



CHAPTER 21

802.1Q 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; 仮想プライベート ネットワーク) は、共有インフラストラクチャ (通常はイーサネットベース) 上で、私設網と同じセキュリティ、プライオリティ、信頼性、および管理性を持つ企業規模の接続を提供します。トンネリングは、ネットワークで複数のカスタマーのトラフィックを伝送するサービス プロバイダーを対象に設計された機能です。このようなサービス プロバイダーは、各カスタマーの VLAN およびレイヤ 2 プロトコル設定を他のカスタマーのトラフィックに影響を与えずに維持する必要があります。Catalyst 4500 シリーズ スイッチは、IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングをサポートしています。



(注) 802.1Q には Cisco Catalyst 4948、Cisco Catalyst 4948-10GE、または Catalyst 4500 シリーズ スイッチ スーパーバイザ エンジン II-Plus-10GE V または V-10GE が必要であることに注意してください。レイヤ 2 プロトコル トンネリングは、すべてのスーパーバイザ エンジン上でサポートされます。

この章の内容は次のとおりです。

- 「802.1Q トンネリングの概要」 (P.21-1)
- 「802.1Q トンネリングの設定」 (P.21-3)
- 「レイヤ 2 プロトコル トンネリングの概要」 (P.21-7)
- 「レイヤ 2 プロトコル トンネリングの設定」 (P.21-9)
- 「トンネリング ステータスの監視およびメンテナンス」 (P.21-13)



(注) この章で使用するスイッチ コマンドの構文および使用方法の詳細については、『Catalyst 4500 Series Switch Cisco IOS Command Reference』および次の URL の関連マニュアルを参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm>

802.1Q トンネリングの概要

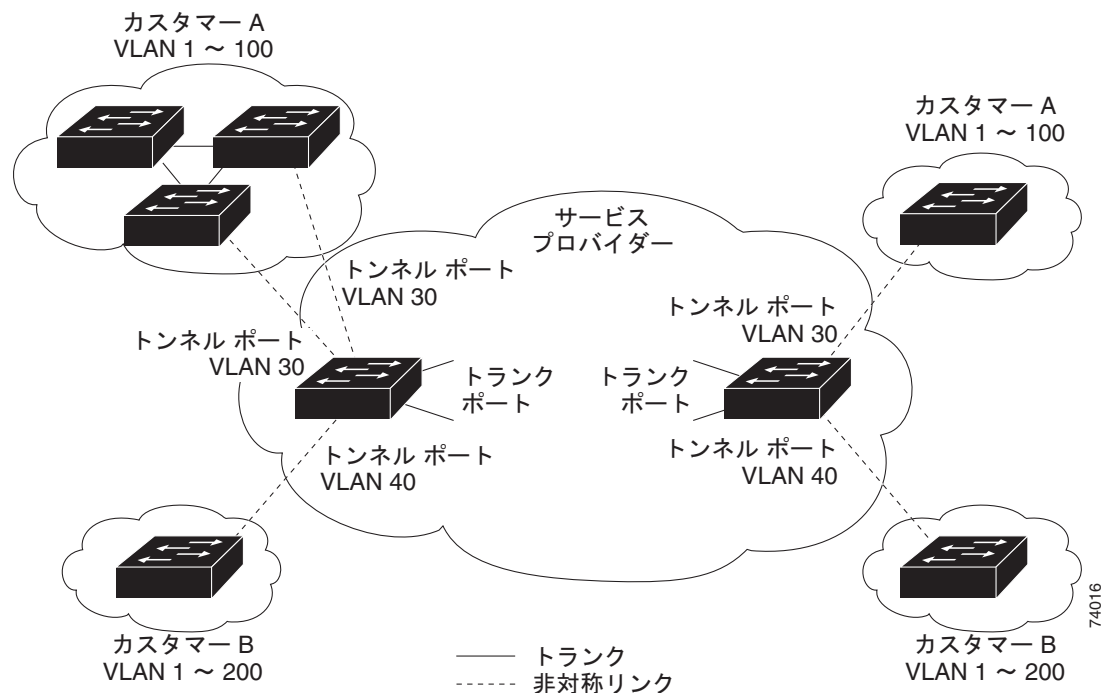
同じサービス プロバイダー ネットワーク内の各カスタマーが要求する VLAN 範囲は重複する場合があります。インフラストラクチャを経由するカスタマー トラフィックが混合する場合があります。カスタマーごとに一意の VLAN ID 範囲を割り当てると、カスタマーの設定が制限され、802.1Q 仕様の VLAN に関する上限 (4096 個) を容易に超えてしまいます。

802.1Q トンネリングを使用すると、サービス プロバイダーは単一の VLAN を使用して、複数の VLAN を持つ顧客をサポートできます。このときに、顧客の VLAN ID は保護され、各顧客 VLAN のトラフィックは分離されます。

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を、トンネル ポートといいます。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。顧客ごとに個別のサービス プロバイダー VLAN ID が必要ですが、その VLAN ID はすべての顧客の VLAN をサポートします。

対応する VLAN ID を使用して通常の方法で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 ポートから送信されて、サービス プロバイダー エッジ スイッチのトンネル ポートに着信します。顧客 デバイスとエッジ スイッチ間のリンクは、非対称リンクです。これは、リンクの一端が 802.1Q トランク ポートとして設定されているのに対し、もう一端はトンネル ポートとして設定されているためです。トンネル ポート インターフェイスに、顧客ごとに一意のアクセス VLAN ID を割り当てます。図 21-1 を参照してください。

図 21-1 サービス プロバイダー ネットワークの 802.1Q トンネル ポート

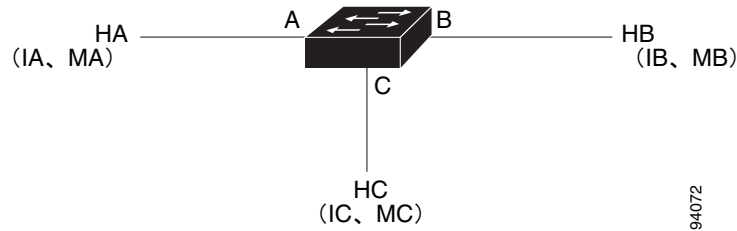


顧客 トランク ポートからサービス プロバイダー エッジ スイッチのトンネル ポートに着信するパケットは、該当する VLAN ID を使用して通常の方法で 802.1Q がタグ付けされます。トランク ポートからサービス プロバイダー ネットワークに送信されたタグ付きパケットは、顧客ごとに一意の VLAN ID を含む別のレイヤの 802.1Q タグ (メトロ タグ) でカプセル化されています。元の顧客 802.1Q タグは、カプセル化されたパケット内に保存されます。したがって、サービス プロバイダー ネットワークに入るパケットは二重にタグ付けされます。メトロ タグには顧客のアクセス VLAN ID が格納され、内側のタグには着信トラフィックの VLAN となる VLAN ID が格納されます。

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。同じコア スイッチ上の別のトランク ポートからパケットが送信される際に、パケットには同じメトロ タグが再び追加されます。

図 21-2 に、元の (通常の) 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 21-2 元の（通常の）802.1Q、および二重タグ付きイーサネット パケット形式



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送信されて、カスタマーのネットワークに入るときは、メトロ タグが追加されません。パケットは通常の 802.1Q タグ付きフレームとして送信され、カスタマーのネットワーク内にある元の VLAN 番号は保存されます。

エッジ スイッチのトンネル ポートを通じてサービス プロバイダー ネットワークに入るパケットは、タグなしの場合も、802.1Q ヘッダーがタグ付けされている場合も、すべてタグなしパケットとして取り扱われます。これらのパケットは、802.1Q トランク ポートのサービス プロバイダー ネットワークを通じて送信される際に、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 ポートのインターフェイス Class of Service (CoS; サービス クラス) プライオリティに設定されています（未設定の場合のデフォルトは 0 です）。

図 21-1 では、カスタマー A には VLAN 30 が、カスタマー B には VLAN 40 が割り当てられています。サービス プロバイダー ネットワークに入って、エッジ スイッチのトンネル ポートに着信する 802.1Q タグ付きパケットは、二重タグ付きになります。この場合、メトロ タグには VLAN ID 30 または 40 が格納され、内側のタグには元のカスタマー VLAN 番号（VLAN 100 など）が格納されています。カスタマー A とカスタマー B の両方にネットワーク内で VLAN 100 が設定されている場合でも、メトロ タグが異なるため、トラフィックはサービス プロバイダー ネットワーク内で分離されたままです。各カスタマーは独自の VLAN 番号スペースを制御します。これは、他のカスタマーが使用する VLAN 番号スペースや、サービス プロバイダー ネットワークが使用する VLAN 番号スペースとは無関係です。

802.1Q トンネリングの設定

ここでは、802.1Q トンネリングの設定について説明します。

- ・「802.1Q トンネリングの設定時の注意事項」(P.21-3)
- ・「802.1Q トンネリングおよび他の機能」(P.21-5)
- ・「802.1Q トンネル ポートの設定」(P.21-6)



(注)

デフォルトのスイッチポート モードが dynamic auto であるため、802.1Q トンネリングはデフォルトでディセーブルです。802.1Q ネイティブ VLAN パケットのタグgingも、すべての 802.1Q トランク ポートでディセーブルです。

802.1Q トンネリングの設定時の注意事項

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 Maximum Transmission Unit (MTU; 最大伝送ユニット) 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.21-5) を参照してください。

ネイティブ VLAN

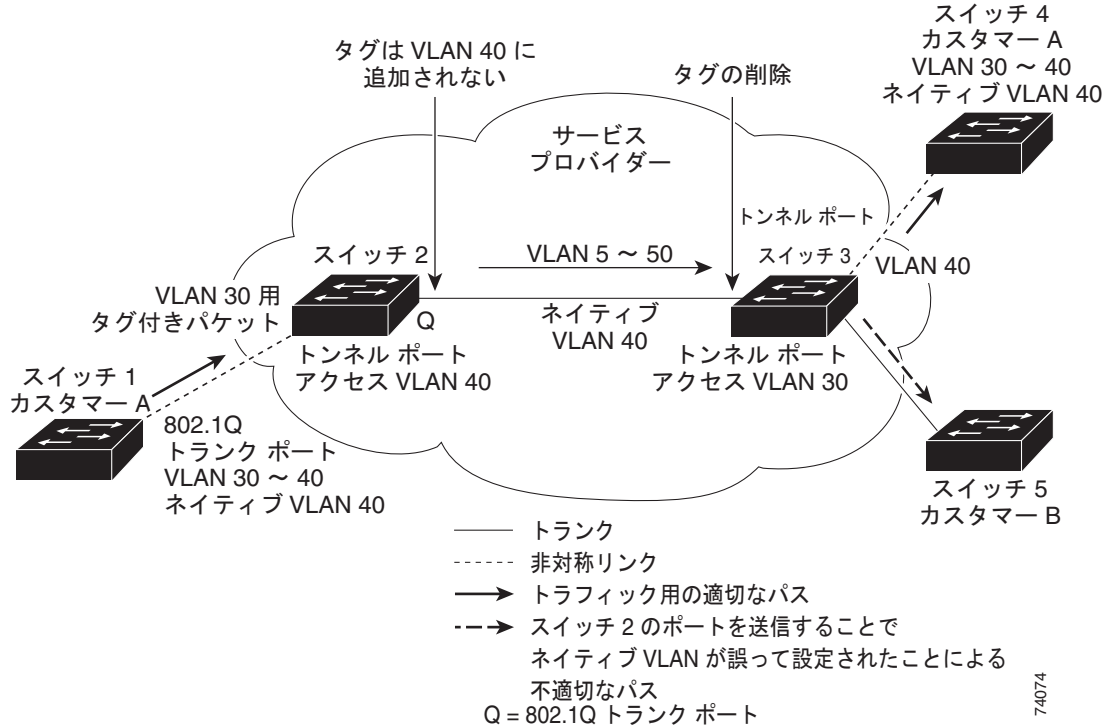
エッジスイッチ上に 802.1Q トンネリングを設定する場合は、サービスプロバイダーネットワークへのパケット送信に 802.1Q トランクポートを使用する必要があります。ただし、サービスプロバイダーネットワークのコアを通過するパケットは、802.1Q トランク、ISL トランク、または非トランクリンクを通じて伝送されることがあります。802.1Q トランクをこれらのコアスイッチで使用する場合には、802.1Q トランクのネイティブ VLAN を、同じスイッチ上の非トランク (トンネリング) ポートのどのネイティブ VLAN にも一致させないでください。ネイティブ VLAN 上のトラフィックが 802.1Q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

図 21-3 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 (スイッチ 2) の入力エッジスイッチで、カスタマー A 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 A のスイッチ 1 は、タグ付きパケットを VLAN 30 から、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内のスイッチ 2 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 トランクポートのネイティブ VLAN (VLAN 40) と同じなので、メトロタグはトンネルポートから受信したタグ付きパケットに追加されません。パケットは、サービスプロバイダーネットワークを通じて VLAN 30 タグだけを出力エッジスイッチ (スイッチ 3) のトランクポートに伝送し、出力スイッチ トンネルポートを通じてカスタマー B に誤って転送してしまいます。

この問題の解決には、次のような方法があります。

- 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したカスタマーインターフェイスは 802.1Q トランクに設定する必要がありますが、コアレイヤ内のスイッチの接続には ISL トランクを使用することを推奨します。
- ネイティブ VLAN を含め、802.1Q トランクから送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するには、**switchport trunk native vlan tag** ポート単位コマンドおよび **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。すべての 802.1Q トランクでネイティブ VLAN パケットにタグ付けするようにスイッチを設定すると、スイッチは、トランクから送信されるパケットすべてにタグ付けされているか確認し、トランクポート上でタグのないパケットを受信しません。
- エッジスイッチ トランクポートのネイティブ VLAN ID がカスタマー VLAN の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 VLAN 100 ~ 200 のトラフィックを伝送する場合は、ネイティブ VLAN にはその範囲外の番号を割り当てます。

図 21-3 802.1Q トンネリングとネイティブ VLAN で予想される問題



システム MTU

Catalyst 4500 シリーズ スイッチ上のトラフィックに対するデフォルトのシステム 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。メトロ タグが追加されたときに、802.1Q トンネリング機能によってフレーム サイズが 4 バイト増えるので、スイッチのシステム MTU サイズを 1504 バイト以上に増やして、サービス プロバイダー ネットワーク内のすべてのスイッチがより大きなフレームを処理できるように設定する必要があります。Catalyst 4500GigabitEthernet スイッチの最大許容システム MTU は、9198 バイトです。FastEthernet スイッチの最大システム MTU は、1552 バイトです。

802.1Q トンネリングおよび他の機能

802.1Q トンネリングは、レイヤ 2 パケット スイッチングに対して適切に機能しますが、レイヤ 2 機能とレイヤ 3 スイッチングとは一部互換性がありません。

- トンネルポートはルーテッドポートにできません。
- IP ルーティングは、802.1Q ポートを含む VLAN ではサポートされません。トンネルポートから受信されたパケットは、レイヤ 2 情報にだけ基づいて転送されます。トンネルポートを含む Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) 上でルーティングがイネーブルの場合は、トンネルポートから受信したタグなし IP パケットがスイッチによって認識され、ルーティングされます。カスタマーはネイティブ VLAN を介して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 に SVI を設定しないでください。
- トンネルポートは、IP Access Control List (ACL; アクセスコントロールリスト) をサポートしません。

802.1Q トンネリングの設定

- レイヤ 3 QoS (Quality Of Service) ACL およびレイヤ 3 に関連するその他の QoS 機能の情報は、トンネル ポートでサポートされません。トンネル ポートでは、MAC ベースの QoS はサポートされません。
- EtherChannel ポート グループは、802.1Q 設定が EtherChannel ポート グループ内で一貫しているかぎりは、トンネル ポートと互換性があります。
- 802.1Q トンネル ポートでは、Port Aggregation Protocol (PAgP)、Link Aggregation Control Protocol (LACP)、および UniDirectional Link Detection (UDLD; 単一方向リンク検出) がサポートされます。
- Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル) は、802.1Q トンネリングと互換性がありません。これは、トンネル ポートおよびトランク ポートとの非対称リンクを手動で設定しなければならないためです。
- ループバック検出は、802.1Q トンネル ポートでサポートされています。
- 802.1Q トンネル ポートとしてポートが設定されている場合、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) フィルタリングは、インターフェイスで自動的にイネーブルに設定されます。Cisco Discovery Protocol (CDP; シスコ検出プロトコル) 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。

802.1Q トンネル ポートの設定

ポートを 802.1Q トンネル ポートとして設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	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)# interface interface-id	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。このインターフェイスは、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とポート チャネル論理インターフェイス (ポート チャネル 1 ~ 64) があります。
ステップ 3	Switch(config-if)# switchport access vlan vlan-id	インターフェイスがトランキングを停止した場合に使用されるデフォルト VLAN を指定します。この VLAN ID は、特定の顧客に対して固有です。
ステップ 4	Switch(config-if)# switchport mode dot1q-tunnel	インターフェイスを 802.1Q トンネル ポートとして設定します。
ステップ 5	Switch(config-if)# exit	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 6	Switch(config)# vlan dot1q tag native	(任意) すべての 802.1Q トランク ポートでネイティブ VLAN パケットのタグングがイネーブルとなるようにスイッチを設定します。このように設定されていない場合、カスタマー VLAN ID がネイティブ VLAN と同じときは、トランク ポートはメトロ タグを適用せず、パケットが誤った宛先に送信されることがあります。
ステップ 7	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 8	Switch# show dot1q-tunnel	スイッチ上のトンネル ポートを表示します。
ステップ 9	Switch# show vlan dot1q tag native	802.1Q ネイティブ VLAN タグング ステータスを表示します。
ステップ 10	Switch# copy running-config startup-config	(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。

ポートを `dynamic auto` のデフォルト ステートに戻すには、`no vlan dot1q tag native` グローバル コマンドおよび `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ging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。

次に、インターフェイスをトンネル ポートとして設定し、ネイティブ VLAN パケットのタグgingをイネーブルにして、設定を確認する方法を示します。この設定では、インターフェイス GigabitEthernet 2/7 に接続しているカスタマーの VLAN ID は VLAN 22 です。

```
Switch(config)# interface gigabitethernet2/7
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 gigabitethernet2/7
Port
-----
LAN Port(s)
-----
Gi2/7
Switch# show vlan dot1q tag native
dot1q native vlan tagging is enabled globally
```

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 ネットワークを通して接続された各サイトのカスタマーは、各種のレイヤ 2 プロトコルを使用してトポロジを拡張し、すべてのリモート サイトおよびローカル サイトを組み込む必要があります。STP が正常に実行され、すべての VLAN で、サービス プロバイダー ネットワークを通してローカル サイトおよびすべてのリモート サイトを組み込んだ適切なスパンニング ツリーを構築する必要があります。Cisco Discovery Protocol (CDP; シスコ検出プロトコル) は、ローカルおよびリモート サイトから近接するシスコ製デバイスを検出する必要があります。VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) は、カスタマー ネットワークのすべてのサイトに一貫した 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になると、サービス プロバイダー ネットワークの着信側のエッジ スイッチは、特殊 MAC アドレスでレイヤ 2 プロトコル パケットをカプセル化し、サービス プロバイダー ネットワークに送信します。ネットワークのコア スイッチはこれらパケットを処理しないで、通常パケットとして転送します。CDP、STP、または VTP 用のレイヤ 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 スイッチに配信されます。同じ VLAN 上のすべてのカスタマー ポートで同じパケットが受信され、次のような結果となります。

- 各カスタマー サイトのユーザは、正常に STP を実行できます。また、すべての VLAN は、ローカル サイトからだけでなくすべてのサイトのパラメータに基づいて、正しいスパンニング ツリーを構築できます。
- CDP は、サービス プロバイダー ネットワークを介して接続した他のシスコ製デバイスに関する情報を検出して、表示します。
- VTP は、サービス プロバイダーを通じてすべてのスイッチに VLAN 設定を伝播し、カスタマー ネットワーク全体で統一します。

レイヤ 2 プロトコル トンネリングは、トランク、アクセス、およびトンネル ポートでイネーブルにすることができます。プロトコル トンネリングがイネーブルでない場合、サービス プロバイダー ネットワークの受信側にあるリモート スイッチは PDU を受信せず、STP、CDP、および VTP を正常に実行

できません。プロトコル トンネリングがイネーブルの場合、各カスタマー 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 ネットワーク内で稼働しているプロトコルとは全面的に切り離されます。

たとえば、[図 21-4](#) では、カスタマー A 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 つのスイッチを持っています。ネットワークが PDU をトンネリングしない場合、ネットワークの遠端のスイッチは STP、CDP、および VTP を正常に実行できません。たとえば、カスタマー A のサイト 1 にあるスイッチ上の VLAN に対する STP は、サイト 2 にあるカスタマー A のスイッチに基づくコンバージェンス パラメータを考慮しないで、そのサイトにあるスイッチ上にスパンニング ツリーを構築します。[図 21-5](#) に、スパンニング ツリー トポロジの一例を示します。

図 21-4 レイヤ 2 プロトコル トンネリング

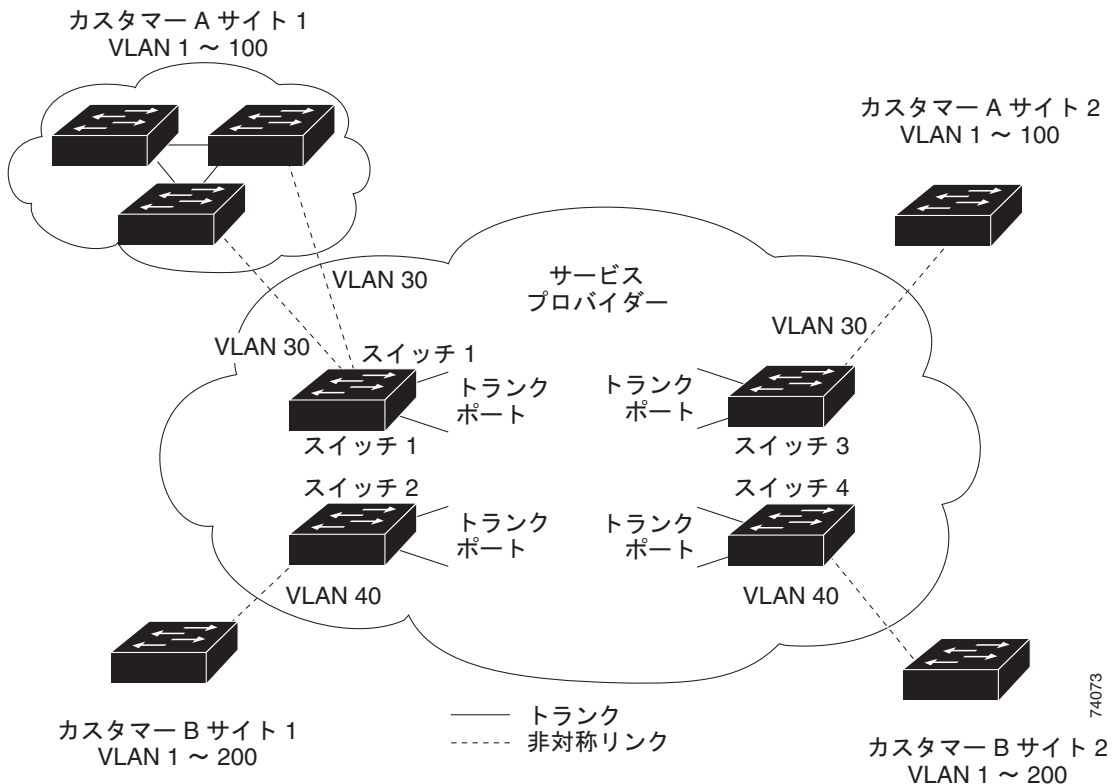
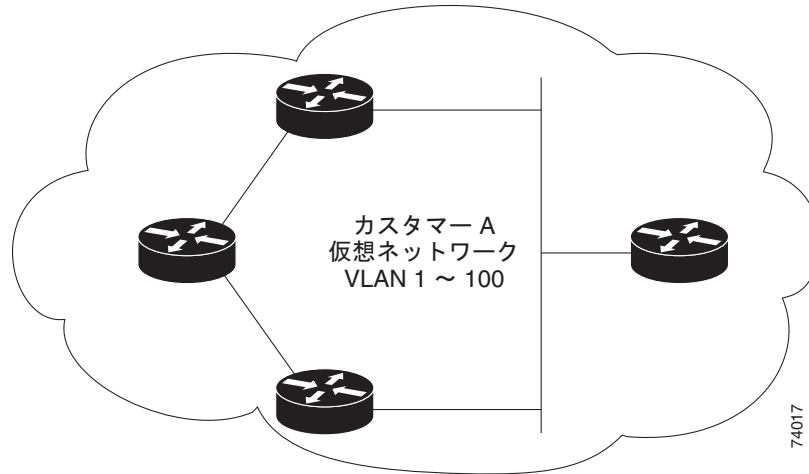


図 21-5 コンバージェンスが不適切なレイヤ 2 ネットワーク トポロジ



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顧客に接続されたアクセス ポート、トンネル ポート、またはトランク 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。顧客 スイッチに接続されたサービス プロバイダーのエッジスイッチは、トンネリング プロセスを実行します。エッジスイッチのトンネル ポートまたは通常のトンネル ポートは、顧客の 802.1Q トランク ポートに接続できます。エッジスイッチのアクセス ポートは、顧客のアクセス ポートに接続されます。

サービス プロバイダーの着信エッジスイッチ ポートに入ったレイヤ 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、顧客 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。802.1Q トンネリングが入力ポートでイネーブルの場合、パケットも二重タグ付きです。外側のタグは顧客のメトロ タグで、内側のタグは顧客の VLAN タグです。

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、顧客 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。ここで、802.1Q トンネリングがイネーブルの場合、パケットは二重タグ付きです。外側のタグは顧客のメトロ タグで、内側のタグは顧客の VLAN タグです。コア スイッチは内側のタグを無視して、同じメトロ VLAN のすべてのトランク ポートにパケットを転送します。発信側のエッジスイッチは、正しいレイヤ 2 プロトコルと MAC アドレス情報を復元して、同じメトロ VLAN のすべてのトンネル ポートまたはアクセス ポートにパケットを転送します。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顧客 ネットワークの反対側に配信されます。

図 21-4 を参照してください。顧客 A と顧客 B は、それぞれアクセス VLAN 30 と 40 内にあります。非対称リンクは、サイト 1 の顧客をサービス プロバイダー ネットワークのエッジスイッチに接続します。サイト 1 の顧客 B からスイッチ 2 に着信するレイヤ 2 PDU (BPDU など) は、宛先 MAC アドレスとして well-known MAC アドレスを持つ二重タグ付きパケットとしてインフラストラクチャに転送されます。この二重タグ付きパケットは、内側の VLAN タグ (VLAN 100 など) だけでなく、メトロ VLAN タグ (40) も備えています。二重タグ付きパケットがスイッチ 4 に着信すると、メトロ VLAN タグ 40 は削除されます。well-known 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 の顧客 B 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。一重タグは、カスタマー固有のアクセス VLAN タグです。

ここでは、次の内容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.21-10)
- 「レイヤ 2 プロトコル トンネリングの設定時の注意事項」(P.21-10)
- 「レイヤ 2 トンネリングの設定」(P.21-11)

レイヤ 2 プロトコル トンネリングのデフォルト設定

表 21-1 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 21-1 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	デフォルト設定値
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。未設定の場合、デフォルトは 5 です。

レイヤ 2 プロトコル トンネリングの設定時の注意事項

ここでは、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について説明します。

- スイッチは、CDP、Multiple STP (MSTP) を含めた STP、および VTP のトンネリングをサポートします。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設定されていますが、802.1Q トンネル ポート、アクセス ポート、またはトランク ポート上でプロトコルごとにイネーブルにできます。
- 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。これは、トンネル ポートおよびトランク ポートとの非対称リンクを手動で設定しなければならないためです。
- 802.1Q 設定が EtherChannel ポート グループ内で一貫している場合、EtherChannel ポート グループはトンネル ポートと互換性があります。
- レイヤ 2 トンネリングがイネーブルに設定されたポートでカプセル化 PDU (独自の宛先 MAC アドレス付き) を受信した場合は、ループを防止するためポートはシャットダウンされます。
- プロトコルに設定されたシャットダウンしきい値に達した場合も、ポートはシャットダウンされません。ポートは手動で再びイネーブルにできます (shutdown および no shutdown コマンドを続けて入力します)。エラーディセーブル回復がイネーブルの場合は、指定インターバル後に処理が再試行されます。
- 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 ネットワーク上で稼動するスパンニング ツリー インスタンスは、レイヤ 2 プロトコル トンネリング ポートに BPDU を転送しません。CDP パケットはレイヤ 2 プロトコル トンネリング 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の場合は、カスタマー ネットワークによって生成された PDU に対して、プロトコル単位、ポート単位でシャットダウンしきい値を設定できます。上限を超過すると、ポートはシャットダウンします。レイヤ 2 プロトコル トンネリング ポートに QoS ACL およびポリシー マップを使用して、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の場合は、カスタマー ネットワークによって生成された PDU に対して、プロトコル単位、ポート単位でドロップしきい値を設定できます。限度を超過した場合は、受信レートがドロップしきい値を下回るまで、PDU はドロップされます。
- カスタマーの仮想ネットワークが正常に動作するように、トンネリングされた PDU (特に STP BPDU) をすべてのリモート サイトに配信する必要がありますので、サービス プロバイダー ネットワーク内の PDU には、同じトンネル ポートで受信したデータ パケットより高いプライオリティを設定してください。デフォルトでは、PDU はデータ パケットと同じ CoS 値を使用します。

レイヤ 2 トンネリングの設定

特定のポートにレイヤ 2 プロトコル トンネリングを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	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)# interface interface-id	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。このインターフェイスは、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とポート チャネル論理インターフェイス (ポート チャネル 1 ~ 64) があります。
ステップ 3	Switch(config-if)# switchport mode access または Switch(config-if)# switchport mode dot1q-tunnel または Switch(config-if)# switchport mode trunk	インターフェイスをアクセス ポート、802.1Q トンネル ポート、またはトランク ポートとして設定します。
ステップ 4	Switch(config-if)# l2protocol-tunnel [cdp stp vtp]	目的のプロトコルに対してプロトコル 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、トンネリングはすべてのレイヤ 2 プロトコルに対してイネーブルです。
ステップ 5	Switch(config-if)# l2protocol-tunnel shutdown-threshold [cdp stp vtp] value	(任意) 1 秒間にカプセル化可能なパケット数を表すしきい値を設定します。設定されたしきい値を超過すると、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、しきい値はトンネリングされた各レイヤ 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ていません。 (注) 現在のインターフェイスにドロップしきい値も設定する場合は、シャットダウンしきい値にドロップしきい値以上の値を指定する必要があります。

■ レイヤ 2 プロトコル トンネリングの設定

	コマンド	目的
ステップ 6	Switch(config-if)# l2protocol-tunnel drop-threshold [cdp stp vtp] value	(任意) 1 秒間にカプセル化可能なパケット数を表すしきい値を設定します。設定されたしきい値を超過すると、インターフェイスはパケットをドロップします。プロトコル オプションを指定しない場合、しきい値はトンネリングされた各レイヤ 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ていません。 (注) 現在のインターフェイスにシャットダウンしきい値も設定する場合は、ドロップしきい値にシャットダウンしきい値以下の値を指定する必要があります。
ステップ 7	Switch(config-if)# exit	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	Switch(config)# errdisable recovery cause l2ptguard	(任意) レイヤ 2 最大レート エラーからの復旧メカニズムを設定して、インターフェイスが再びイネーブルになり、再試行できるようにします。エラーディセーブル回復はデフォルトでディセーブルに設定されています。イネーブルにした場合、デフォルトのタイム インターバルは 300 秒です。
ステップ 9	Switch(config)# l2protocol-tunnel cos value	(任意) トンネリングされたすべてのレイヤ 2 PDU に対して CoS 値を設定します。指定できる範囲は 0 ~ 7 です。デフォルトは、インターフェイスのデフォルトの CoS 値です。未設定の場合、デフォルトは 5 です。
ステップ 10	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 11	Switch# show l2protocol	設定済みのプロトコル、しきい値、カウンタも含めてスイッチのレイヤ 2 トンネル ポートを表示します。
ステップ 12	Switch# copy running-config startup-config	(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。

3 つのレイヤ 2 プロトコルのいずれか、またはすべてに対してプロトコル 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]** および **no l2protocol-tunnel drop-threshold [cdp | stp | vtp]** コマンドを使用します。

次に、802.1Q トンネル ポートに CDP、STP、および VTP のレイヤ 2 プロトコル トンネリングを設定し、その設定を確認する例を示します。

```
Switch(config)# interface FastEthernet2/1
Switch(config-if)# switchport mode dot1q-tunnel
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
-----
Fa2/11   cdp          1500    1000 2288          2282          0
          stp          1500    1000  116           13            0
          vtp          1500    1000   3             67            0
```

トンネリング ステータスの監視およびメンテナンス

表 21-2 に、802.1Q およびレイヤ 2 プロトコル トンネリングを監視およびメンテナンスするためのコマンドを示します。

表 21-2 トンネリングを監視およびメンテナンスするためのコマンド

コマンド	目的
Switch# <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。
Switch# <code>show dot1q-tunnel</code>	スイッチの 802.1Q トンネル ポートを表示します。
Switch# <code>show dot1q-tunnel interface interface-id</code>	特定の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。
Switch# <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。
Switch# <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 ステートの回復タイマーがイネーブルかどうかを確認します。
Switch# <code>show l2protocol-tunnel interface interface-id</code>	特定のレイヤ 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。
Switch# <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。
Switch# <code>show vlan dot1q native</code>	スイッチのネイティブ VLAN タギングのステータスを表示します。



(注) Cisco IOS リリース 12.2(20)EW では、dot1q およびレイヤ 2 プロトコル トンネリング用の BPDU フィルタリング設定は、実行コンフィギュレーションで「`spanning-tree bpdupfilter enable`」として表示されません。代わりに、**show spanning tree int detail** コマンドの出力に表示されます（次を参照）。

```
Switch# show spann int f6/1 detail
Port 321 (FastEthernet6/1) of VLAN0001 is listening
  Port path cost 19, Port priority 128, Port Identifier 128.321.
  Designated root has priority 32768, address 0008.e341.4600
  Designated bridge has priority 32768, address 0008.e341.4600
  Designated port id is 128.321, designated path cost 0
  Timers: message age 0, forward delay 2, hold 0
  Number of transitions to forwarding state: 0
  Link type is point-to-point by default
  ** Bpdu filter is enabled internally **
  BPDU: sent 0, received 0
```

■ トンネリング ステータスの監視およびメンテナンス