



## 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

バーチャルプライベートネットワーク（VPN）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顧客のトラフィックを運び、その他の顧客のトラフィックに影響を与えずに、それぞれの顧客の 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 3550 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、このリリースに対応する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.14-1)
- 「IEEE 802.1Q トンネリングの設定」(P.14-4)
- 「レイヤ 2 プロトコル トンネリングの概要」(P.14-7)
- 「レイヤ 2 プロトコル トンネリングの設定」(P.14-10)
- 「トンネリングステータスのモニタリングおよびメンテナンス」(P.14-18)

## IEEE 802.1Q トンネリングの概要

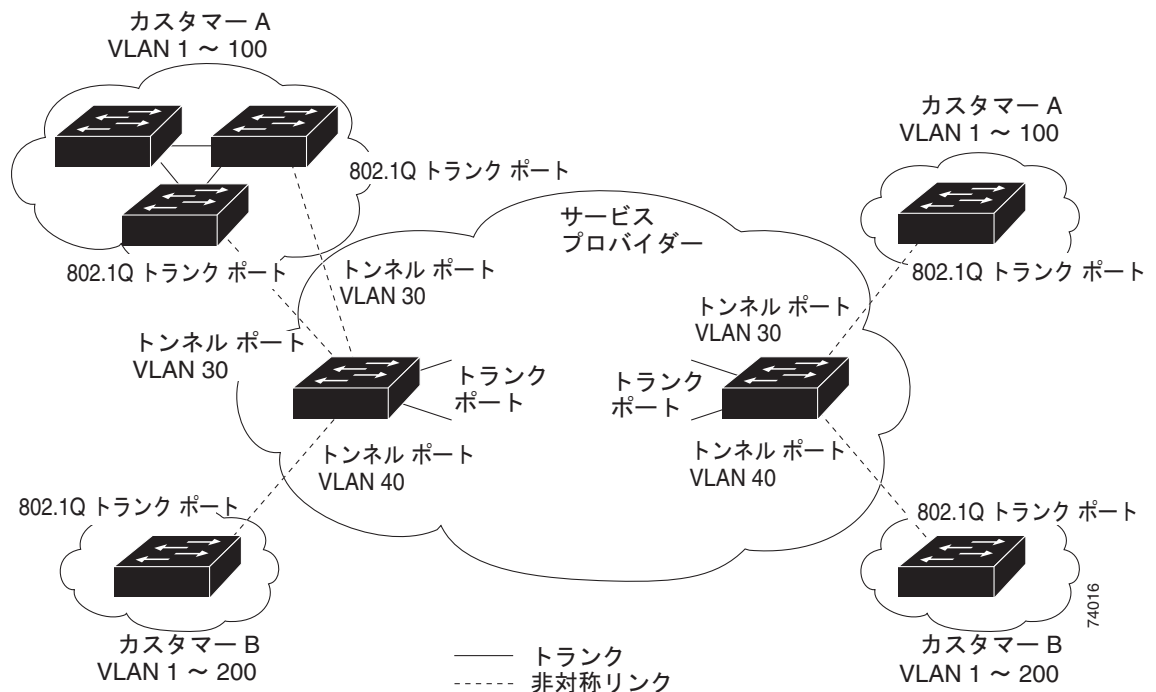
サービスプロバイダーのビジネス顧客には、多くの場合、サポートする VLAN ID および VLAN の数に固有の要件があります。同一サービスプロバイダーネットワークのさまざまな顧客が必要とする VLAN 範囲は重複し、インフラストラクチャを通る顧客のトラフィックは混合してしまうことがあります。それぞれの顧客に VLAN ID の固有の範囲を割り当てると、顧客の設定が制限され、IEEE 802.1Q 仕様の VLAN 制限（4096）を簡単に超えてしまうことがあります。

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 を含む顧客をサポートできます。顧客の VLAN ID は、同一 VLAN にあるように見えても保護され、さまざまな顧客のトラフィックは、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場合、VLAN-in-VLAN 階層構造およびタグ付きパケットへのタグ付けによって、VLAN スペースを拡張できます。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。それぞれのカスタマーには別個のサービスプロバイダー VLAN ID が必要ですが、その VLAN ID ではすべてのカスタマーの 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カスタマーのトラフィックは、カスタマー 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。カスタマー 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。それぞれのカスタマーに固有のアクセス 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 14-1 を参照してください。

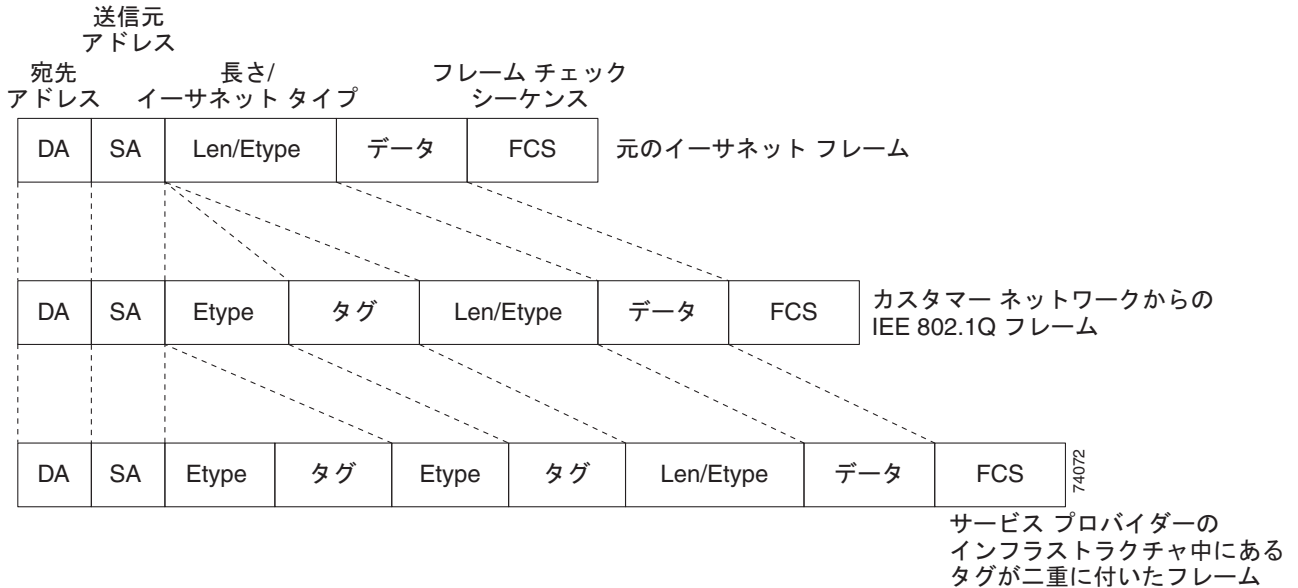
図 14-1 サービス プロバイダー ネットワークにおける IEEE 802.1Q トンネル ポート



カスタマーのトランク 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。トランク ポートからサービスプロバイダー ネットワークに送信されたタグ付きパケットは、カスタマーごとに一意の VLAN ID を含む別のレイヤの IEEE 802.1Q タグ (メトロ タグ) でカプセル化されています。カスタマーの元の 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、カスタマーのアクセス 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、二重のタグが付きます。

二重タグ付き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 ポートに着信すると、スイッチがパケットを処理するときに、メトロ タグが除去されます。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 14-2 に、元の (通常) フレームで開始するイーサネット パケットタグ構造を示します。

図 14-2 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 プロバイダー出カスイッチのトランク ポートに着信すると、スイッチがパケットを処理するときに、メトロ タグが再び除去されます。ただし、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場合、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 14-1 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場合、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、メトロ 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。

エッジスイッチのトンネルポートを通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 サービス クラス（CoS）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、IEEE 802.1Q トンネリングの設定に関する次の事項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.14-4)
- 「IEEE 802.1Q トンネリング設定時の注意事項」(P.14-4)
- 「IEEE 802.1Q トンネリングおよびその他の機能」(P.14-5)
- 「IEEE 802.1Q トンネリング ポートの設定」(P.14-6)

## IEEE 802.1Q トンネリングのデフォルト設定

デフォルトでは、デフォルト switchport モードが dynamic desirable 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、トンネルを通過するトラフィックに対して常に非対称リンクを使用し、トンネルごとに 1 つの VLAN を専用にする必要があります。また、ネイティブ VLAN の設定要件と最大伝送単位 (MTU) にも注意する必要があります。MTU の詳細については、「システム MTU」(P.14-5) を参照してください。

## 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。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、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。

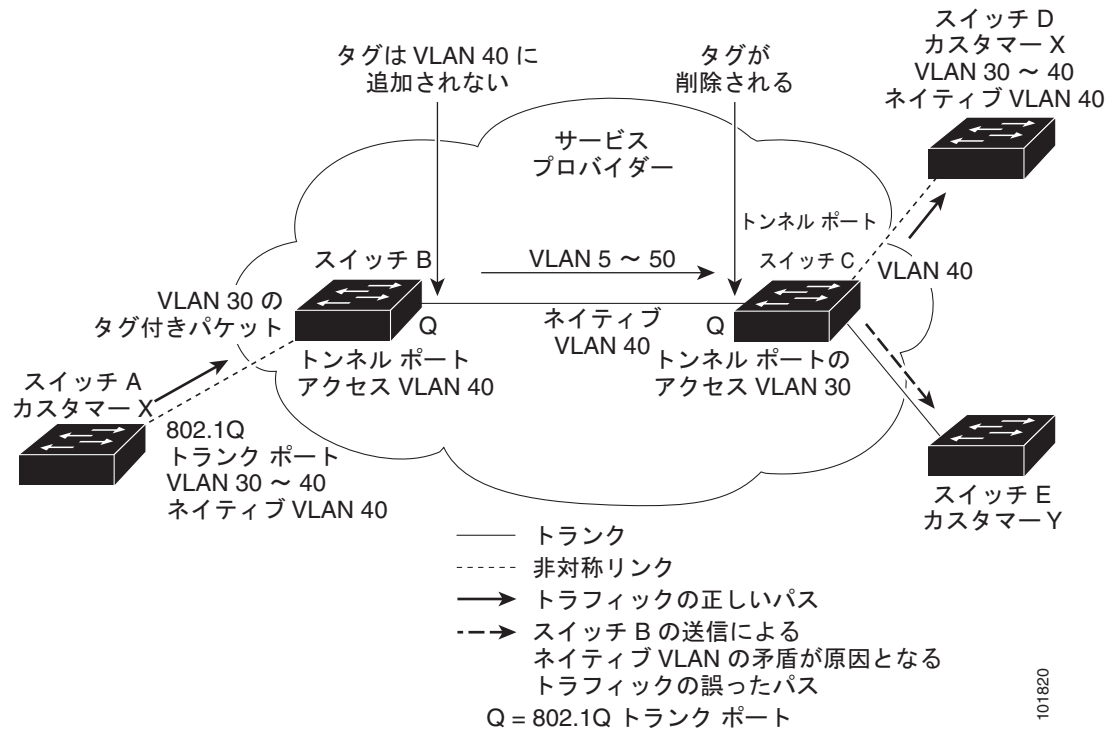
図 14-3 を参照してください。VLAN 40 は、サービスプロバイダー ネットワークの入力エッジスイッチ (スイッチ B) において、カスタマー X からの IEEE 802.1Q トランク ポートのネイティブ VLAN として設定されています。カスタマー X のスイッチ A は、VLAN 30 のタグ付きパケットを、アクセス VLAN 40 に属する、サービスプロバイダー ネットワークのスイッチ B の入力トンネル ポートに送信します。トンネル ポートのアクセス VLAN (VLAN 40) は、エッジスイッチのトランク ポートのネイティブ VLAN (VLAN 40) と同じなので、トンネル 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。

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。
- 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 範囲内でないことを確認します。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。

図 14-3 IEEE 802.1Q トンネリングおよびネイティブ VLAN に潜在する問題



## システム MTU

スイッチのトラフィックのデフォルト システム MTU は 1500 バイトです。system mtu グローバル コンフィギュレーション コマンドを使用すると、より大きなフレームをサポートするようにスイッチを設定できます。IEEE 802.1Q トンネリング機能では、メトロ タグが追加されると、フレーム サイズが 4 バイト増加するので、スイッチ システム MTU サイズを最低 1504 バイトに増加してより大きなフレームを処理できるように、サービス プロバイダー ネットワークのすべてのスイッチを設定する必要があります。Catalyst 3550 GigabitEthernet スイッチの最大許容システム MTU は、2000 バイトです。FastEthernet スイッチの最大システム MTU は、1546 バイトです。

## IEEE 802.1Q トンネリングおよびその他の機能

IEEE 802.1Q トンネリングはレイヤ 2 パケット スイッチングで適切に動作しますが、一部のレイヤ 2 機能およびレイヤ 3 スイッチングの間には非互換性があります。

- トンネル ポートはルーテッド ポートにできません。

- IEEE 802.1Q ポートを含む VLAN では IP ルーティングがサポートされません。トンネル ポートから受信したパケットは、レイヤ 2 情報だけに基づいて転送されます。トンネル ポートを含むスイッチ仮想インターフェイス (SVI) でルーティングがイネーブルである場合、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 アクセス コントロール リスト (ACL) がサポートされません。
- レイヤ 3 の Quality of Service (QoS) ACL およびレイヤ 3 情報に関連する他の QoS 機能は、トンネル ポートではサポートされていません。MAC ベース QoS はトンネル ポートで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。
- ポート集約プロトコル (PAgP)、Link Aggregation Control Protocol (LACP)、UniDirectional Link Detection (UDLD; 単一方向リンク検出) は、IEEE 802.1Q トンネル 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、ダイナミック トランッキング プロトコル (DTP) には IEEE 802.1Q トンネリングとの互換性はありません。
- 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、スパニングツリー ブリッジ プロトコル データ ユニット (BPDU) 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) は、インターフェイスで自動的にディセーブルに設定されます。

## 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。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 ~ 64) 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 dot1q-tunnel</code>	スイッチ上のトンネル 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。

以下は、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、さまざまなサイトに散在するカスタマーは、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。Cisco Discovery Protocol (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。VLAN トランキンング プロトコル (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 プロトコル データ ユニット (PDU) 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 を適切に実行できます。また、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。

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 トンネリングを向上させることができます。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分離されます。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 14-4 の場合、カスタマー X には、サービスプロバイダー ネットワーク経由で接続された同じ VLAN 上のスイッチが 4 つあります。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、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ンニングツリーを構築します。そのトポロジを図 14-5 に示します。



図 14-4 レイヤ 2 プロトコル トンネリング

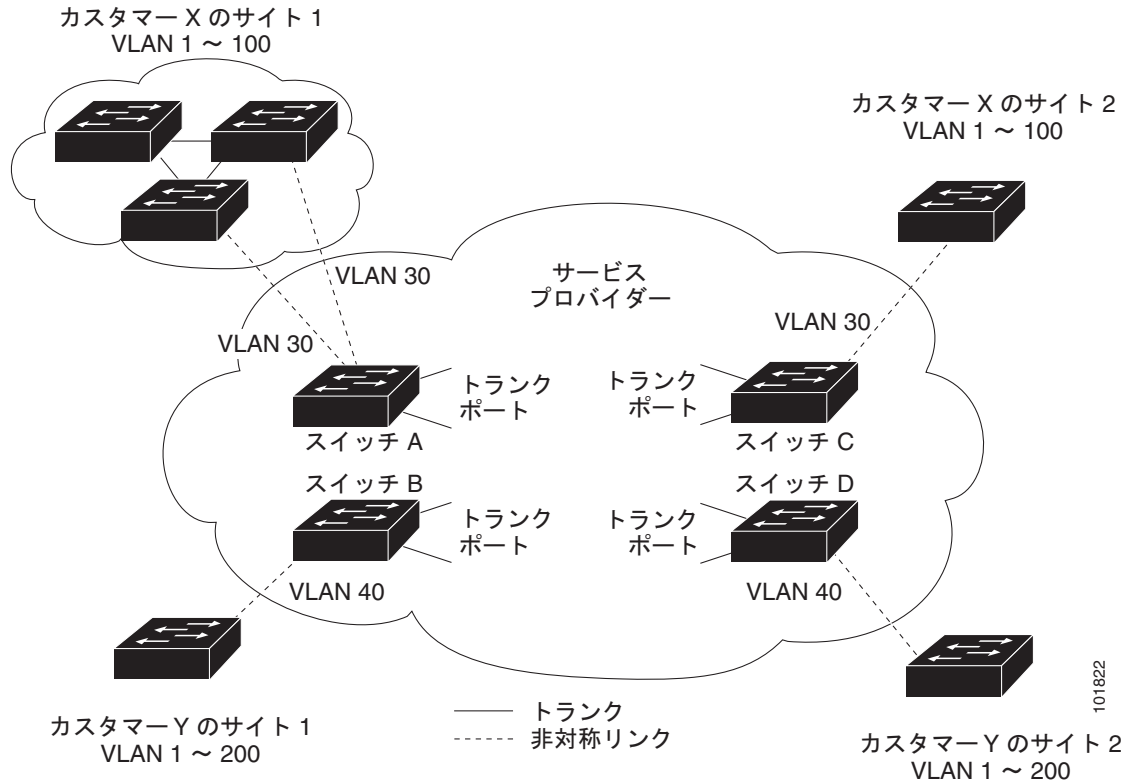
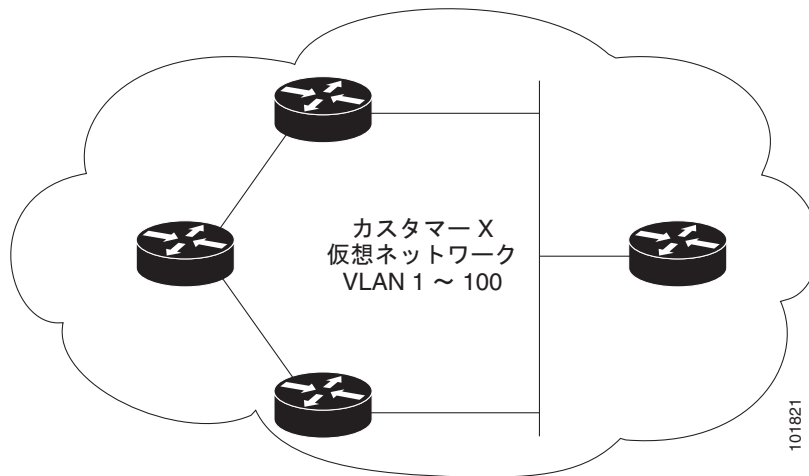


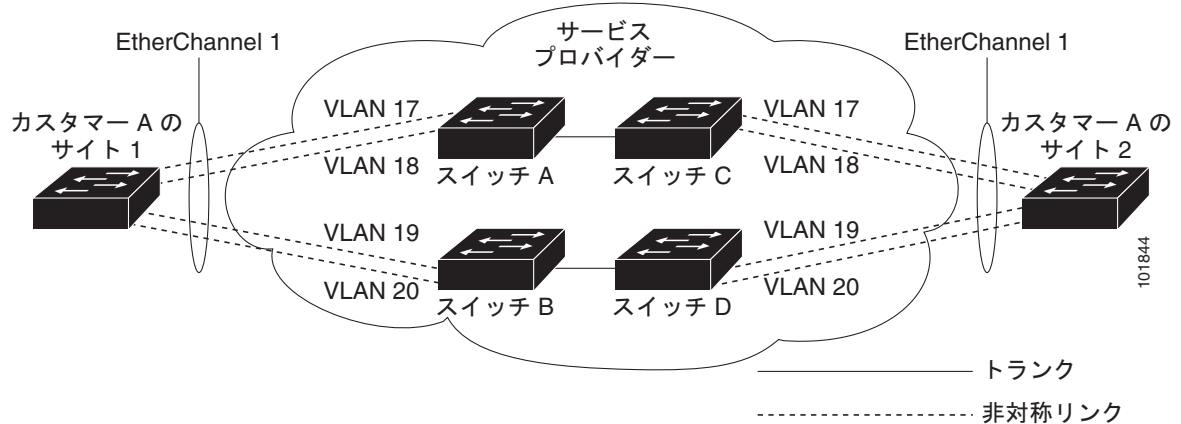
図 14-5 適切なコンバージェンスを含まないレイヤ 2 ネットワーク トポロジ



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、ポイントツーポイント ネットワーク トポロジをエミュレートして、EtherChannel の作成を向上させることができます。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、リモート顧客 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 14-6 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、EtherChannel の自動作成をネゴシエーションできます。EtherChannel のレイヤ 2 プロトコル トンネリングの設定については「EtherChannel のレイヤ 2 トンネリングの設定」(P.14-14) を参照してください。

図 14-6 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のカスタマーに接続されたアクセスポートまたはトンネルポートで、レイヤ 2 プロトコル トンネリング (プロトコルを使用) を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。

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。



### 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。設定を間違えたことによりトンネリング パケットが多くのポートに送信されると、ネットワーク障害が発生する可能性があります。

トンネルポートまたはアクセスポートを介して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、トランクポートを介してサービスプロバイダー ネットワークに入ると、スイッチは、カスタマー PDU 宛先 MAC アドレスをシスコ独自の well-known マルチキャストアドレス (01-00-0c-cd-cd-d0) で上書きします。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。したがって、レイヤ 2 PDU は完全な状態のまま保持され、サービスプロバイダー ネットワークを介してカスタマー ネットワークの反対側に配信されます。

図 14-4 を参照してください。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、および VLAN 100 などの内部 VLAN タグが付いています。二重タグ付きパケットがスイッチ D に着信すると、メトロ VLAN タグ 40 は削除されます。既知の MAC アドレスは各レイヤ 2 プロトコル MAC アドレスに置き換わり、パケットは VLAN 100 の一重タグ付き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に接続されたエッジスイッチのアクセスポートで、レイヤ 2 プロトコル トンネリングをイネーブルにすることもできます。この場合、カプセル化とカプセル化解除のプロセスは、上記の説明と同じです。ただし、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付けされません。カスタマー固有のアクセス VLAN タグの 1 重タグになります。

ここでは、レイヤ 2 プロトコル トンネリングの設定手順を説明します。具体的な内容は次のとおりです。

- 「レイヤ 2 プロトコル トンネリングのデフォルト設定」 (P.14-11)
- 「レイヤ 2 プロトコル トンネリング設定時の注意事項」 (P.14-11)
- 「レイヤ 2 トンネリングの設定」 (P.14-12)
- 「EtherChannel のレイヤ 2 トンネリングの設定」 (P.14-14)

## レイヤ 2 プロトコル トンネリングのデフォルト設定

表 14-1 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 14-1 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	データ パケット用のインターフェイスに CoS 値が設定されている場合は、その値がレイヤ 2 PDU に使用されるデフォルトです。設定されていない場合、デフォルトは 5 です。

## レイヤ 2 プロトコル トンネリング設定時の注意事項

以下は、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、CDP、STP (Multiple STP (MSTP) を含む)、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。
- トンネリングは、トランクポートではサポートされません。トランクポート上で **l2protocol-tunnel** インターフェイス コンフィギュレーション コマンドを入力した場合、コマンドは許可されますが、ポートをトンネルポートまたはアクセスポートに変更するまで、レイヤ 2 トンネリングが有効になりません。

## ■ レイヤ 2 プロトコル トンネリングの設定

- 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ことを推奨します。
- 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。制限を超えると、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。制限を超えると、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 がドロップされます。
- トンネリングされた PDU (特に 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 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	<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、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 ~ 64) に設定できます。

	コマンド	目的
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。  (注) 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の値は、ドロップしきい値の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ドロップされます。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、ドロップしきい値の値は、シャットダウンしきい値の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。

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。

以下は、CDP、STP、VTP のレイヤ 2 プロトコル トンネリングを設定し、設定を確認する方法の例です。

```
Switch(config)# interface FastEthernet0/11
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)# l2protocol-tunnel stp
```

## ■ レイヤ 2 プロトコル トンネリングの設定

```

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。
ステップ 4	<b>l2protocol-tunnel point-to-point</b> <b>[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。
		 <p><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。</p>

コマンド	目的
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の値は、ドロップしきい値の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ドロップされます。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、ドロップしきい値の値は、シャットダウンしきい値の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	<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	<b>switchport trunk encapsulation dot1q</b>	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	<b>switchport mode trunk</b>	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	<b>udld enable</b>	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	<b>channel-group channel-group-number mode desirable</b>	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 30 章「EtherChannel の設定」</a> を参照してください。
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>interface port-channel port-channel number</b>	ポートチャンネル インターフェイス モードを開始します。
ステップ 9	<b>shutdown</b>	インターフェイスをシャットダウンします。
ステップ 10	<b>no shutdown</b>	インターフェイスをイネーブルにします。
ステップ 11	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 12	<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 13	<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。

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 14-6 (P.14-10) を参照)。

以下は、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 を設定する方法の例です。VLAN 17、18、19、20 はアクセス VLAN であり、ファスト イーサネット インターフェイス 0/1 および 0/2 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 ポートであり、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 0/3 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
```

次は、サイト 1 のカスタマー スイッチを設定する方法の例です。ファストイーサネット インターフェイス 0/1、0/2、0/3、0/4 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って 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リングおよびメンテナンス

表 14-2 は、IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングのモニタリングとメンテナンスを行う特権 EXEC コマンドの説明です。

表 14-2 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 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、このリリースに対応するコマンド リファレンスを参照してください。