだけがサポートされます。

カスタマー ネットワークから発信されるトラフィックにタグ（ネイティブ VLAN フレーム）が付いていない場合、そのパケットのブリッジングまたはルーティングは通常パケットとして行われます。エッジスイッチのトンネルポートを通過してサービス プロバイダー ネットワークに入るすべてのパケットは、タグが付いていないか、IEEE 802.1Q ヘッダーですでにタグが付いているかに関係なく、タグなしパケットとして扱われます。パケットは、IEEE 802.1Q トランクポートでサービス プロバイダー ネットワークを通じて送信される場合、メトロ タグ VLAN ID（トンネルポートのアクセス VLAN に設定）でカプセル化されます。メトロ タグのプライオリティフィールドは、トンネルポートで設定されているインターフェイス Class of Service (CoS; サービス クラス) プライオリティに設定されます（設定されていない場合、デフォルトはゼロです）。

## IEEE 802.1Q トンネリングの設定

ここでは、次の設定情報について説明します。

- 「IEEE 802.1Q トンネリングのデフォルト設定」(P.17-4)
- 「IEEE 802.1Q トンネリング設定時の注意事項」(P.17-4)

- 「IEEE 802.1Q トンネリングおよびその他の機能」(P.17-5)
- 「IEEE 802.1Q トンネリング ポートの設定」(P.17-6)

## IEEE 802.1Q トンネリングのデフォルト設定

デフォルトの場合、デフォルト switchport モードが dynamic auto であるため、IEEE 802.1Q トンネルはディセーブルです。すべての IEEE 802.1Q トランク ポートにおける IEEE 802.1Q ネイティブ VLAN パケットのタグ付けもディセーブルです。

## IEEE 802.1Q トンネリング設定時の注意事項

IEEE 802.1Q トンネリングを設定する場合は、カスタマー デバイスおよびエッジ スイッチの間で非対称リンクを常に使用する必要があります。カスタマー デバイスのポートを IEEE 802.1Q トランク ポートに、エッジ スイッチのポートをトンネル ポートとして設定してください。

トンネリングに使用する VLAN だけにトンネル ポートを割り当ててください。

ネイティブ VLAN および Maximum Transmission Unit (MTU; 最大伝送ユニット) の設定要件については、次のセクションで説明します。

## ネイティブ VLAN

エッジ スイッチで IEEE 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、IEEE 802.1Q トランク ポートを使用する必要があります。しかしサービス 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、IEEE 802.1Q トランク、ISL トランク、非トランキング リンクのいずれかで送信できます。コア スイッチで IEEE 802.1Q トランクを使用する場合、IEEE 802.1Q トランクのネイティブ VLAN を、同一スイッチの非トランキング (トンネリング) ポートのネイティブ VLAN と一致させることはできません。ネイティブ VLAN のトラフィックに、IEEE 802.1Q 送信トランク ポートでタグが付かないためです。

**図 17-3** を参照してください。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 IEEE 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 に属している、サービス プロバイダー 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メトロ タグは追加されません。パケットには VLAN 30 タグだけが付き、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 ポートによってカスタマー Y に間違えて送信されます。

この問題の解決方法は次のとおりです。

- サービス プロバイダー ネットワークのコア スイッチ間で ISL トランクを使用します。エッジ スイッチに接続されているカスタマー インターフェイスは IEEE 802.1Q トランクとしますが、コア レイヤのスイッチの接続には ISL トランクの使用を推奨します。
- **vlan dot1q tag native** グローバル コンフィギュレーション コマンドを使用し、ネイティブ VLAN を含む、IEEE 802.1Q トランクから発信されるすべてのパケットが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 IEEE 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。



る場合、トンネル ポートから受信したタグなし IP パケットは、スイッチに認識されてルーティングされます。カスタマーは、ネイティブ VLAN でインターネットにアクセスできます。このアクセスが必要ない場合は、トンネル ポートを含む VLAN で SVI を設定しないでください。

- フォールバック ブリッジングは、トンネル ポートでサポートされません。トンネル ポートから受信したすべての IEEE 802.1Q タグ付きパケットは IP 以外のパケットとして扱われるので、トンネル ポートが設定されている VLAN でフォールバック ブリッジングがイネーブルである場合、IP パケットは VLAN を越えて不適切にブリッジングされます。このため、トンネル ポートを含む VLAN ではフォールバック ブリッジングをイネーブルにしないでください。
- トンネル ポートでは IP Access Control List (ACL; アクセス コントロール リスト) がサポートされません。
- レイヤ 3 情報に関連するレイヤ 3 Quality of Service (QoS) ACL およびその他の QoS 機能は、トンネル ポートでサポートされません。MAC ベース QoS はトンネル ポートでサポートされます。
- IEEE 802.1Q 設定が EtherChannel ポート グループ内で矛盾しない場合、EtherChannel ポート グループにはトンネル ポートとの互換性があります。
- Port Aggregation Protocol (PAgP; ポート集約プロトコル)、Link Aggregation Control Protocol (LACP)、UniDirectional Link Detection (UDLD; 単一方向リンク検出) は、IEEE 802.1Q トンネリング ポートでサポートされます。
- トンネル ポートとトランク ポートで非対称リンクを手動で設定する必要があるため、Dynamic Trunking Protocol (DTP; ダイナミック トランッキング プロトコル) には IEEE 802.1Q トンネリングとの互換性はありません。
- VLAN Trunking Protocol (VTP) は、非対称リンクで接続されているデバイス間、またはトンネルを通して通信を行うデバイス間で動作しません。
- IEEE 802.1Q トンネル ポートでは、ループバック検出がサポートされます。
- IEEE 802.1Q トンネル ポートとしてポートを設定すると、スパンニング ツリー Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) フィルタリングがインターフェイスで自動的にイネーブルになります。Cisco Discovery Protocol (CDP; シスコ検出プロトコル) および Layer Link Discovery Protocol (LLDP) は、インターフェイスで自動的にディセーブルになります。

## IEEE 802.1Q トンネリング ポートの設定

IEEE 802.1Q トンネル ポートとしてポートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	トンネル ポートとして設定す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。これは、カスタマー スwitch に接続するサービス プロバイダー ネットワークのエッジ ポートである必要があります。有効なインターフェイスには、物理インターフェイス およびポートチャネル論理インターフェイス (ポート チャネル 1 ~ 48) が含まれます。
ステップ 3	<code>switchport access vlan vlan-id</code>	デフォルト VLAN を指定します。これは、インターフェイスがトランッキングを停止した場合に使用されます。この VLAN ID は特定カスタマーに固有です。
ステップ 4	<code>switchport mode dot1q-tunnel</code>	IEEE 802.1Q 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 5	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 6	<code>vlan dot1q tag native</code>	(任意) すべての IEEE 802.1Q トランク ポートでネイティブ VLAN パケットのタグ付けをイネーブルにするようにスイッチを設定します。これを設定せず、カスタマー VLAN ID がネイティブ VLAN と同じである場合、トランク ポートはメトロ タグを適用せず、パケットは誤った宛先に送信される可能性があります。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show running-config</code> <code>show dot1q-tunnel</code>	IEEE 802.1Q トンネリング用に設定したポートを表示します。 トンネリング モードになっているポートを表示します。
ステップ 9	<code>show vlan dot1q tag native</code>	IEEE 802.1Q ネイティブ VLAN タグ付けステータスを表示します。
ステップ 10	<code>copy running-config startup-config</code>	(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。

`dynamic desirable` のデフォルト状態にポートを戻すには、`no switchport mode dot1q-tunnel` インターフェイス コンフィギュレーション コマンドを使用します。ネイティブ VLAN パケットのタグ付けをディセーブルにするには、`no vlan dot1q tag native` グローバル コンフィギュレーション コマンドを使用します。

次は、トンネル ポートとしてインターフェイスを設定してネイティブ VLAN パケットのタグ付けをイネーブルにし、設定を確認する方法の例です。この設定では、ギガビットイーサネット インターフェイス 7 に接続するカスタマーの VLAN ID は、VLAN 22 になります。

```
Switch(config)# interface gigabitethernet0/7
Switch(config-if)# switchport access vlan 22
% Access VLAN does not exist. Creating vlan 22
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# exit
Switch(config)# vlan dot1q tag native
Switch(config)# end
Switch# show dot1q-tunnel interface gigabitethernet0/7
Port
-----
Gi0/1Port
-----

Switch# show vlan dot1q tag native
dot1q native vlan tagging is enabled
```

## レイヤ 2 プロトコル トンネリングの概要

サービス プロバイダー ネットワークを越えて接続されている、さまざまなサイトのカスタマーは、さまざまなレイヤ 2 プロトコルを使用してトポロジをスケールし、すべてのリモート サイトおよびローカル サイトを含める必要があります。STP を適切に動作させる必要があります。サービス プロバイダー ネットワークを越えたローカル サイトおよびすべてのリモート サイトを含む、適切なスパンニング ツリーをすべての VLAN で構築する必要があります。CDP では、隣接するシスコ デバイスをローカル サイトおよびリモート サイトから検出する必要があります。VTP では、カスタマー ネットワークのすべてのサイトで矛盾しない VLAN 設定を提供する必要があります。

プロトコル トンネリングがイネーブルである場合、サービス プロバイダー ネットワークの着信側のエッジスイッチでは、特殊 MAC アドレスでレイヤ 2 プロトコル パケットがカプセル化され、サービス プロバイダー ネットワークを越えて送信されます。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、VTP のレイヤ 2 Protocol Data

Unit (PDU; プロトコル データ ユニット) は、サービス プロバイダー ネットワークをまたがり、サービス プロバイダー ネットワークの発信側のカスタマー スイッチに配信されます。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、次のような結果になります。

- それぞれのカスタマー サイトのユーザは STP を適切に実行でき、すべての VLAN では、ローカル サイトだけではなく、すべてのサイトからのパラメータに基づいて、正しいスパンニング ツリーが構築されます。
- CDP では、サービス プロバイダー ネットワークによって接続されているその他のシスコ デバイスに関する情報が検出されて表示されます。
- VTP ではカスタマー ネットワーク全体で矛盾しない VLAN 設定が提供され、サービス プロバイダーを通してすべてのスイッチに伝播されます。



(注)

サードパーティ ベンダーとの相互運用性を提供するには、レイヤ 2 プロトコル トンネル バイパス機能を使用します。バイパス モードでは、プロトコル トンネリングの制御方法が異なるベンダー スイッチに制御 PDU が透過的に転送されます。バイパス モードを実装するには、出力トランク ポートでレイヤ 2 プロトコル トンネリングをイネーブルにします。レイヤ 2 プロトコル トンネリングがトランク ポートでイネーブルの場合、カプセル化された MAC アドレスが削除されて、プロトコル パケットに通常の MAC アドレスを有するようになります。

レイヤ 2 プロトコル トンネリングは個別に使用できます。レイヤ 2 プロトコル トンネリングでは、IEEE 802.1Q トンネリングを拡張することができます。IEEE 802.1Q トンネリング ポートでプロトコル 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 PDU が受信されず、STP、CDP、VTP を適切に実行できません。プロトコル 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。IEEE 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。IEEE 802.1Q トンネリングを使用しない場合は、アクセス ポートでカスタマー スイッチに接続し、サービス プロバイダーのアクセス ポートでトンネリングをイネーブルにすることで、レイヤ 2 プロトコル トンネリングをイネーブルにできます。

たとえば図 17-4 の場合、カスタマー X には同一 VLAN に 4 つのスイッチがあり、サービス プロバイダー ネットワークで接続されています。ネットワークで PDU がトンネルされない場合、ネットワークの向こう側のスイッチでは、STP、CDP、VTP を適切に実行できません。たとえば、カスタマー X のサイト 1 内のスイッチ上の VLAN に対する STP は、サイト 2 のカスタマー X 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、サイト 1 のスイッチ上にスパンニング ツリーを構築します。そのトポロジを図 17-5 に示します。

図 17-4 レイヤ 2 プロトコル トンネリング

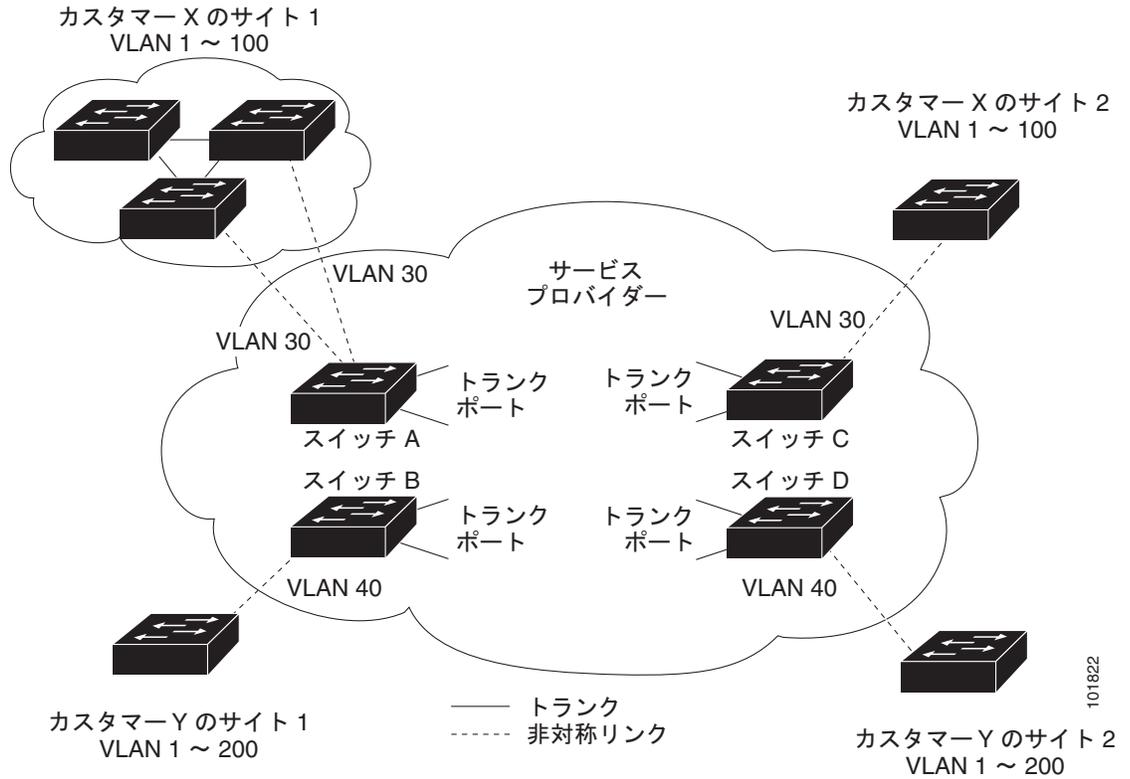
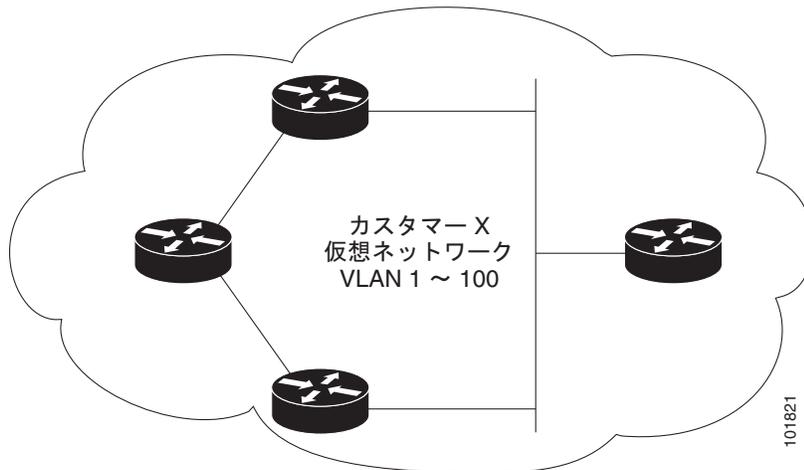


図 17-5 適切なコンバージェンスを含まないレイヤ 2 ネットワーク トポロジ

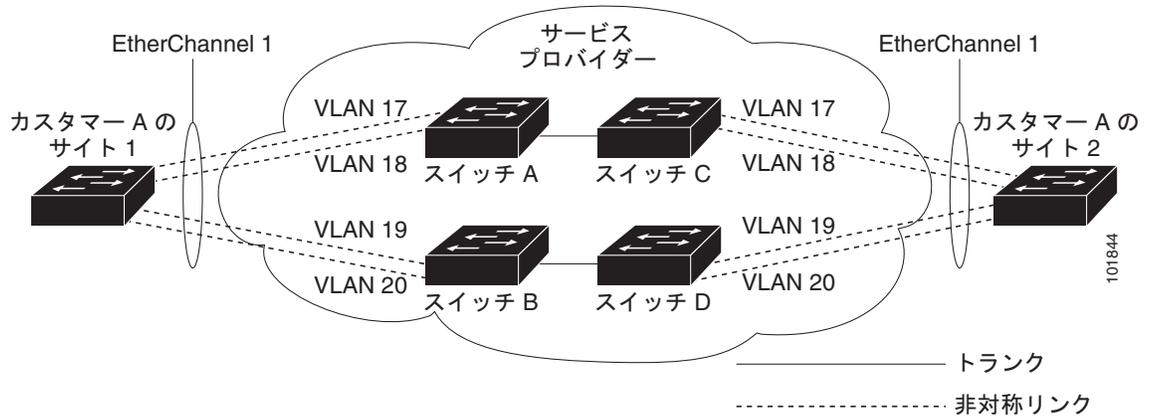


サービス プロバイダー ネットワークでは、レイヤ 2 プロトコル トンネリングを使用し、ポイントツープイント ネットワーク トポロジをエミュレートして、EtherChannel の作成を拡張することができます。サービス プロバイダー スイッチでプロトコル トンネリング (PAgP または LACP) をイネーブルにすると、リモート カスタマー スイッチでは PDU が受信され、EtherChannel の自動作成をネゴシエーションできるようになります。

たとえば図 17-6 の場合、カスタマー A には同一 VLAN に 2 つのスイッチがあり、サービス プロバイダー ネットワークで接続されています。ネットワークで PDU がトンネリングされると、ネットワークの向こう側のスイッチでは、専用回線を必要とせずに、EtherChannel の自動作成をネゴシエーション

できます。手順については、「EtherChannel のレイヤ 2 トンネリングの設定」(P.17-14) を参照してください。

図 17-6 EtherChannel のレイヤ 2 プロトコル トンネリング



## レイヤ 2 プロトコル トンネリングの設定

サービス プロバイダー ネットワークのエッジ スイッチで、カスタマーに接続されているポートにおいて、レイヤ 2 プロトコル トンネリングをプロトコルごとにイネーブルにできます。カスタマー スイッチに接続されているサービス プロバイダー エッジ スイッチでは、トンネリング処理が実行されます。エッジ スイッチ トンネル ポートは、カスタマーの IEEE 802.1Q トランク ポートに接続します。エッジ スイッチ アクセス ポートは、カスタマー アクセス ポートに接続します。カスタマー スイッチに接続されているエッジ スイッチでは、トンネリング処理が実行されます。

アクセス ポートまたはトンネル ポートのいずれかとして設定されているポートでは、レイヤ 2 プロトコル トンネリングをイネーブルにできます。switchport モードが **dynamic auto** (デフォルト モード) または **dynamic desirable** に設定されているポートでは、レイヤ 2 プロトコル トンネリングをイネーブルにすることができません。

スイッチでは、CDP、STP、VTP のレイヤ 2 プロトコル トンネリングがサポートされます。ポイント ツーポイント ネットワーク トポロジのエミュレートの場合は、PAgP、LACP、UDLD のプロトコルもサポートされます。スイッチでは、LLDP のレイヤ 2 プロトコル トンネリングはサポートされません。



注意

PAgP、LACP、UDLD プロトコル トンネリングでは、ポイント ツーポイント トポロジのエミュレートだけが目的です。トンネリングされるパケットが多く、ポートに送信されるエラー設定では、ネットワーク障害となることがあります。

レイヤ 2 プロトコルがイネーブルになっているポートでサービス プロバイダーの着信エッジ スイッチに入ったレイヤ 2 PDU が、トランク ポートからサービス プロバイダー ネットワークに出る場合、スイッチでは、カスタマー PDU 宛先 MAC アドレスが、既知のシスコ独自のマルチキャスト アドレス (01-00-0c-cd-cd-d0) で上書きされます。IEEE 802.1Q トンネリングがイネーブルである場合、パケットにはタグが二重に付きます。外部タグはカスタマーのメトロ タグであり、内部タグはカスタマーの VLAN タグです。コア スイッチでは内部タグが無視され、同じメトロ VLAN のすべてのトランク ポートにパケットが転送されます。発信側のエッジ スイッチでは、適切なレイヤ 2 プロトコル情報および MAC アドレス情報が復元され、同じメトロ VLAN のすべてのトンネル ポートかアクセス ポートにパケットが転送されます。このため、レイヤ 2 PDU はそのまま残り、サービス プロバイダー インフラストラクチャを越えてカスタマー ネットワークの反対側に配信されます。

図 17-4 を参照すると、カスタマー X およびカスタマー Y が、それぞれアクセス VLAN 30 および 40 になっています。非対称リンクにより、サイト 1 のカスタマーは、サービスプロバイダー ネットワークのエッジスイッチに接続されています。サイト 1 のカスタマー Y からスイッチ 2 に発信されたレイヤ 2 PDU (たとえば BPDU) は、既知の MAC アドレスが宛先 MAC アドレスになっている二重タグパケットとしてインフラストラクチャに転送されます。この二重タグパケットには、40 というメトロ VLAN タグと VLAN 100 などの内部 VLAN タグが付いています。二重タグパケットがスイッチ D に入ると、外部 VLAN タグ 40 が外され、既知の MAC アドレスがそれぞれのレイヤ 2 プロトコル MAC アドレスに置換され、パケットは、VLAN 100 の一重タグフレームとしてサイト 2 のカスタマー Y に送信されます。

カスタマースイッチのアクセスポートまたはトランクポートに接続されているエッジスイッチのアクセスポートでも、レイヤ 2 プロトコル トンネリングをイネーブルにできます。この場合は、カプセル化プロセスとカプセル化解除プロセスは前の段落で説明したものと同じですが、パケットはサービスプロバイダーネットワークで二重タグになりません。カスタマー固有のアクセス VLAN タグの一重タグになります。

ここでは、次の設定情報について説明します。

- 「レイヤ 2 プロトコル トンネリングのデフォルト設定」(P.17-11)
- 「レイヤ 2 プロトコル トンネリング設定時の注意事項」(P.17-11)
- 「レイヤ 2 プロトコル トンネリングの設定」(P.17-13)
- 「EtherChannel のレイヤ 2 トンネリングの設定」(P.17-14)

## レイヤ 2 プロトコル トンネリングのデフォルト設定

表 17-1 に、レイヤ 2 プロトコル トンネリングのデフォルト設定を示します。

表 17-1 レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定

機能	デフォルト設定
レイヤ 2 プロトコル トンネリング	ディセーブル。
シャットダウンしきい値	未設定。
ドロップしきい値	未設定。
CoS 値	インターフェイスで CoS 値が設定されている場合は、その値がレイヤ 2 プロトコル トンネリングの BPDU CoS 値を設定するために使用されます。インターフェイス レベルで CoS 値が設定されていない場合、L2 プロトコル トンネリング BPDU の CoS マーキングのデフォルト値は 5 です。これだデータトラフィックには適用されません。

## レイヤ 2 プロトコル トンネリング設定時の注意事項

次は、レイヤ 2 プロトコル トンネリングの設定時の注意事項および動作特性です。

- スイッチでは、Multiple STP (MSTP) を含む CDP、STP および VTP のトンネリングがサポートされます。プロトコル トンネリングはデフォルトでディセーブルになっていますが、IEEE 802.1Q トンネルポート、またはアクセスポートでプロトコルごとにイネーブルにできます。
- スイッチでは、**switchport** モードが **dynamic auto** または **dynamic desirable** に設定されているポートにおいて、レイヤ 2 プロトコル トンネリングがサポートされません。

- DTP はレイヤ 2 プロトコル トンネリングと互換性がありません。
- サービス プロバイダー ネットワークの発信側のエッジスイッチでは、適切なレイヤ 2 プロトコル 情報および MAC アドレス情報が復元され、同じメトロ VLAN のすべてのトンネル ポートおよび アクセス ポートにパケットが転送されます。
- サードパーティ ベンダー スイッチとの相互運用性のため、スイッチではレイヤ 2 プロトコル トンネル バイパス機能がサポートされます。バイパス モードでは、プロトコル トンネリングの制御方法が異なるベンダー スイッチに制御 PDU が透過的に転送されます。スイッチの入力ポートでレイヤ 2 プロトコル トンネルがイネーブルである場合は、出力トランク ポートにより、トンネリングされたパケットが特殊なカプセル化で転送されます。出力トランク ポートでもレイヤ 2 プロトコル トンネリングをイネーブルにすると、この動作がバイパスされて、スイッチによって、処理や修正が行われずに制御 PDU が転送されます。
- スイッチでは、ポイントツーポイント ネットワーク トポロジのエミュレートの場合、PAgP、LACP、UDLD のトンネリングがサポートされます。プロトコル トンネリングはデフォルトでディセーブルになっていますが、IEEE 802.1Q トンネル ポート、またはアクセス ポートでプロトコルごとにイネーブルにできます。
- PAgP トンネリングまたは LACP トンネリングの場合は、リンク障害検出を高速にするため、インターフェイスで UDLD もイネーブルにするよう推奨します。
- PAgP パケット、LACP パケット、UDLD パケットのうちいずれかのレイヤ 2 プロトコル トンネリングでは、ループバック検出がサポートされません。
- IEEE 802.1Q 設定が EtherChannel ポート グループ内で矛盾しない場合、EtherChannel ポート グループにはトンネル ポートとの互換性があります。
- 独自の宛先 MAC アドレスでカプセル化された PDU が、レイヤ 2 トンネリングがイネーブルになっているトンネル ポートまたはアクセス ポートから受信される場合、トンネル ポートは、ループを防止するためにシャットダウンされます。このポートは、プロトコル用に設定されたシャットダウンしきい値に達した場合にもシャットダウンされます。**shutdown** コマンドに続けて **no shutdown** コマンドを入力すると、ポートを再び手動でイネーブルにできます。**errdisable recovery** がイネーブルである場合は、指定された間隔で動作が再試行されます。
- カプセル化が解除された PDU だけがカスタマー ネットワークに転送されます。サービス プロバイダー ネットワーク上で動作しているスパンニング ツリー インスタンスでは、BPDU がトンネル ポートに転送されません。CDP パケットはトンネル ポートから転送されません。
- インターフェイスでプロトコル トンネリングがイネーブルである場合は、カスタマー ネットワークによって生成された PDU 用に、プロトコルごとのシャットダウンしきい値やポートごとのシャットダウンしきい値を設定できます。制限を越えると、ポートはシャットダウンされます。QoS ACL およびポリシー マップをトンネル ポートで使用すると、BPDU レートを制限することもできます。
- インターフェイスでプロトコル トンネリングがイネーブルである場合は、カスタマー ネットワークによって生成された PDU 用に、プロトコルごとのドロップしきい値やポートごとのドロップしきい値を設定できます。制限を越えると、ポートが PDU を受信するレートがドロップしきい値未満になるまで、ポートで PDU が廃棄されます。
- トンネリングされた PDU (具体的には STP BPDU) は、カスタマーの仮想ネットワークが正しく動作するためにすべてのリモート サイトに配信される必要があるため、同じトンネル ポートから受信されるデータ パケットよりも PDU のプライオリティをサービス プロバイダー ネットワーク内で高くできます。デフォルトの場合、PDU ではデータ パケットと同じ CoS 値が使用されます。

## レイヤ 2 プロトコル トンネリングの設定

レイヤ 2 プロトコル トンネリング用にポートを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<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	<b>interface interface-id</b>	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、トンネル ポートとして設定するインターフェイスを入力します。これは、カスタマースイッチに接続するサービス プロバイダー ネットワークのエッジポートである必要があります。有効なインターフェイスは、物理インターフェイスおよびポートチャネル論理インターフェイス（ポート チャネル 1～48）です。
ステップ 3	<b>switchport mode access</b> または <b>switchport mode dot1q-tunnel</b>	アクセス ポートまたは IEEE 802.1Q 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	<b>l2protocol-tunnel [cdp   stp   vtp]</b>	目的のプロトコルのプロトコル トンネリングをイネーブルにします。キーワードを入力しない場合、トンネリングは、3 つすべてのレイヤ 2 プロトコルでイネーブルになります。
ステップ 5	<b>l2protocol-tunnel shutdown-threshold [cdp   stp   vtp] value</b>	(任意) カプセル化用に 1 秒間に受信するパケット数のしきい値を設定します。設定したしきい値を超えると、インターフェイスはディセーブルになります。プロトコル オプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1～4096 です。デフォルトでは、しきい値は設定されません。 <b>(注)</b> このインターフェイスでドロップしきい値も設定する場合、シャットダウンしきい値は、ドロップしきい値以上とする必要があります。
ステップ 6	<b>l2protocol-tunnel drop-threshold [cdp   stp   vtp] value</b>	(任意) カプセル化用に 1 秒間に受信するパケット数のしきい値を設定します。設定したしきい値を超えると、インターフェイスによってパケットが廃棄されます。プロトコル オプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1～4096 です。デフォルトでは、しきい値は設定されません。 このインターフェイスでシャットダウンしきい値も設定する場合、ドロップしきい値は、シャットダウンしきい値以下である必要があります。
ステップ 7	<b>exit</b>	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	<b>errdisable recovery cause l2ptguard</b>	(任意) インターフェイスを再びイネーブルにして再試行できるようにするため、レイヤ 2 最大レート エラーからの回復メカニズムを設定します。errdisable recovery はデフォルトでディセーブルになっています。イネーブルにした場合、デフォルトの間隔は 300 秒です。
ステップ 9	<b>l2protocol-tunnel cos value</b>	(任意) トンネリングされたすべてのレイヤ 2 PDU の CoS 値を設定します。範囲は 0～7 です。デフォルトは、インターフェイスのデフォルト CoS 値です。設定されていない場合、デフォルトは 5 です。
ステップ 10	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 11	<b>show l2protocol</b>	設定されているプロトコル、しきい値、カウンタを含めた、スイッチのレイヤ 2 トンネル ポートを表示します。
ステップ 12	<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。

## ■ レイヤ 2 プロトコル トンネリングの設定

いずれかのレイヤ 2 プロトコルまたは 3 つすべてのレイヤ 2 プロトコルのプロトコル トンネリングをディセーブルにするには、**no l2protocol-tunnel [cdp | stp | vtp]** インターフェイス コンフィギュレーション コマンドを使用します。シャットダウンしきい値およびドロップしきい値をデフォルト設定に戻すには、**no l2protocol-tunnel shutdown-threshold [cdp | stp | vtp]** コマンドおよび **no l2protocol-tunnel drop-threshold [cdp | stp | vtp]** コマンドを使用します。

次に、CDP、STP、VTP のレイヤ 2 プロトコル トンネリングを設定し、設定を確認する例を示します。

```
Switch(config)# interface fastethernet0/11
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel stp
Switch(config-if)# l2protocol-tunnel vtp
Switch(config-if)# l2protocol-tunnel shutdown-threshold 1500
Switch(config-if)# l2protocol-tunnel drop-threshold 1000
Switch(config-if)# exit
Switch(config)# l2protocol-tunnel cos 7
Switch(config)# end
Switch# show l2protocol
COS for Encapsulated Packets: 7
Port      Protocol Shutdown Drop Encapsulation Decapsulation Drop
          Threshold Threshold Counter          Counter          Counter
-----
Fa0/11    cdp          1500    1000 2288          2282            0
          stp          1500    1000 116           13              0
          vtp          1500    1000 3             67              0
          pagp       ----     ---- 0             0               0
          lacp       ----     ---- 0             0               0
          udld       ----     ---- 0             0               0
```

## EtherChannel のレイヤ 2 トンネリングの設定

レイヤ 2 ポイントツーポイント トンネリングを設定して EtherChannel の自動作成を容易にするには、サービス プロバイダー エッジ スイッチおよびカスタマー スイッチの両方を設定する必要があります。

### サービス プロバイダー エッジ スイッチの設定

EtherChannel のレイヤ 2 プロトコル トンネリング用にサービス プロバイダー エッジ スイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<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	<b>interface interface-id</b>	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、トンネルポートとして設定するインターフェイスを入力します。これは、カスタマー スイッチに接続するサービス プロバイダー ネットワークのエッジポートである必要があります。有効なインターフェイスは物理インターフェイスです。
ステップ 3	<b>switchport mode dot1q-tunnel</b>	IEEE 802.1Q トンネルポートとしてインターフェイスを設定します。

コマンド	目的
ステップ 4 <b>l2protocol-tunnel point-to-point [pagp   lacp   udld]</b>	(任意) 目的のプロトコルのポイントツーポイント プロトコル トンネリングをイネーブルにします。キーワードを入力しない場合、トンネリングは、3 つすべてのプロトコルでイネーブルになります。   <b>注意</b> ネットワーク障害を避けるため、ネットワークがポイントツーポイント トポロジになっていることを確認してから、PAgP パケット、LACP パケット、UDLD パケットのうちいずれかのトンネリングをイネーブルにしてください。
ステップ 5 <b>l2protocol-tunnel shutdown-threshold [point-to-point [pagp   lacp   udld]] value</b>	(任意) カプセル化用に 1 秒間に受信するパケット数のしきい値を設定します。設定したしきい値を超えると、インターフェイスはディセーブルになります。プロトコル オプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ~ 4096 です。デフォルトでは、しきい値は設定されません。  <b>(注)</b> このインターフェイスでドロップしきい値も設定する場合、シャットダウンしきい値は、ドロップしきい値以上とする必要があります。
ステップ 6 <b>l2protocol-tunnel drop-threshold [point-to-point [pagp   lacp   udld]] value</b>	(任意) カプセル化用に 1 秒間に受信するパケット数のしきい値を設定します。設定したしきい値を超えると、インターフェイスによってパケットが廃棄されます。プロトコル オプションを指定しない場合、しきい値は、それぞれのトンネリングされたレイヤ 2 プロトコル タイプに適用されます。指定できる範囲は 1 ~ 4096 です。デフォルトでは、しきい値は設定されません。  <b>(注)</b> このインターフェイスでシャットダウンしきい値も設定する場合、ドロップしきい値は、シャットダウンしきい値以下である必要があります。
ステップ 7 <b>no cdp enable</b>	インターフェイス上で CDP をディセーブルにします。
ステップ 8 <b>spanning-tree bpdupfilter enable</b>	インターフェイス上で BPDU フィルタリングをイネーブルにします。
ステップ 9 <b>exit</b>	グローバル コンフィギュレーション モードに戻ります。
ステップ 10 <b>errdisable recovery cause l2ptguard</b>	(任意) インターフェイスを再びイネーブルにして再試行できるようにするため、レイヤ 2 最大レート エラーからの回復メカニズムを設定します。errdisable recovery はデフォルトでディセーブルになっています。イネーブルにした場合、デフォルトの間隔は 300 秒です。
ステップ 11 <b>l2protocol-tunnel cos value</b>	(任意) トンネリングされたすべてのレイヤ 2 PDU の CoS 値を設定します。範囲は 0 ~ 7 です。デフォルトは、インターフェイスのデフォルト CoS 値です。設定されていない場合、デフォルトは 5 です。
ステップ 12 <b>end</b>	特権 EXEC モードに戻ります。
ステップ 13 <b>show l2protocol</b>	設定されているプロトコル、しきい値、カウンタを含めた、スイッチのレイヤ 2 トンネル ポートを表示します。
ステップ 14 <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。

いずれかのレイヤ 2 プロトコルまたは 3 つすべてのレイヤ 2 プロトコルのポイントツーポイント プロトコル トンネリングをディセーブルにするには、**no l2protocol-tunnel [point-to-point [pagp | lacp | udld]]** インターフェイス コンフィギュレーション コマンドを使用します。シャットダウンしきい値およびドロップしきい値をデフォルト設定に戻すには、**no l2protocol-tunnel shutdown-threshold [point-to-point [pagp | lacp | udld]]** コマンドおよび **no l2protocol-tunnel drop-threshold [[point-to-point [pagp | lacp | udld]]** コマンドを使用します。

## カスタマー スイッチの設定

サービス プロバイダー エッジ スイッチを設定したら、特権 EXEC モードで次の手順を実行し、EtherChannel のレイヤ 2 プロトコル トンネリング用にカスタマー スイッチを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	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	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始します。これは、カスタマー スイッチ ポートにする必要があります。
ステップ 3	<code>switchport trunk encapsulation dot1q</code>	トランキング カプセル化形式を IEEE 802.1Q に設定します。
ステップ 4	<code>switchport mode trunk</code>	インターフェイス上でトランキングをイネーブルにします。
ステップ 5	<code>udld enable</code>	インターフェイスの通常モードで UDLD をイネーブルにします。
ステップ 6	<code>channel-group channel-group-number mode desirable</code>	チャンネル グループにインターフェイスを割り当て、PAgP モードに <b>desirable</b> を指定します。EtherChannel の設定の詳細については、 <a href="#">第 36 章「EtherChannel およびリンクステート トラッキングの設定」</a> を参照してください。
ステップ 7	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	<code>interface port-channel port-channel number</code>	ポートチャンネル インターフェイス モードに入ります。
ステップ 9	<code>shutdown</code>	インターフェイスをシャットダウンします。
ステップ 10	<code>no shutdown</code>	インターフェイスをイネーブルにします。
ステップ 11	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 12	<code>show l2protocol</code>	設定されているプロトコル、しきい値、カウンタを含めた、スイッチのレイヤ 2 トンネル ポートを表示します。
ステップ 13	<code>copy running-config startup-config</code>	(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。

インターフェイスをデフォルト設定に戻すには、**no switchport mode trunk**、**no udld enable**、**no channel group channel-group-number mode desirable** インターフェイス コンフィギュレーション コマンドを使用します。

EtherChannel の場合は、サービス プロバイダー エッジ スイッチおよびカスタマー スイッチをレイヤ 2 プロトコル トンネリング用に設定する必要があります (図 17-6 (P.17-10) を参照)。

次に、サービス プロバイダーのエッジ スイッチ 1 およびエッジ スイッチ 2 を設定する例を示します。VLAN 17、18、19、20 はアクセス VLAN、ファスト イーサネット インターフェイス 1 および 2 は PAgP および UDLD がイネーブルになっているポイントツーポイント トンネル ポート、ドロップしきい値は 1000、ファスト イーサネット インターフェイス 3 はトランク ポートです。

サービス プロバイダー エッジ スイッチ 1 の設定は次のとおりです。

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport access vlan 17
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
Switch(config-if)# l2protocol-tunnel point-to-point udld
Switch(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if)# exit
Switch(config)# interface fastethernet0/2
Switch(config-if)# switchport access vlan 18
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# l2protocol-tunnel point-to-point pagp
```

```
Switch(config-if) # l2protocol-tunnel point-to-point uddl
Switch(config-if) # l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if) # exit
Switch(config) # interface fastethernet0/3
Switch(config-if) # switchport trunk encapsulation isl
Switch(config-if) # switchport mode trunk
```

サービス プロバイダー エッジ スイッチ 2 の設定は次のとおりです。

```
Switch(config) # interface fastethernet0/1
Switch(config-if) # switchport access vlan 19
Switch(config-if) # switchport mode dot1q-tunnel
Switch(config-if) # l2protocol-tunnel point-to-point pagp
Switch(config-if) # l2protocol-tunnel point-to-point uddl
Switch(config-if) # l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if) # exit
Switch(config) # interface fastethernet0/2
Switch(config-if) # switchport access vlan 20
Switch(config-if) # switchport mode dot1q-tunnel
Switch(config-if) # l2protocol-tunnel point-to-point pagp
Switch(config-if) # l2protocol-tunnel point-to-point uddl
Switch(config-if) # l2protocol-tunnel drop-threshold point-to-point pagp 1000
Switch(config-if) # exit
Switch(config) # interface fastethernet0/3
Switch(config-if) # switchport trunk encapsulation isl
Switch(config-if) # switchport mode trunk
```

次に、サイト 1 のカスタマー スイッチの設定例を示します。ファストイーサネット インターフェイス 1、2、3、4 は IEEE 802.1Q トランッキング用に設定されており、UDLD はイネーブル、EtherChannel グループ 1 はイネーブル、ポート チャネルはシャットダウンされたあとでイネーブルになり EtherChannel 設定がアクティブになります。

```
Switch(config) # interface fastethernet0/1
Switch(config-if) # switchport trunk encapsulation dot1q
Switch(config-if) # switchport mode trunk
Switch(config-if) # udld enable
Switch(config-if) # channel-group 1 mode desirable
Switch(config-if) # exit
Switch(config) # interface fastethernet0/2
Switch(config-if) # switchport trunk encapsulation dot1q
Switch(config-if) # switchport mode trunk
Switch(config-if) # udld enable
Switch(config-if) # channel-group 1 mode desirable
Switch(config-if) # exit
Switch(config) # interface fastethernet0/3
Switch(config-if) # switchport trunk encapsulation dot1q
Switch(config-if) # switchport mode trunk
Switch(config-if) # udld enable
Switch(config-if) # channel-group 1 mode desirable
Switch(config-if) # exit
Switch(config) # interface fastethernet0/4
Switch(config-if) # switchport trunk encapsulation dot1q
Switch(config-if) # switchport mode trunk
Switch(config-if) # udld enable
Switch(config-if) # channel-group 1 mode desirable
Switch(config-if) # exit
Switch(config) # interface port-channel 1
Switch(config-if) # shutdown
Switch(config-if) # no shutdown
Switch(config-if) # exit
```

# トンネリング ステータスのモニタおよびメンテナンス

表 17-2 に、IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングのモニタとメンテナンスを行う特権 EXEC コマンドの説明を示します。

表 17-2 トンネリングのモニタおよびメンテナンスのためのコマンド

コマンド	目的
<code>clear l2protocol-tunnel counters</code>	レイヤ 2 プロトコル トンネリング ポートのプロトコル カウンタをクリアします。
<code>show dot1q-tunnel</code>	スイッチの IEEE 802.1Q トンネル ポートを表示します。
<code>show dot1q-tunnel interface interface-id</code>	特定インターフェイスがトンネル ポートであるかどうかを確認します。
<code>show l2protocol-tunnel</code>	レイヤ 2 プロトコル トンネリング ポートに関する情報を表示します。
<code>show errdisable recovery</code>	レイヤ 2 プロトコル トンネル エラー ディセーブル状態からの回復タイマーがイネーブルかどうかを確認します。
<code>show l2protocol-tunnel interface interface-id</code>	特定レイヤ 2 プロトコル トンネリング ポートに関する情報を表示します。
<code>show l2protocol-tunnel summary</code>	レイヤ 2 プロトコルのサマリー情報だけを表示します。
<code>show vlan dot1q tag native</code>	スイッチのネイティブ VLAN タグのステータスを表示します。

この表示の詳細については、このリリースのコマンドリファレンスを参照してください。