CHAPTER 22

802.1Q 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、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） Supervisor Engine 6-E は、レイヤ 2 プロトコル トンネリングをサポート*しません*。

（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。

この章で説明する内容は、次のとおりです。

（注） この章のスイッチ 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/en/US/products/ps6350/index.html

802.1Q トンネリングの概要

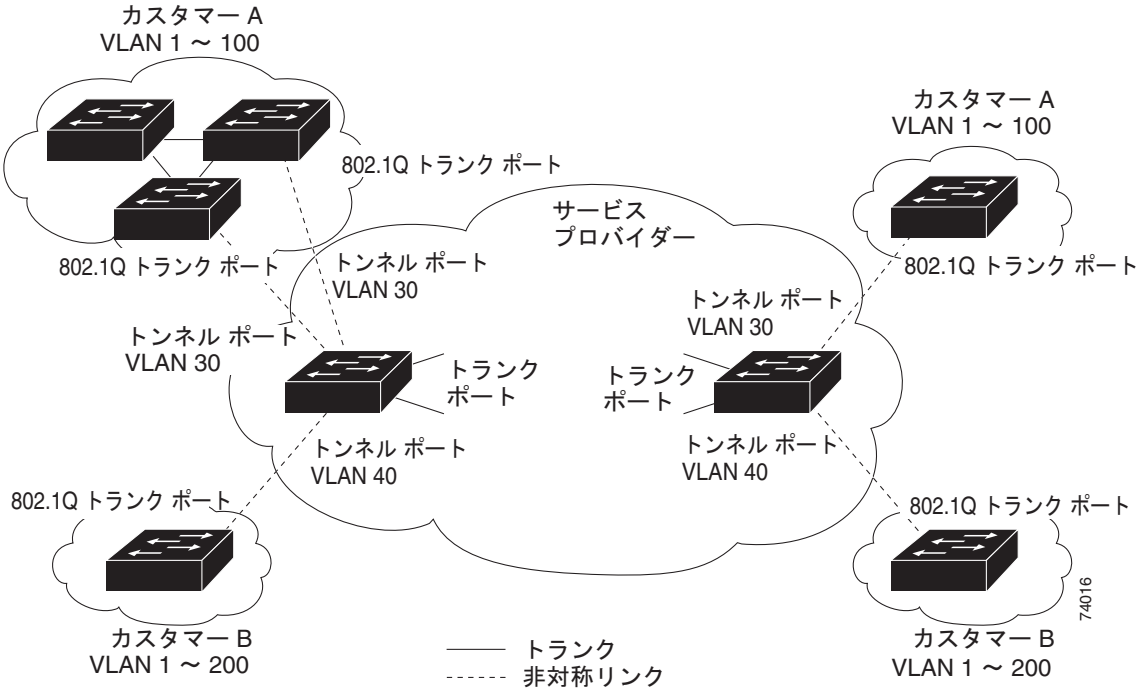
同じサービス プロバイダー ネットワーク内の各カスタマーが要求する VLAN 範囲は重複する場合があり、インフラストラクチャを経由するカスタマー トラフィックが混合する場合もあります。カスタマーごとに一意の VLAN ID 範囲を割り当てると、カスタマーの設定が制限され、802.1Q 仕様の VLAN に関する上限（4096 個）を容易に超えてしまいます。

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 を持つカスタマーをサポートできます。このときに、カスタマーの VLAN ID は保護され、各カスタマー 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。カスタマー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 はすべてのカスタマーの 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カスタマーのトラフィックは、カスタマー 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。カスタマー 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、カスタマーごとに一意のアクセス VLAN ID を割り当てます。図 22-1 を参照してください。

図 22-1　　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

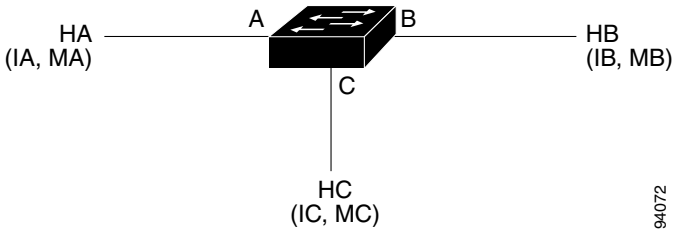


カスタマー トランク ポートからサービス プロバイダー エッジ スイッチのトンネル ポートに着信するパケットは、該当する VLAN ID を使用して通常の方法で 802.1Q がタグ付けされます。トランク ポートからサービス プロバイダー ネットワークに送信されたタグ付きパケットは、カスタマーごとに一意の VLAN ID を含む別のレイヤの 802.1Q タグ（*メトロ タグ*）でカプセル化されています。元のカスタ

マー 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 タグにはカスタマーのアクセス 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。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 22-2 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 22-2　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 ポートからカスタマー ネットワークに送信されるとき、メトロ タグは追加されません。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ときに、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）。

図 22-1 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。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.22-4）
- 「802.1Q トンネリングおよび他の機能」（P.22-5）
- 「802.1Q トンネル ポートの設定」（P.22-6）

（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 パケットのタギングも、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.22-5）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。

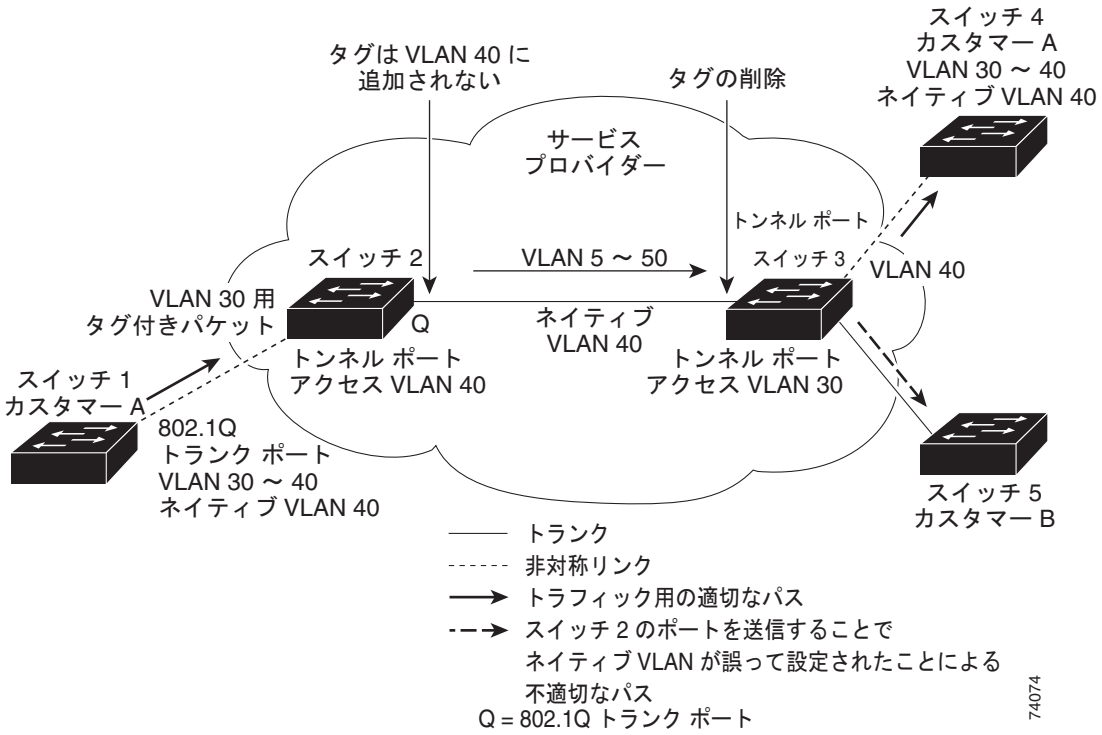
図 22-3 を参照してください。VLAN 40 は、サービス プロバイダー ネットワーク（スイッチ 2）の入力エッジ スイッチで、カスタマー A の 802.1Q トランク ポートのネイティブ VLAN として設定されています。カスタマー A のスイッチ 1 は、タグ付きパケットを VLAN 30 から、アクセス VLAN 40 に属するサービス プロバイダー ネットワーク内のスイッチ 2 の入力トンネル ポートに送信します。トンネル ポートのアクセス VLAN（VLAN 40）は、エッジ スイッチのトランク ポートのネイティブ VLAN（VLAN 40）と同じなので、トンネル ポートから受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 22-3　802.1Q 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 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 で SVI を設定しないでください。

- 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す。
- EtherChannel ポート グループは、802.1Q 設定が EtherChannel ポート グループ内で整合性がとれている限り、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、ポート集約プロトコル（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。
- ダイナミック トランキング プロトコル（DTP）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）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	`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 は特定カスタマーに固有です。
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 パケットのタギ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	`Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンド	目的
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 タギング 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、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

（注）　Supervisor Engine 6-E は、レイヤ 2 プロトコル トンネリングをサポート*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ニングツリーを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 用のレイヤ 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。

- 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 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 22-4 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 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ニングツリーを構築します。図 22-5 に、スパニングツリー トポロジの一例を示します。

図 22-4　　レイヤ 2 プロトコル トンネリング

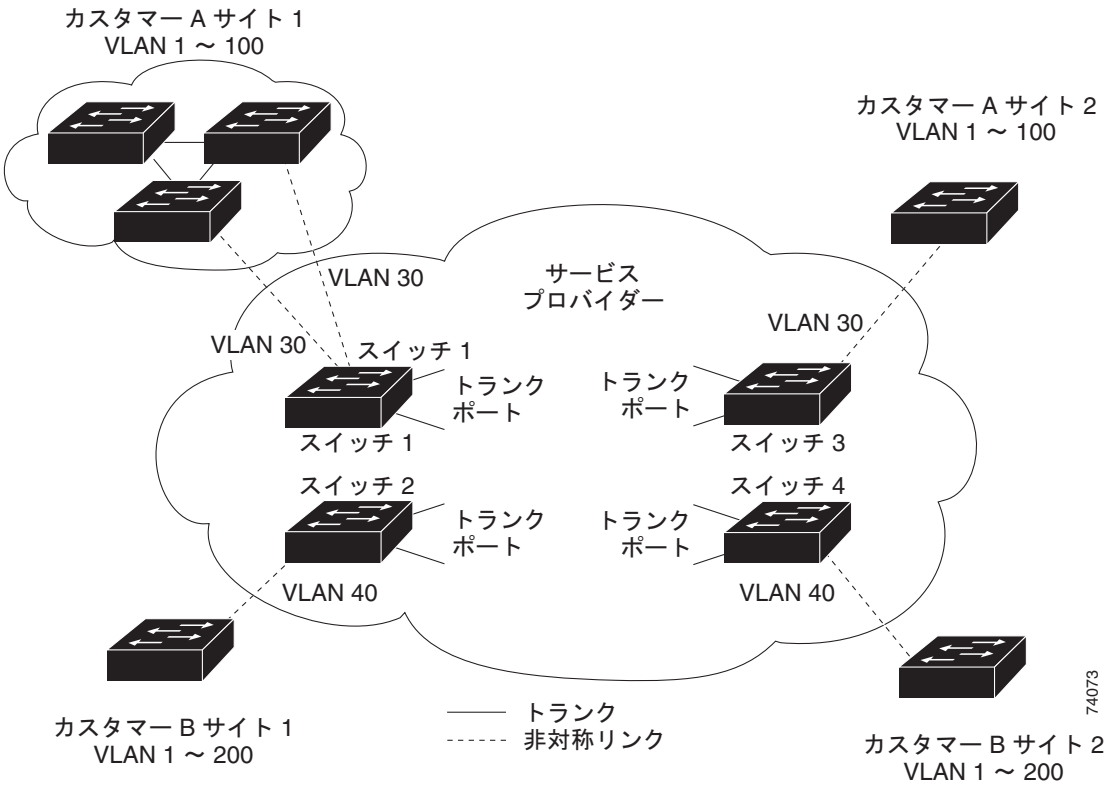
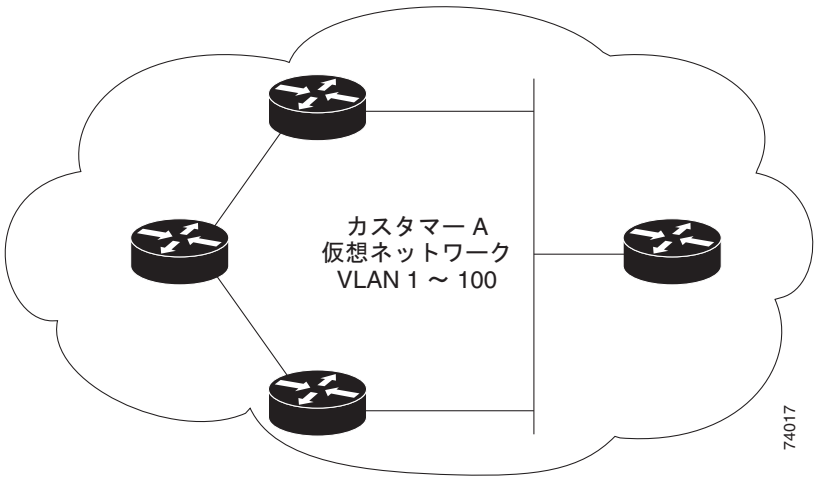


図 22-5　適切なコンバージェンスを含まないレイヤ 2 ネットワーク トポロジ



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、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。カスタマー 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、カスタマーの 802.1Q トランク ポートに接続できます。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。

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、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。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。外側のタグはカスタマーのメトロ タグで、内側のタグはカスタマーの 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、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。802.1Q トンネリングがイネーブルの場合、パケットも二重タグ付きです。外側のタグはカスタマーのメトロ タグで、内側の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で保持され、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 22-4 を参照してください。カスタマー A とカスタマー 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 のカスタマーをサービス 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 のカスタマー 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 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 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 のカスタマー 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。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、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

表 22-1 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 22-1　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。
- ダイナミック トランキング プロトコル（DTP）は、レイヤ 2 プロトコル トンネリングとは非互換です。トンネル ポートとトランク ポートのある非対称リンクを手動で設定する必要があるからです。
- 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。
- 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 ネットワーク上で稼働するスパニングツリー 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。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。
- 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るので、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

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。

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、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。

	コマンド	目的
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	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。 **（注）** 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	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。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	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。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	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。

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、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 ステータスのモニタリングおよびメンテナンス

表 22-2 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 22-2　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
Switch# **clear l2protocol-tunnel counters**	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# **show dot1q-tunnel**	スイッチの 802.1Q トンネル ポートを表示します。
Switch# **show dot1q-tunnel interface** *interface-id*	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# **show l2protocol-tunnel**	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# **show errdisable recovery**	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# **show l2protocol-tunnel interface** *interface-id*	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# **show l2protocol-tunnel summary**	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# **show vlan dot1q native**	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 Release 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 bpdufilter 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
```