



VLAN の設定

この章では、Catalyst 3750-E および 3560-E スイッチでの標準範囲 VLAN (VLAN ID 1 ~ 1005) および拡張範囲 VLAN (VLAN ID 1006 ~ 4094) の設定手順について説明します。VLAN メンバシップモード、VLAN コンフィギュレーションモード、VLAN トランク、および VLAN Membership Policy Server (VMPS; VLAN メンバシップ ポリシー サーバ) からのダイナミック VLAN 割り当てについても説明します。特に明記しないかぎり、スイッチという用語は Catalyst 3750-E または 3560-E スタンドアロンスイッチおよび Catalyst 3750-E スイッチ スタックを意味します。



(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。

- 「VLAN の概要」 (P.13-1)
- 「標準範囲 VLAN の設定」 (P.13-4)
- 「拡張範囲 VLAN の設定」 (P.13-11)
- 「VLAN の表示」 (P.13-15)
- 「VLAN トランクの設定」 (P.13-15)
- 「VMPS の設定」 (P.13-27)

VLAN の概要

VLAN は、ユーザの物理的な位置に関係なく、機能、プロジェクト チーム、またはアプリケーションなどで論理的に分割されたスイッチド ネットワークです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンド ステーションもグループ化できます。どのスイッチ ポートも VLAN に割り当てることができます。ユニキャスト、ブロードキャスト、およびマルチキャスト パケットは、VLAN 内のエンド ステーションだけに転送およびフラッディングが行われます。各 VLAN は 1 つの論理ネットワークと見なされ、VLAN に割り当てられていないステーション宛てのパケットは、ルータまたはフォールバック ブリッジングをサポートするスイッチを経由して転送しなければなりません (図 13-1 を参照)。スイッチ スタックでは、VLAN はスタック全体にまたがる複数のポートに設定できます。VLAN はそれぞれが独立した論理ネットワークと見なされるので、VLAN ごとに独自のブリッジ Management Information Base (MIB; 管理情報ベース) 情報があり、スパニングツリーの独自の実装をサポートできます。第 18 章「STP の設定」を参照してください。

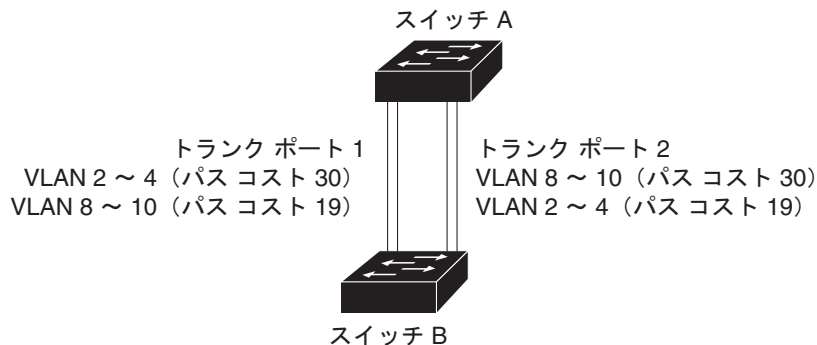


(注)

VLAN を作成する前に、VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) を使用してネットワークのグローバルな VLAN 設定を維持するかどうかを決定する必要があります。VTP の詳細については、第 14 章「VTP の設定」を参照してください。

図 13-1 に、論理的に定義されたネットワークにセグメント化された VLAN の例を示します。

図 13-1 論理的に定義されたネットワークとしての VLAN



VLAN は通常、IP サブネットワークに対応付けられます。たとえば、特定の IP サブネットに含まれるすべてのエンドステーションは同一の VLAN に所属させます。スイッチ上のインターフェイスの VLAN メンバシップは、インターフェイスごとに手動で割り当てます。この方法でスイッチ インターフェイスを VLAN に割り当てた場合、これをインターフェイス ベース (またはスタティック) VLAN メンバシップと呼びます。

VLAN 間のトラフィックは、ルーティングまたはフォールバックブリッジする必要があります。スイッチは、Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) を使用して、VLAN 間でトラフィックをルーティングできます。

VLAN 間でトラフィックをルーティングするには、SVI を明示的に設定して IP アドレスを割り当てる必要があります。詳細については、「SVI」(P.12-5) および「レイヤ 3 インターフェイスの設定」(P.12-34) を参照してください。



(注)

スイッチに多数の VLAN を設定し、ルーティングをイネーブル化しない予定の場合は、`sdm prefer vlan` グローバル コンフィギュレーション コマンドを使用して Switch Database Management (SDM; スイッチ データベース管理) 機能を VLAN テンプレートに設定できます。このテンプレートは、最大数のユニキャスト MAC アドレスをサポートするようにシステム リソースを設定します。SDM テンプレートの詳細については、第 8 章「SDM テンプレートの設定」、またはこのリリースのコマンドリファレンスの `sdm prefer` コマンドを参照してください。

サポートされる VLAN

スイッチは、VTP クライアント、サーバ、およびトランスペアレント モードで VLAN をサポートします。VLAN は、1 ~ 4094 の番号で識別します。VLAN ID 1002 ~ 1005 は、トークンリングおよび Fiber Distributed Data Interface (FDDI; ファイバ分散データ インターフェイス) VLAN 専用です。VTP バージョン 1 およびバージョン 2 は標準範囲 VLAN (VLAN ID 1 ~ 1005) のみをサポートします。これらのバージョンで、1006 ~ 4094 の VLAN ID を作成する場合は、スイッチを VTP トランスペアレント モードにする必要があります。Cisco IOS Release 12.2(52)SE 以降では、VTP バージョン 3

をサポートしています。VTP バージョン 3 は全範囲の VLAN (VLAN 1 ~ 4094) をサポートします。拡張範囲 VLAN (VLAN 1006 ~ 4094) は VTP バージョン 3 でのみサポートされます。ドメインに拡張 VLAN が設定されている場合、VTP バージョン 3 から VTP バージョン 2 に変換できません。

スイッチまたはスイッチ スタックは合計 1005 の (標準範囲および拡張範囲) VLAN をサポートします。ただし、ルーテッドポート、SVI、およびその他の設定済み機能の個数によって、スイッチハードウェアの使用状況は左右されます。

スイッチは、最大 128 のスパンニングツリー インスタンスを持つ Per-VLAN Spanning-Tree Plus (PVST+) または Rapid-PVST+ をサポートします。VLAN ごとに 1 つずつスパンニングツリー インスタンスを使用できます。スパンニングツリー インスタンス数および VLAN 数の詳細については、「標準範囲 VLAN 設定時の注意事項」(P.13-6) を参照してください。スイッチは、イーサネット ポート経由の VLAN トラフィックの送信方式として、Inter Switch Link (ISL; スイッチ間リンク) および IEEE 802.1Q トランッキングの両方をサポートします。

VLAN ポート メンバシップ モード

VLAN に所属するポートは、メンバシップ モードを割り当てることで設定します。メンバシップ モードは、各ポートが伝送できるトラフィックの種類、および所属できる VLAN の数を指定します。

表 13-1 に、各種メンバシップ モード、およびそれぞれのメンバシップと VTP の特性を示します。

表 13-1 ポートのメンバシップ モードとその特性

メンバシップ モード	VLAN メンバシップの特性	VTP の特性
スタティック アクセス	スタティック アクセス ポートは、手動で割り当てられ、1 つの VLAN だけに所属します。 詳細については、「VLAN へのスタティック アクセス ポートの割り当て」(P.13-10) を参照してください。	VTP は必須ではありません。VTP を使用して情報をグローバルに伝播させない場合は、VTP モードをトランスペアレントに設定します。VTP に参加するには、スイッチまたはスイッチ スタックの最低 1 つのトランク ポートが、別のスイッチまたはスイッチ スタックのトランク ポートに接続されている必要があります。
トランク (ISL または IEEE 802.1Q)	デフォルトで、トランク ポートは拡張範囲 VLAN を含むすべての VLAN のメンバーです。ただし、メンバシップは許可 VLAN リストを設定して制限できます。また、プルーニング適格リストを変更して、リストに指定したトランク ポート上の VLAN へのフラッドングトラフィックを阻止することもできます。 トランク ポートの設定については、「トランク ポートとしてのイーサネット インターフェイスの設定」(P.13-19) を参照してください。	VTP を推奨しますが、必須ではありません。VTP は、ネットワーク全体にわたって VLAN の追加、削除、名前変更を管理することにより、VLAN 設定の整合性を維持します。VTP はトランクリンクを通じて他のスイッチと VLAN コンフィギュレーション メッセージを交換します。

表 13-1 ポートのメンバシップモードとその特性 (続き)

メンバシップモード	VLAN メンバシップの特性	VTP の特性
ダイナミックアクセス	<p>ダイナミックアクセスポートは 1 つの VLAN (VLAN ID が 1 ~ 4094) にだけ所属し、VMPS によって動的に割り当てられます。VMPS には Catalyst 5000 または Catalyst 6500 シリーズスイッチを使用できますが、Catalyst 3750-E または 3560-E スイッチは使用できません。Catalyst 3750-E または 3560-E スイッチは VMPS クライアントです。</p> <p>同一スイッチ上でダイナミックアクセスポートとトランクポートを使用できますが、ダイナミックアクセスポートは別のスイッチではなく、エンドステーションまたはハブに接続する必要があります。</p> <p>設定情報については、「VMPS クライアント上のダイナミックアクセスポートの設定」(P.13-30) を参照してください。</p>	<p>VTP は必須です。</p> <p>VMPS およびクライアントを同じ VTP ドメイン名で設定してください。</p> <p>VTP に加入するには、スイッチまたはスイッチスタックの最低 1 つのトランクポートが、別のスイッチまたはスイッチスタックのトランクポートに接続されている必要があります。</p>
音声 VLAN	<p>音声 VLAN ポートは、Cisco IP Phone に接続し、電話に接続されたデバイスからの音声トラフィックに 1 つの VLAN を、データトラフィックに別の VLAN を使用するように設定されたアクセスポートです。</p> <p>音声 VLAN ポートの詳細については、第 15 章「音声 VLAN の設定」を参照してください。</p>	<p>VTP は不要です。VTP は音声 VLAN に作用しません。</p>

アクセスモードとトランクモード、および機能の定義の詳細については、[表 13-4 \(P.13-17\)](#) を参照してください。

ポートが VLAN に所属すると、スイッチは VLAN 単位で、ポートに対応するアドレスを学習して管理します。詳細については、「[MAC アドレステーブルの管理](#)」(P.7-12) を参照してください。

標準範囲 VLAN の設定

標準範囲 VLAN は、VLAN ID が 1 ~ 1005 の VLAN です。スイッチが VTP サーバまたはトランスペアレントモードの場合、VLAN データベース内の VLAN 2 ~ 1001 の設定を追加、変更、または削除できます (VLAN ID 1 および 1002 ~ 1005 は自動作成され、削除できません)。

VTP バージョン 1 および 2 では、拡張範囲 VLAN (ID が 1006 から 4094 の VLAN) を作成する場合、スイッチは VTP トランスペアレントモードである必要がありますが、これらの VLAN は VLAN データベースに保存されません。VTP バージョン 3 は VTP サーバモードおよびトランスペアレントモードで拡張範囲 VLAN をサポートしています。「[拡張範囲 VLAN の設定](#)」(P.13-11) を参照してください。

VLAN ID 1 ~ 1005 の設定はファイル *vlan.dat* (VLAN データベース) に書き込まれます。この設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。*vlan.dat* ファイルはフラッシュメモリに格納されます。Catalyst 3750-E スイッチでは、*vlan.dat* ファイルはスタックマスターのフラッシュメモリに格納されます。スタックメンバーは、スタックマスターと一貫性のある *vlan.dat* ファイルを持ちます。

**注意**

vlan.dat ファイルを手動で削除しようとする、VLAN データベースの不整合が生じる可能性があります。VLAN 設定を変更する場合は、ここに記載されたコマンド、およびこのリリースに対応するコマンドリファレンスに記載されたコマンドを使用します。このリリースに対応するコマンドリファレンスに記載されたコマンドを使用します。VTP 設定の変更手順については、第 14 章「VTP の設定」を参照してください。

さらに、インターフェイス コンフィギュレーション モードを使用して、ポートのメンバシップ モードの定義、VLAN に対するポートの追加および削除を行います。これらのコマンドの実行結果は、実行コンフィギュレーションファイルに書き込まれます。このファイルを表示するには、**show running-config** 特権 EXEC コマンドを使用します。

VLAN データベースに新しい標準範囲 VLAN を作成したり、VLAN データベース内の既存の VLAN を変更したりする場合、次のパラメータを設定できます。

- VLAN ID
- VLAN 名
- VLAN タイプ (イーサネット、FDDI、FDDI Network Entity Title (NET)、TrBRF または TrCRF、トークンリング、トークンリング Net)
- VLAN ステート (アクティブまたはサスペンド)
- VLAN の Maximum Transmission Unit (MTU; 最大伝送ユニット)
- Security Association Identifier (SAID)
- Token Ring Bridge Relay Function (TrBRF; トークンリングブリッジリレー機能) VLAN のブリッジ識別番号
- FDDI および TrCRF VLAN のリング番号
- Token Ring Concentrator Relay Function (TrCRF; トークンリングコンセントレータリレー機能) VLAN の親 VLAN 番号
- TrCRF VLAN の Spanning-Tree Protocol (STP; スパニングツリープロトコル) タイプ
- ある VLAN タイプから別の VLAN タイプに変換するときに使用する VLAN 番号

**(注)**

ここでは、これらのパラメータの大部分の設定手順について説明しません。VLAN 設定を制御するコマンドおよびパラメータの詳細については、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。

ここでは、標準範囲 VLAN の設定情報について説明します。

- 「トークンリング VLAN」(P.13-6)
- 「標準範囲 VLAN 設定時の注意事項」(P.13-6)
- 「標準範囲 VLAN の設定」(P.13-7)
- 「VLAN 設定の保存」(P.13-7)
- 「イーサネット VLAN のデフォルト設定」(P.13-8)
- 「イーサネット VLAN の作成または変更」(P.13-8)
- 「VLAN の削除」(P.13-9)
- 「VLAN へのスタティック アクセス ポートの割り当て」(P.13-10)

トークン リング VLAN

このスイッチはトークン リング接続をサポートしていませんが、トークン リング接続を行っている Catalyst 5000 シリーズ スイッチなどのリモート デバイスを、サポート対象スイッチのうちの 1 台から管理できます。VTP バージョン 2 が稼動しているスイッチは、次のトークン リング VLAN に関する情報をアドバタイズします。

- トークン リング TrBRF VLAN
- トークン リング TrCRF VLAN

トークン リング VLAN の詳しい設定手順については、『*Catalyst 5000 Series Software Configuration Guide*』を参照してください。

標準範囲 VLAN 設定時の注意事項

ネットワーク内で標準範囲 VLAN を作成または変更する場合には、次の注意事項に従ってください。

- スイッチは、VTP クライアント、サーバ、およびトランスペアレントの各モードで 1005 の VLAN をサポートしています。
- 標準範囲 VLAN は、1 ~ 1001 の番号で識別します。VLAN 番号 1002 ~ 1005 は、トークン リングおよび Fiber Distributed Data Interface (FDDI; ファイバ分散データ インターフェイス) VLAN 専用です。
- VLAN 1 ~ 1005 の VLAN 設定は、常に VLAN データベースに格納されます。VTP モードがトランスペアレントの場合、VTP および VLAN 設定はスイッチの実行コンフィギュレーション ファイルにも格納されます。
- VTP バージョン 1 および 2 では、スイッチは VTP トランスペアレント モード (VTP はディセーブル) でのみ、VLAN ID 1006 ~ 4094 をサポートします。これらは拡張範囲 VLAN であり、設定オプションには制限があります。VTP トランスペアレント モードで作成された拡張範囲 VLAN は VLAN データベースに保存されず、伝播されません。VTP バージョン 3 では拡張範囲 VLAN (VLAN 1006 ~ 4094) データベース伝播をサポートします。拡張 VLAN を設定している場合、VTP バージョン 3 からバージョン 1 または 2 に変換できません。「[拡張範囲 VLAN の設定](#)」(P.13-11) を参照してください。
- VLAN を作成する前に、スイッチを VTP サーバ モードまたは VTP トランスペアレント モードにしておく必要があります。スイッチが VTP サーバである場合には、VTP ドメインを定義する必要があります。VTP ドメインを定義しないと、VTP は機能しません。
- スイッチは、トークンリングまたは FDDI メディアをサポートしません。スイッチは FDDI、FDDI-Net、TrCRF、または TrBRF トラフィックを伝送しませんが、VTP を介して VLAN 設定を伝播します。
- スイッチは 128 のスパニングツリー インスタンスをサポートします。スイッチのアクティブな VLAN 数が、サポートされているスパニングツリー インスタンス数よりも多い場合、スパニングツリーは 128 の VLAN でイネーブルにできます。残りの VLAN で、スパニングツリーはディセーブルになります。スイッチ上の使用可能なスパニングツリー インスタンスをすべて使い切ってしまったあとに、VTP ドメインの中にさらに別の VLAN を追加すると、そのスイッチ上にスパニングツリーが稼動しない VLAN が生成されます。そのスイッチのトランク ポート上でデフォルトの許可リスト (すべての VLAN を許可するリスト) が設定されていると、すべてのトランク ポート上に新しい VLAN が割り当てられます。ネットワーク トポロジによっては、新しい VLAN 上で、切断されないループが生成されることがあります。特に、複数の隣接スイッチでスパニングツリー インスタンスをすべて使用してしまっている場合には注意が必要です。スパニングツリー インスタンスの割り当てを使い果たしたスイッチのトランク ポートに許可リストを設定することにより、このような可能性を防ぐことができます。

スイッチ上の VLAN の数がサポートされているスパニングツリー インスタンスの最大数を超える場合、スイッチ上に IEEE 802.1s Multiple STP (MSTP) を設定して、複数の VLAN を単一のスパニングツリー インスタンスにマッピングすることを推奨します。MSTP の詳細については、第 19 章「MSTP の設定」を参照してください。

- スタック内のスイッチが新たな VLAN を学習したか、既存の VLAN を（ネットワーク ポート上の VTP または CLI を通じて）削除または変更した場合は、VLAN 情報がすべてのスタック メンバーに通知されます。
- スイッチがスタックに加入したか、複数のスタックがマージされた場合、新規スイッチの VTP 情報（vlan.dat ファイル）はスタック マスターの VTP 情報と一貫性を維持します。

標準範囲 VLAN の設定

vlan グローバル コンフィギュレーション コマンドで VLAN ID を入力して、VLAN を設定します。新規の VLAN ID を入力して VLAN を作成するか、または既存の VLAN ID を入力してその VLAN を変更します。デフォルトの VLAN 設定を使用するか（表 13-2 を参照）、複数のコマンドを入力して VLAN を設定できます。このモードで使用できるコマンドの詳細については、このリリースのコマンドリファレンスに記載されている **vlan** グローバル コンフィギュレーション コマンドを参照してください。設定を終了したら、VLAN コンフィギュレーション モードを終了して、設定を有効にする必要があります。VLAN 設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。

VLAN 設定の保存

VLAN ID 1 ~ 1005 の設定は、常に VLAN データベースに保存されます（vlan.dat ファイル）。VTP モードがトランスペアレントの場合、それらの設定もスイッチの実行コンフィギュレーション ファイルに格納されます。**copy running-config startup-config** 特権 EXEC コマンドを使用して、スタートアップ コンフィギュレーション ファイルに設定を保存できます。スイッチ スタックでは、スタック全体で同一の vlan.dat ファイルと実行コンフィギュレーションを使用します。VLAN 設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。

VLAN および VTP 情報（拡張範囲 VLAN 設定情報を含む）をスタートアップ コンフィギュレーション ファイルに保存して、スイッチを再起動すると、スイッチの設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントで、VLAN データベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ~ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。
- VTP バージョン 1 および 2 では、VTP モードがサーバである場合、VLAN ID 1 ~ 1005 のドメイン名と VLAN 設定で VLAN データベース情報が使用されます。VTP バージョン 3 は VLAN 1006 ~ 4094 もサポートします。

イーサネット VLAN のデフォルト設定

表 13-2 にイーサネット VLAN のデフォルト設定を示します。



(注) スイッチがサポートするのは、イーサネット インターフェイスだけです。FDDI およびトークン リング VLAN は、ローカルではサポートされないため、FDDI およびトークン リング メディア固有の特性は、他のスイッチに対する VTP グローバル アドバタイズメントにだけ設定します。

表 13-2 イーサネット VLAN のデフォルト値および範囲

パラメータ	デフォルト値	範囲
VLAN ID	1	1 ~ 4094 (注) VTP バージョン 3 では、拡張範囲 VLAN (VLAN ID 1006 ~ 4094) のみが VLAN データベースに保存されます。
VLAN 名	VLANxxxx. xxxx は VLAN ID 番号に等しい 4 桁の数字 (先行ゼロを含む) です。	範囲なし
IEEE 802.10 SAID	100001 (100000 と VLAN ID の和)	1 ~ 4294967294
MTU サイズ	1500	1500 ~ 18190
トランスレーショナルブリッジ 1	0	0 ~ 1005
トランスレーショナルブリッジ 2	0	0 ~ 1005
VLAN ステート	アクティブ	アクティブ、サスペンド
リモート SPAN	ディセーブル	イネーブル、ディセーブル
プライベート VLAN	設定なし	2 ~ 1001、1006 ~ 4094

イーサネット VLAN の作成または変更

VLAN データベース内の各イーサネット VLAN には、1 ~ 1001 の 4 桁の一意の ID が設定されています。VLAN ID 1002 ~ 1005 は、トークン リングおよび FDDI VLAN 専用です。標準範囲 VLAN を作成して VLAN データベースに追加するには、VLAN に番号および名前を割り当てます。



(注) VTP バージョン 1 および 2 では、スイッチが VTP トランスペアレント モードにある場合、1006 より大きい VLAN ID を割り当てることができますが、それらは VLAN データベースに追加されません。「[拡張範囲 VLAN の設定](#)」(P.13-11) を参照してください。

VLAN の追加時に指定されるデフォルト パラメータの一覧は、「[標準範囲 VLAN の設定](#)」(P.13-4) を参照してください。

イーサネット VLAN を作成または変更するには、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>vlan vlan-id</code>	VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。新規の VLAN ID を入力して VLAN を作成するか、または既存の VLAN ID を入力してその VLAN を変更します。 (注) このコマンドで指定できる VLAN ID 範囲は 1 ~ 4094 です。1005 を超える VLAN ID (拡張範囲 VLAN) を追加する手順については、「 拡張範囲 VLAN の設定 」(P.13-11) を参照してください。
ステップ 3	<code>name vlan-name</code>	(任意) VLAN の名前を入力します。VLAN 名を指定しなかった場合には、デフォルトとして、VLAN という語の後ろに先行ゼロを含めた <code>vlan-id</code> が付加されます。たとえば、VLAN 4 のデフォルトの VLAN 名は VLAN0004 になります。
ステップ 4	<code>mtu mtu-size</code>	(任意) 最大伝送ユニット サイズ (または他の VLAN 特性) を変更します。
ステップ 5	<code>remote-span</code>	(任意) リモート Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) セッションに対する RSPAN VLAN として、VLAN を設定します。リモート SPAN の詳細については、 第 30 章「SPAN および RSPAN の設定」 を参照してください。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show vlan {name vlan-name id vlan-id}</code>	設定を確認します。
ステップ 8	<code>copy running-config startup config</code>	(任意) スイッチが VTP トランスペアレント モードである場合、VLAN 設定は実行コンフィギュレーション ファイルと VLAN データベースに保存されます。この場合、スイッチのスタートアップ コンフィギュレーション ファイルに設定が保存されます。

VLAN 名をデフォルトの設定に戻すには、`no name`、`no mtu` または `no remote-span` コマンドを使用します。

次に、イーサネット VLAN 20 を作成し、`test20` という名前を付け、VLAN データベースに追加する例を示します。

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# name test20
Switch(config-vlan)# end
```

VLAN の削除

VTP サーバ モードのスイッチから VLAN を削除すると、VTP ドメイン内のすべてのスイッチの VLAN データベースから、その VLAN が削除されます。VTP トランスペアレント モードのスイッチから VLAN を削除した場合、そのスイッチまたはスイッチ スタック上の VLAN だけが削除されます。

メディア タイプが異なるデフォルトの VLAN は削除できません。たとえば、イーサネット VLAN 1、および FDDI または トークン リング VLAN の 1002 ~ 1005 は削除できません。

**注意**

VLAN を削除すると、その VLAN に割り当てられていたすべてのポートが非アクティブになります。これらのポートは、新しい VLAN に割り当てられるまで、元の VLAN に（非アクティブで）対応付けられたままです。

スイッチ上で VLAN を削除するには、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	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	no vlan <i>vlan-id</i>	VLAN ID を入力して、VLAN を削除します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show vlan brief	VLAN が削除されたことを確認します。
ステップ 5	copy running-config startup config	(任意) スイッチが VTP トランスペアレント モードである場合、VLAN 設定は実行コンフィギュレーション ファイルと VLAN データベースに保存されます。この場合、スイッチのスタートアップ コンフィギュレーション ファイルに設定が保存されます。

VLAN へのスタティック アクセス ポートの割り当て

VTP をディセーブルにすることによって (VTP トランスペアレント モード)、VTP に VLAN 設定情報をグローバルに伝播させずに、スタティック アクセス ポートを VLAN に割り当てることができます。

クラスタ メンバー スイッチのポートを VLAN に割り当てる場合、最初に **rcommand** 特権 EXEC コマンドを使用して、そのクラスタ メンバー スイッチにログインします。

**(注)**

存在しない VLAN にインターフェイスを割り当てると、新しい VLAN が作成されます ([「イーサネット VLAN の作成または変更」 \(P.13-8\)](#) を参照)。

VLAN データベース内の VLAN にポートを割り当てるには、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	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	interface <i>interface-id</i>	VLAN に追加するインターフェイスを入力します。
ステップ 3	switchport mode access	ポート (レイヤ 2 アクセス ポート) の VLAN メンバシップ モードを定義します。
ステップ 4	switchport access vlan <i>vlan-id</i>	VLAN にポートを割り当てます。有効な VLAN ID は 1 ~ 4094 です。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show running-config interface <i>interface-id</i>	インターフェイスの VLAN メンバシップ モードを確認します。
ステップ 7	show interfaces <i>interface-id</i> switchport	表示された <i>Administrative Mode</i> および <i>Access Mode VLAN</i> フィールドの設定を確認します。
ステップ 8	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。

インターフェイスをデフォルト設定に戻すには、**default interface *interface-id*** 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。

次に、VLAN 2 のアクセス ポートとしてポートを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# end
```

拡張範囲 VLAN の設定

VTP バージョン 1 およびバージョン 2 では、スイッチが VTP トランスペアレントモード (VTP がディセーブル) の場合、拡張範囲 VLAN (1006 ~ 4094) を作成できます。VTP バージョンでは、サーバまたはトランスペアレントモードで拡張範囲 VLAN をサポートします。サービス プロバイダーは拡張範囲 VLAN を使用することにより、インフラストラクチャを拡張して、多数の顧客に対応できます。拡張範囲 VLAN ID は、VLAN ID が許可されている任意の switchport コマンドで使用できます。

VTP バージョン 1 または 2 では、拡張範囲 VLAN の設定は VLAN データベースには格納されません。ただし、VTP モードがトランスペアレントであるため、スイッチの実行コンフィギュレーション ファイルに格納されます。設定をスタートアップ コンフィギュレーション ファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを使用します。VTP バージョン 3 で作成された拡張範囲 VLAN は VLAN データベースに格納されます。



(注) スイッチは 4094 の VLAN ID をサポートしますが、実際にサポートされる VLAN の数については、「サポートされる VLAN」(P.13-2) を参照してください。

ここでは、拡張範囲 VLAN の設定情報について説明します。

- 「VLAN のデフォルト設定」(P.13-11)
- 「拡張範囲 VLAN 設定時の注意事項」(P.13-11)
- 「拡張範囲 VLAN の作成」(P.13-12)
- 「内部 VLAN ID を指定した拡張範囲 VLAN の作成」(P.13-14)

VLAN のデフォルト設定

イーサネット VLAN のデフォルト設定については、表 13-2 (P.13-8) を参照してください。拡張範囲 VLAN については最大伝送ユニット サイズ、プライベート VLAN、およびリモート SPAN 設定ステータスしか変更できません。残りのすべての特性はデフォルト ステータスのままでなければなりません。

拡張範囲 VLAN 設定時の注意事項

拡張範囲 VLAN を作成するときは次の注意事項に従ってください。

- スイッチが VTP バージョン 3 を実行していない限り、拡張範囲の VLAN ID は VLAN データベースに保存されず、VTP によって認識されません。
- プルーニング適格範囲に拡張範囲 VLAN を含めることはできません。

- VTP バージョン 1 および 2 では、拡張範囲 VLAN を作成する場合、スイッチが VTP トランスペアレントモードである必要があります。VTP モードがサーバまたはクライアントの場合、エラーメッセージが生成され、拡張範囲 VLAN が拒否されます。VTP バージョン 3 はサーバおよびトランスペアレントモードで、拡張 VLAN をサポートします。
- VTP バージョン 1 または 2 では、グローバル コンフィギュレーション モードで VTP モードをトランスペアレントに設定できます。「[VTP モードの設定](#)」(P.14-11) を参照してください。VTP トランスペアレントモードでスイッチが起動するように、この設定をスタートアップ コンフィギュレーションに保存する必要があります。このようにしないと、スイッチをリセットした場合に、拡張範囲 VLAN 設定が失われます。VTP バージョン 3 で拡張範囲 VLAN を作成する場合、VTP バージョン 1 または 2 に変換できません。
- 拡張範囲 VLAN では、STP はデフォルトでイネーブルになりますが、**no spanning-tree vlan *vlan-id*** グローバル コンフィギュレーション コマンドを使用してディセーブルにできます。スイッチ上に最大数のスパンニングツリー インスタンスが存在している場合に、VLAN を新規作成すると、この VLAN 上でスパンニングツリーはディセーブルになります。スイッチ上の VLAN の数がスパンニングツリー インスタンスの最大数を超える場合、スイッチ上に IEEE 802.1s MSTP を設定して、複数の VLAN を単一のスパンニングツリー インスタンスにマッピングすることを推奨します。MSTP の詳細については、[第 19 章「MSTP の設定」](#)を参照してください。
- スイッチ上の各ルーテッドポートは、内部 VLAN を使用するために作成します。この内部 VLAN は拡張範囲 VLAN 番号を使用し、その内部 VLAN ID は拡張範囲 VLAN には使用できません。内部 VLAN として割り当て済みの VLAN ID を指定して拡張範囲 VLAN を作成すると、エラーメッセージが生成され、コマンドは拒否されます。
 - 内部 VLAN ID は拡張範囲の下部の方なので、拡張範囲 VLAN を作成するには最大の番号 (4094) から始めて最小値 (1006) へと動いて、内部 VLAN ID を使用する可能性を減らすことを推奨します。
 - 拡張範囲 VLAN を設定する前に、**show vlan internal usage** 特権 EXEC コマンドを入力して、どの VLAN が内部 VLAN として割り当てられているかを確認します。
 - 必要に応じて、内部 VLAN に割り当てられたルーテッドポートをシャットダウンできます。これにより、内部 VLAN が解放され、拡張範囲 VLAN を作成してポートを再度イネーブルにし、別の VLAN を内部 VLAN として使用します。「[内部 VLAN ID を指定した拡張範囲 VLAN の作成](#)」(P.13-14) を参照してください。
- スイッチまたはスイッチ スタックは合計 1005 の (標準範囲および拡張範囲) VLAN をサポートしますが、ルーテッドポート、SVI、およびその他の設定済み機能の個数によって、スイッチのハードウェアの使用状況は左右されます。拡張範囲 VLAN を作成するときに、使用できるハードウェアリソースが不足していると、エラーメッセージが生成され、拡張範囲 VLAN が拒否されます。
- スイッチ スタックでは、スタック全体が同一の実行コンフィギュレーションと保存済みコンフィギュレーションを使用し、拡張範囲 VLAN 情報はスタック全体で共有されます。

拡張範囲 VLAN の作成

グローバル コンフィギュレーション モードで拡張範囲 VLAN を作成するには、**vlan** グローバル コンフィギュレーション コマンドを入力し、1006 ~ 4094 の VLAN ID を指定します。拡張範囲 VLAN はイーサネット VLAN のデフォルトの特性を備えており (表 13-2 を参照)、最大伝送ユニットサイズ、プライベート VLAN、RSPAN 設定だけが変更できるパラメータです。全パラメータのデフォルト設定については、コマンドリファレンスに記載されている **vlan** グローバル コンフィギュレーション コマンドを参照してください。VTP バージョン 1 または 2 では、スイッチが VTP トランスペアレントモードでない場合に拡張範囲 VLAN ID を入力すると、VLAN コンフィギュレーション モードの終了時にエラーメッセージが生成され、拡張範囲 VLAN が作成されません。

VTP バージョン 1 および 2 では、拡張範囲 VLAN は VLAN データベースに保存されず、スイッチの実行コンフィギュレーションファイルに保存されます。拡張範囲 VLAN 設定をスイッチのスタートアップコンフィギュレーションファイルに保存するには、**copy running-config startup-config** 特権 EXEC コマンドを使用します。VTP バージョン 3 では拡張範囲 VLAN が VLAN データベースに保存されます。



(注) 拡張範囲 VLAN を作成する前に、**show vlan internal usage** 特権 EXEC コマンドを入力して、VLAN ID が内部的に使用されていないことを確認します。VLAN ID が内部的に使用されている場合に、それを解放するには、「内部 VLAN ID を指定した拡張範囲 VLAN の作成」(P.13-14) を参照してから拡張範囲 VLAN を作成してください。

拡張範囲 VLAN を作成するには、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	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	vtp mode transparent	スイッチを VTP トランスペアレント モードに設定し、VTP をディセーブルにします。 (注) この手順は、VTP バージョン 3 では必要ありません。
ステップ 3	vlan vlan-id	拡張範囲 VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 1006 ~ 4094 です。
ステップ 4	mtu mtu-size	(任意) MTU サイズを変更して、VLAN を変更します。 (注) CLI ヘルプにすべての VLAN コマンドが表示されますが、拡張範囲 VLAN でサポートされているのは、 mtu mtu-size コマンド、 private-vlan コマンド、 remote-span コマンドだけです。
ステップ 5	remote-span	(任意) RSPAN VLAN として VLAN を設定します。「RSPAN VLAN としての VLAN の設定」(P.30-20) を参照してください。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	show vlan id vlan-id	VLAN が作成されたことを確認します。
ステップ 8	copy running-config startup config	スイッチのスタートアップコンフィギュレーションファイルに設定を保存します。拡張範囲 VLAN 設定を保存するには、VTP トランスペアレントモード設定および拡張範囲 VLAN 設定をスイッチのスタートアップコンフィギュレーションファイルに保存する必要があります。これらを保存しないと、スイッチをリセットした場合に、スイッチがデフォルトで VTP サーバモードになり、拡張範囲 VLAN ID は保存されません。 (注) VTP バージョン 3 では、VLAN の設定も VLAN データベースに保存されます。

拡張範囲 VLAN を削除するには、**no vlan vlan-id** 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。

スタティック アクセス ポートを拡張範囲 VLAN に割り当てる手順は、標準範囲 VLAN の手順と同じです。「VLAN へのスタティック アクセス ポートの割り当て」(P.13-10) を参照してください。

次に、すべてデフォルトの特性で拡張範囲 VLAN を新規作成し、VLAN コンフィギュレーション モードを開始して、新規 VLAN をスイッチのスタートアップコンフィギュレーションファイルに保存する例を示します。

```
Switch(config)# vtp mode transparent
Switch(config)# vlan 2000
```

```
Switch(config-vlan)# end
Switch# copy running-config startup config
```

内部 VLAN ID を指定した拡張範囲 VLAN の作成

内部 VLAN に割り当て済みの拡張範囲 VLAN ID を入力すると、エラーメッセージが生成され、拡張範囲 VLAN は拒否されます。内部 VLAN ID を手動で解放するには、内部 VLAN ID を使用しているルーテッドポートを一時的にシャットダウンする必要があります。

内部 VLAN に割り当てられた VLAN ID を解放してその ID で拡張範囲 VLAN を作成するには、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>show vlan internal usage</code>	スイッチが内部的に使用している VLAN ID を表示します。使用したい VLAN ID が内部 VLAN である場合は、その VLAN ID を使用しているルーテッドポートが表示されます。そのポート番号をステップ 3 で入力してください。
ステップ 2	<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 3	<code>interface interface-id</code>	その VLAN ID を使用しているルーテッドポートのインターフェイス ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<code>shutdown</code>	ポートをシャットダウンして内部 VLAN ID を解放します。
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。
ステップ 6	<code>vtp mode transparent</code>	VTP モードをトランスパレントに設定して拡張範囲 VLAN を作成します。 (注) この手順は、VTP バージョン 3 では必要ありません。
ステップ 7	<code>vlan vlan-id</code>	新しい拡張範囲 VLAN ID を入力し、VLAN コンフィギュレーション モードを開始します。
ステップ 8	<code>exit</code>	VLAN コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻ります。
ステップ 9	<code>interface interface-id</code>	ステップ 4 でシャットダウンしたルーテッドポートのインターフェイス ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 10	<code>no shutdown</code>	ルーテッドポートを再度イネーブルにします。新しい内部 VLAN ID が割り当てられます。
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>copy running-config startup config</code>	スイッチのスタートアップ コンフィギュレーション ファイルに設定を保存します。拡張範囲 VLAN 設定を保存するには、スイッチのスタートアップ コンフィギュレーション ファイルに VTP トランスパレントモード設定と拡張範囲 VLAN 設定を保存する必要があります。これらを保存しないと、スイッチをリセットした場合に、スイッチがデフォルトで VTP サーバモードになり、拡張範囲 VLAN ID は保存されません。 (注) VTP バージョン 3 では、VLAN が VLAN データベースに保存されるため、この手順は必要ありません。

VLAN の表示

拡張範囲 VLAN を含む、スイッチ上のすべての VLAN のリストを表示するには、**show vlan** 特権 EXEC コマンドを使用します。VLAN ステータス、ポート、および設定情報も表示されます。

表 13-3 に、VLAN を監視するためのコマンドを示します。

表 13-3 VLAN モニタリング コマンド

コマンド	コマンド モード	目的
show interfaces [vlan <i>vlan-id</i>]	特権 EXEC	スイッチ上に設定されたすべてのインターフェイスまたは特定の VLAN の特性を表示します。
show vlan [id <i>vlan-id</i>]	特権 EXEC	スイッチ上のすべての VLAN または特定の VLAN のパラメータを表示します。

show コマンド オプションおよび出力フィールドの詳細については、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。

VLAN トランクの設定

ここでは、次の概要について説明します。

- 「トランキングの概要」 (P.13-15)
- 「カプセル化タイプ」 (P.13-17)
- 「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」 (P.13-18)
- 「トランク ポートとしてのイーサネット インターフェイスの設定」 (P.13-19)
- 「トランク ポートのロード シェアリングの設定」 (P.13-23)

トランキングの概要

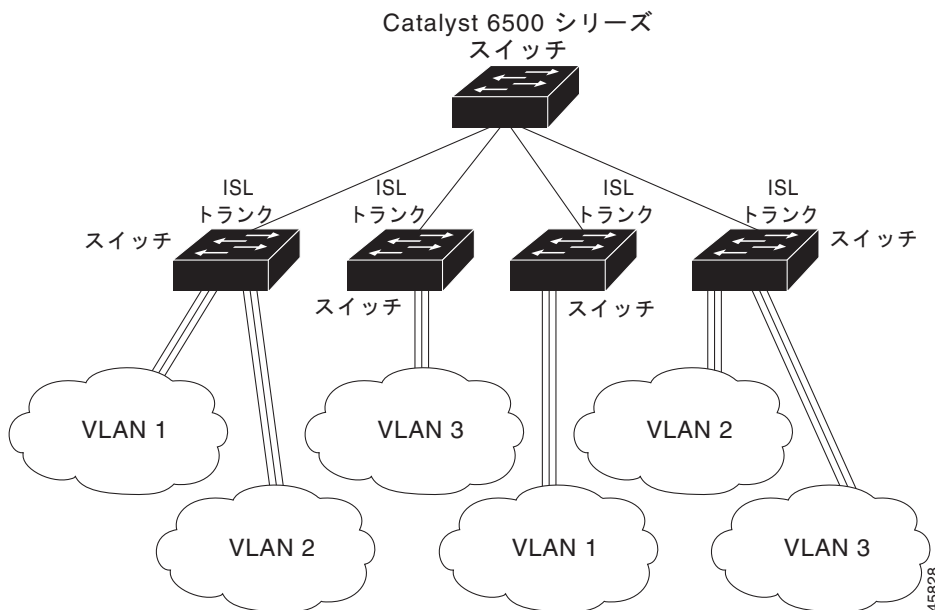
トランクとは、1 つまたは複数のイーサネット スイッチ インターフェイスと他のネットワーク デバイス（ルータ、スイッチなど）の間のポイントツーポイント リンクです。イーサネット トランクは VLAN をネットワーク全体に拡張できます。1 つのリンクを介して複数の VLAN トラフィックを搬送するので、VLAN をネットワーク全体に拡張できます。

すべてのイーサネット インターフェイス上で、2 種類のトランキング カプセル化方式を使用できます。

- ISL : ISL はシスコ独自のトランキング カプセル化方式です。
- IEEE 802.1Q : 業界標準のトランキング カプセル化方式です。

図 13-2 に、ISL トランクで接続されているスイッチ ネットワークを示します。

図 13-2 ISL トランキング環境のスイッチ



トランクを設定できるのは、1 つのイーサネット インターフェイスまたは EtherChannel バンドルに対してです。EtherChannel の詳細については、第 38 章「EtherChannel およびリンクステートトラッキングの設定」を参照してください。

イーサネット トランク インターフェイスは、表 13-4 に示すトランキング モードをサポートしていません。インターフェイスをトランキングまたは非トランキングとして設定したり、隣接インターフェイスとトランキングのネゴシエーションを行ったりするように設定できます。トランキングを自動ネゴシエーションするには、インターフェイスが同じ VTP ドメインに存在する必要があります。

トランク ネゴシエーションは、Point-to-Point Protocol (PPP; ポイントツーポイント プロトコル) である Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル) によって管理されます。ただし、一部のインターネットワーキング デバイスによって DTP フレームが不正に転送されて、矛盾した設定となる場合があります。

この事態を避けるには、DTP をサポートしないデバイスに接続されたインターフェイスが DTP フレームを転送しないように、つまり DTP をオフにするように設定する必要があります。

- これらのリンクを介してトランキングを行わない場合は、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、トランキングをディセーブルにします。
- DTP をサポートしていないデバイスへのトランキングをイネーブルにするには、**switchport mode trunk** および **switchport nonegotiate** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスがトランクになっても DTP フレームを生成しないように設定します。
switchport trunk encapsulation isl または **switchport trunk encapsulation dot1q** インターフェイスを使用して、トランク ポートのカプセル化タイプを選択します。

トランクに ISL カプセル化を使用させるのか、IEEE 802.1Q カプセル化を使用させるのか、それともカプセル化タイプの自動ネゴシエーションを行うのかを DTP インターフェイス上で指定することもできます。DTP は ISL トランクおよび IEEE 802.1Q トランクの両方の自動ネゴシエーションをサポートします。



(注) DTP はプライベート VLAN ポートまたはトンネル ポートではサポートされていません。

表 13-4 レイヤ 2 インターフェイス モード

モード	機能
<code>switchport mode access</code>	インターフェイス（アクセス ポート）を永続的な非トランキング モードにして、リンクの非トランク リンクへの変換をネゴシエートします。インターフェイスは、隣接インターフェイスがトランク インターフェイスかどうかに関係なく、非トランク インターフェイスになります。
<code>switchport mode dynamic auto</code>	インターフェイスがリンクをトランク リンクに変換できるようにします。インターフェイスは、隣接インターフェイスが <i>trunk</i> または <i>desirable</i> モードに設定されている場合、トランク インターフェイスになります。すべてのイーサネット インターフェイスのデフォルトのスイッチポート モードは dynamic auto です。
<code>switchport mode dynamic desirable</code>	インターフェイスがリンクのトランク リンクへの変換をアクティブに実行するようにします。インターフェイスは、隣接インターフェイスが <i>trunk</i> 、 <i>desirable</i> 、または <i>auto</i> モードに設定されている場合、トランク インターフェイスになります。
<code>switchport mode trunk</code>	インターフェイスを永続的なトランキング モードにして、隣接リンクのトランク リンクへの変換をネゴシエートします。インターフェイスは、隣接インターフェイスがトランク インターフェイスでない場合でも、トランク インターフェイスになります。
<code>switchport nonegotiate</code>	インターフェイスが DTP フレームを生成しないようにします。このコマンドは、インターフェイス スイッチポート モードが access または trunk の場合だけ使用できます。トランク リンクを確立するには、手動で隣接インターフェイスをトランク インターフェイスとして設定する必要があります。
<code>switchport mode dot1q-tunnel</code>	インターフェイスをトンネル（非トランキング）ポートとして設定し、IEEE 802.1Q トランク ポートと非対称リンクで接続されるようにします。IEEE 802.1Q トンネリングは、サービス プロバイダー ネットワーク全体でカスタマー VLAN の整合性を維持するのに使用されます。トンネル ポートの詳細については、 第 17 章「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」 を参照してください。

カプセル化タイプ

表 13-5 に、イーサネット トランクのカプセル化タイプおよびキーワードを示します。

表 13-5 イーサネット トランクのカプセル化タイプ

カプセル化	機能
<code>switchport trunk encapsulation isl</code>	トランク リンクに ISL カプセル化を指定します。
<code>switchport trunk encapsulation dot1q</code>	トランク リンクに IEEE 802.1Q カプセル化を指定します。
<code>switchport trunk encapsulation negotiate</code>	インターフェイスが隣接インターフェイスとネゴシエーションを行い、隣接インターフェイスの設定および機能に応じて ISL トランク（優先）または IEEE 802.1Q トランクになるように指定します。これがスイッチのデフォルトです。



(注)

スイッチはレイヤ 3 トランクをサポートしません。したがって、サブインターフェイスを設定したり、レイヤ 3 インターフェイスで **encapsulation** キーワードを使用したりすることはできません。ただし、スイッチは、同等の機能を備えたレイヤ 2 トランクおよびレイヤ 3 VLAN インターフェイスをサポートします。

リンクが ISL トランクまたは IEEE 802.1Q トランクのどちらになるかは、接続された 2 つのインターフェイスのトランキングモード、トランク カプセル化タイプ、およびハードウェア機能によって決まります。

IEEE 802.1Q の設定に関する考慮事項

IEEE 802.1Q トランクは、ネットワークのトランキング方式について次の制約があります。

- IEEE 802.1Q トランクを使用して接続している Cisco スイッチのネットワークでは、スイッチはトランク上で許容される VLAN ごとに 1 つのスパニングツリー インスタンスを維持します。他社製のデバイスは、すべての VLAN でスパニングツリー インスタンスを 1 つサポートする場合があります。

IEEE 802.1Q トランクを使用して Cisco スイッチを他社製のデバイスに接続する場合、Cisco スイッチは、トランクの VLAN のスパニングツリー インスタンスを、他社製の IEEE 802.1Q スイッチのスパニングツリー インスタンスと結合します。ただし、各 VLAN のスパニングツリー情報は、他社製の IEEE 802.1Q スイッチからなるクラウドにより分離された Cisco スイッチによって維持されます。Cisco スイッチを分離する他社製の IEEE 802.1Q クラウドは、スイッチ間の単一トランク リンクとして扱われます。

- IEEE 802.1Q トランクに対応するネイティブ VLAN が、トランク リンクの両側で一致していなければなりません。トランクの片側のネイティブ VLAN と反対側のネイティブ VLAN が異なっていると、スパニングツリー ループが発生する可能性があります。
- ネットワーク上のすべてのネイティブ VLAN についてスパニングツリーをディセーブルにせず、IEEE 802.1Q トランクのネイティブ VLAN 上のスパニングツリーをディセーブルにすると、スパニングツリー ループが発生することがあります。IEEE 802.1Q トランクのネイティブ VLAN 上でスパニングツリーをイネーブルのままにしておくか、またはネットワーク上のすべての VLAN でスパニングツリーをディセーブルにすることを推奨します。また、ネットワークにループがないことを確認してから、スパニングツリーをディセーブルにしてください。

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

表 13-6 に、レイヤ 2 イーサネット インターフェイス VLAN のデフォルト設定を示します。

表 13-6 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
インターフェイス モード	switchport mode dynamic auto
トランク カプセル化	switchport trunk encapsulation negotiate
VLAN 許容範囲	VLAN 1 ~ 4094
プルーニングに適切な VLAN 範囲	VLAN 2 ~ 1001
デフォルト VLAN (アクセス ポート用)	VLAN 1
ネイティブ VLAN (IEEE 802.1Q トランク用)	VLAN 1

トランク ポートとしてのイーサネット インターフェイスの設定

トランク ポートは VTP アドバタイズメントを送受信するので、VTP を使用する場合は、スイッチ上で少なくとも 1 つのトランク ポートが設定されており、そのトランク ポートが第 2 のスイッチのトランク ポートに接続されていることを確認する必要があります。そうでない場合、スイッチは VTP アドバタイズメントを受信できません。

ここでは、次の設定情報について説明します。

- 「他の機能との相互作用」(P.13-19)
- 「トランクでの許可 VLAN の定義」(P.13-21)
- 「プルーニング適格リストの変更」(P.13-22)
- 「タグなしトラフィック用ネイティブ VLAN の設定」(P.13-23)



(注)

デフォルトでは、インターフェイスはレイヤ 2 モードです。レイヤ 2 インターフェイスのデフォルトモードは、**switchport mode dynamic auto** です。隣接インターフェイスがトランキングをサポートし、トランキングを許可するように設定されている場合、リンクはレイヤ 2 トランクです。また、インターフェイスがレイヤ 3 モードの場合は、**switchport** インターフェイス コンフィギュレーション コマンドを入力するとレイヤ 2 トランクになります。デフォルトでは、トランクはカプセル化のネゴシエーションを行います。隣接インターフェイスが ISL および IEEE 802.1Q カプセル化をサポートしていて、なおかつ両方のインターフェイスがカプセル化タイプのネゴシエーションを行うように設定されている場合、トランクは ISL カプセル化を使用します。

他の機能との相互作用

トランキングは他の機能と次のように相互作用します。

- トランク ポートは、セキュア ポートにできません。
- トランク ポートは、トンネル ポートにできません。
- トランク ポートは、まとめて EtherChannel ポート グループにできますが、グループ内のすべてのトランクに同じ設定をする必要があります。グループを初めて作成したときには、そのグループに最初に追加されたポートのパラメータ設定値をすべてのポートが引き継ぎます。次のパラメータのいずれかについて、設定を変更すると、入力した設定値がスイッチによってグループ内のすべてのポートに伝播されます。
 - 許可 VLAN リスト
 - 各 VLAN の STP ポート プライオリティ
 - STP PortFast の設定値
 - トランク ステータス：ポート グループ内の 1 つのポートがトランクでなくなると、すべてのポートがトランクでなくなります。
- PVST モードで設定するトランク ポートは 24 まで、MST モードで設定するトランク ポートは 40 までにすることを推奨します。
- トランク ポートで IEEE 802.1x をイネーブルにしようとする、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートをトランクに変更しようとしても、ポート モードは変更されません。
- ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで IEEE 802.1x をイネーブルにしようとする、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートを動的に変更しようとしても、ポート モードは変更されません。

トランク ポートの設定

ポートをトランク ポートとして設定するには、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>	トランクに設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport trunk encapsulation {isl dot1q negotiate}</code>	ISL または IEEE 802.1Q カプセル化をサポートする、またはカプセル化タイプについて隣接インターフェイスとネゴシエーションを行う (デフォルト) ようにポートを設定します。 同じカプセル化タイプを指定して、リンクの各終端を設定する必要があります。
ステップ 4	<code>switchport mode {dynamic {auto desirable} trunk}</code>	インターフェイスをレイヤ 2 トランクとして設定します (インターフェイスがレイヤ 2 アクセス ポートまたはトンネル ポートであり、トランキング モードを設定する場合に限り必要となります)。 <ul style="list-style-type: none"> • dynamic auto : 隣接インターフェイスが trunk または desirable モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。これがデフォルトです。 • dynamic desirable : 隣接インターフェイスが trunk、desirable、または auto モードに設定されている場合に、インターフェイスをトランク リンクとして設定します。 • trunk : 隣接インターフェイスがトランク インターフェイスでない場合でも、インターフェイスを永続的なトランキング モードに設定して、リンクをトランク リンクに変換するようにネゴシエートします。
ステップ 5	<code>switchport access vlan vlan-id</code>	(任意) 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するデフォルト VLAN を指定します。
ステップ 6	<code>switchport trunk native vlan vlan-id</code>	IEEE 802.1Q トランク用のネイティブ VLAN を指定します。
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 interfaces interface-id switchport</code>	インターフェイスのスイッチポート設定を表示します。 <i>Administrative Mode</i> および <i>Administrative Trunking Encapsulation</i> フィールドに表示されます。
ステップ 9	<code>show interfaces interface-id trunk</code>	インターフェイスのトランク設定を表示します。
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。

インターフェイスをデフォルト設定に戻すには、**default interface interface-id** 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。トランキング インターフェイスのすべてのトランキング 特性をデフォルトにリセットするには、**no switchport trunk** 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。トランキングをディセーブルにするには、**switchport mode access** インターフェイス コンフィギュレーション コマンドを使用して、ポートをスタティック アクセス ポートとして設定します。

次に、IEEE 802.1Q トランクとしてポートを設定する例を示します。この例では、ネイバーのインターフェイスが IEEE 802.1Q トランキングをサポートするように設定されていることを前提としています。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/0/2
```

```
Switch(config-if)# switchport mode dynamic desirable
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# end
```

トランクでの許可 VLAN の定義

デフォルトでは、トランク ポートはすべての VLAN に対してトラフィックを送受信します。各トランクですべての VLAN ID (1 ~ 4094) が許可されます。ただし、許可リストから VLAN を削除することにより、それらの VLAN からのトラフィックがトランク上を流れないようにすることができます。トランクが伝送するトラフィックを制限するには、**switchport trunk allowed vlan remove vlan-list** インターフェイス コンフィギュレーション コマンドを使用して、許可リストから特定の VLAN を削除します。



(注)

VLAN 1 は、すべての Cisco スイッチのすべてのトランク ポートのデフォルト VLAN です。以前は、すべてのトランク リンクで VLAN 1 を必ずイネーブルにする必要がありました。VLAN 1 の最小化機能を使用して、個々の VLAN トランク リンクで VLAN 1 をディセーブルに設定できます。これにより、ユーザトラフィック (スパニングツリー アドバタイズメントなど) は VLAN 1 で送受信されなくなります。

スパニングツリー ループまたはストームのリスクを軽減するには、許可リストから VLAN 1 を削除して個々の VLAN トランク ポートで VLAN 1 をディセーブルにします。トランク ポートから VLAN 1 を削除した場合、インターフェイスは引き続き VLAN 1 内で Cisco Discovery Protocol (CDP)、ポート集約プロトコル、Link Aggregation Control Protocol (LACP)、DTP、および VTP などの管理トラフィックを送受信します。

VLAN 1 をディセーブルにしたトランク ポートが非トランク ポートになると、そのポートはアクセス VLAN に追加されます。アクセス VLAN が 1 に設定されると、**switchport trunk allowed** の設定には関係なく、ポートは VLAN 1 に追加されます。ポート上でディセーブルになっている任意の VLAN について同様のことが当てはまります。

トランク ポートは、VLAN がイネーブルになっており、VTP が VLAN を認識し、なおかつポートの許可リストにその VLAN が登録されている場合に、VLAN のメンバーになることができます。VTP が新しくイネーブルにされた VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されている場合、トランク ポートは自動的にその VLAN のメンバーになります。VTP が新しい VLAN を認識し、その VLAN がトランク ポートの許可リストに登録されていない場合には、トランク ポートはその VLAN のメンバーにはなりません。

トランクの許可リストを変更するには、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	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	interface interface-id	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switchport mode trunk	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 4	switchport trunk allowed vlan {add all except remove} vlan-list	(任意) トランク上で許可される VLAN のリストを設定します。 add 、 all 、 except 、および remove キーワードの使用方法については、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。 <i>vlan-list</i> パラメータは、1 ~ 4094 の単一の VLAN 番号、または 2 つの VLAN 番号 (小さい方が先、ハイフンで区切る) で指定された VLAN 範囲です。カンマで区切った VLAN パラメータの間、またはハイフンで指定した範囲の間には、スペースを入れしないでください。 デフォルトでは、すべての VLAN が許可されます。

	コマンド	目的
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show interfaces interface-id switchport</code>	表示された <i>Trunking VLANs Enabled</i> フィールドの設定を確認します。
ステップ 7	<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。

すべての VLAN の許可 VLAN リストをデフォルトに戻すには、**no switchport trunk allowed vlan** 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。

次に、ポートの許可 VLAN リストから VLAN 2 を削除する例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk allowed vlan remove 2
Switch(config-if)# end
```

プルーニング適格リストの変更

プルーニング適格リストは、トランク ポートだけに適用されます。トランク ポートごとに専用の適格リストがあります。この手順を有効にするには、VTP プルーニングがイネーブルに設定されている必要があります。VTP プルーニングをイネーブルにする方法については、「[VTP プルーニングのイネーブル化](#)」(P.14-17) を参照してください。

トランク ポートのプルーニング適格リストから VLAN を削除するには、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>	VLAN プルーニングを適用するトランク ポートを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport trunk pruning vlan {add except none remove} vlan-list [,vlan[,vlan[,...]]</code>	トランクからのプルーニングを許可する VLAN のリストを設定します (「 VTP プルーニング 」(P.14-6) を参照)。 add 、 except 、 none 、および remove キーワードの使用方法については、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。 連続していない VLAN ID は、カンマ (スペースなし) で区切ります。ID の範囲はハイフンで指定します。有効な ID 範囲は 2 ~ 1001 です。拡張範囲 VLAN (VLAN ID 1006 ~ 4094) はプルーニングできません。 プルーニング不適格の VLAN は、フラッドイング トラフィックを受信します。 デフォルトでは、プルーニングが許可される VLAN のリストには、VLAN 2 ~ 1001 が含まれます。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show interfaces interface-id switchport</code>	表示された <i>Pruning VLANs Enabled</i> フィールドの設定を確認します。
ステップ 6	<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。

すべての VLAN のプルーニング適格リストをデフォルトに戻すには、**no switchport trunk pruning vlan** 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。

タグなしトラフィック用ネイティブ VLAN の設定

IEEE 802.1Q タギングが設定されたトランク ポートは、タグ付きトラフィックおよびタグなしトラフィックの両方を受信できます。デフォルトでは、タグなしトラフィックは、ポートに設定されたネイティブ VLAN に転送されます。ネイティブ VLAN は、デフォルトでは VLAN 1 です。



(注) ネイティブ VLAN には任意の VLAN ID を割り当てることができます。

IEEE 802.1Q 設定の詳細については、「[IEEE 802.1Q の設定に関する考慮事項](#)」(P.13-18) を参照してください。

IEEE 802.1Q トランクでネイティブ VLAN 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>	IEEE 802.1Q トランクとして設定するインターフェイスを定義して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport trunk native vlan vlan-id</code>	トランク ポート上でタグなしトラフィックを送受信する VLAN を設定します。 <i>vlan-id</i> に指定できる範囲は、1 ~ 4094 です。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show interfaces interface-id switchport</code>	<i>Trunking Native Mode VLAN</i> フィールドの設定を確認します。
ステップ 6	<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。

ネイティブ VLAN をデフォルト (VLAN 1) に戻すには、`no switchport trunk native vlan` 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。

パケットの VLAN ID が出力ポートのネイティブ VLAN ID と同じであれば、そのパケットはタグなしで送信されます。ネイティブ VLAN ID と異なる場合は、スイッチはそのパケットをタグ付きで送信します。

トランク ポートのロード シェアリングの設定

ロードシェアリングにより、スイッチに接続しているパラレル トランクの提供する帯域幅が分割されます。STP は通常、ループを防止するために、スイッチ間で 1 つのパラレル リンク以外のすべてのリンクをブロックします。ロードシェアリングを行うと、トラフィックの所属する VLAN に基づいて、リンク間でトラフィックが分散されます。

トランク ポートでロードシェアリングを設定するには、STP ポートプライオリティまたは STP パスコストを使用します。STP ポートプライオリティを使用してロードシェアリングを設定する場合には、両方のロードシェアリングリンクを同じスイッチに接続する必要があります。STP パスコストを使用してロードシェアリングを設定する場合には、それぞれのロードシェアリングリンクを同一のスイッチにも、2 台の異なるスイッチにも接続できます。STP の詳細については、第 18 章「[STP の設定](#)」を参照してください。

STP ポート プライオリティによるロード シェアリング

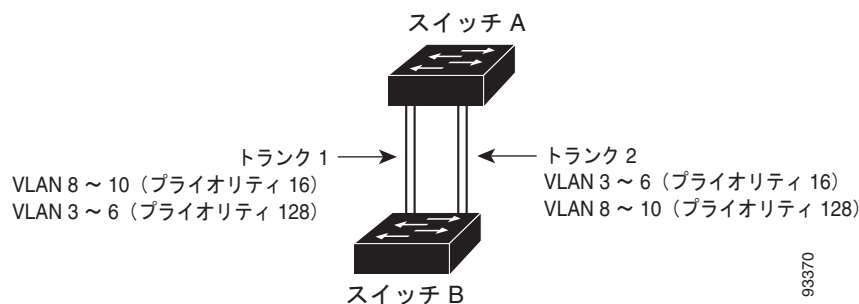
同一スイッチ上の 2 つのポートがループを形成すると、スイッチは STP ポート プライオリティを使用して、どのポートをイネーブルとし、どのポートをブロッキング ステートとするかを判断します。パラレル トランク ポートにプライオリティを設定することにより、そのポートに、特定の VLAN のすべてのトラフィックを伝送させることができます。VLAN に対するプライオリティの高い（値の小さい）トランク ポートがその VLAN のトラフィックを転送します。同じ VLAN に対してプライオリティの低い（値の大きい）トランク ポートは、その VLAN に対してブロッキング ステートのままです。1 つのトランク ポートが特定の VLAN に関するすべてのトラフィックを送受信することになります。

図 13-3 に、サポート対象スイッチを接続する 2 つのトランクを示します。この例では、スイッチは次のように設定されています。

- VLAN 8 ~ 10 は、トランク 1 で 16 というポート プライオリティが割り当てられています。
- VLAN 3 ~ 6 は、トランク 1 でデフォルトのポート プライオリティである 128 のままです。
- VLAN 3 ~ 6 は、トランク 2 で 16 というポート プライオリティが割り当てられています。
- VLAN 8 ~ 10 は、トランク 2 でデフォルトのポート プライオリティである 128 のままです。

このように設定すると、トランク 1 が VLAN 8 ~ 10 のトラフィックを伝送し、トランク 2 が VLAN 3 ~ 6 のトラフィックを伝送します。アクティブ トランクで障害が起きた場合には、プライオリティの低いトランクが引き継ぎ、それらすべての VLAN のトラフィックを伝送します。いずれのトランク ポート上でも、トラフィックの重複は発生しません。

図 13-3 STP ポート プライオリティによるロード シェアリング



(注)

スイッチがスイッチ スタックのメンバーの場合は、**spanning-tree [vlan vlan-id] port-priority priority** インターフェイス コンフィギュレーション コマンドの代わりに、**spanning-tree [vlan vlan-id] cost cost** インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスをフォワーディング ステートにするように選択する必要があります。最初に選択させたいインターフェイスには小さいコスト値を、最後に選択させたいインターフェイスには大きいコスト値を割り当てます。詳細については、「**STP パス コストによるロード シェアリング**」(P.13-26) を参照してください。

図 13-3 のようにネットワークを設定するには、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	configure terminal	スイッチ A で、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	vtp domain domain-name	VTP 管理ドメインを設定します。 1 ~ 32 文字のドメイン名を使用できます。

	コマンド	目的
ステップ 3	<code>vtp mode server</code>	スイッチ A を VTP サーバとして設定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show vtp status</code>	スイッチ A および B の両方で、VTP 設定を確認します。 表示された <i>VTP Operating Mode</i> および <i>VTP Domain Name</i> フィールドをチェックします。
ステップ 6	<code>show vlan</code>	スイッチ A のデータベースに VLAN が存在していることを確認します。
ステップ 7	<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 8	<code>interface gigabitethernet1/ 0/1</code>	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 9	<code>switchport trunk encapsulation {isl dot1q negotiate}</code>	ISL または IEEE 802.1Q カプセル化をサポートする、または隣接インターフェイスとネゴシエーションを行うようにポートを設定します。同じカプセル化タイプを指定して、リンクの各終端を設定する必要があります。
ステップ 10	<code>switchport mode trunk</code>	ポートをトランク ポートとして設定します。
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 interfaces gigabitethernet1/ 0/1 switchport</code>	VLAN 設定を確認します。
ステップ 13		スイッチまたはスイッチ スタックでスイッチ A の 2 番目のポートについて、ステップ 7 ~ 11 を繰り返します。
ステップ 14		スイッチ B でステップ 7 ~ 11 を繰り返し、スイッチ A に設定したトランク ポートにトランク ポートを接続するように設定します。
ステップ 15	<code>show vlan</code>	トランク リンクがアクティブになると、VTP がスイッチ B に VTP および VLAN 情報を渡します。スイッチ B が VLAN 設定を学習したことを確認します。
ステップ 16	<code>configure terminal</code>	スイッチ A で、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 17	<code>interface gigabitethernet1/ 0/1</code>	STP のポート プライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 18	<code>spanning-tree vlan 8-10 port-priority 16</code>	VLAN 8 ~ 10 にポート プライオリティ 16 を割り当てます。
ステップ 19	<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 20	<code>interface gigabitethernet1//0/2</code>	STP のポート プライオリティを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 21	<code>spanning-tree vlan 3-6 port-priority 16</code>	VLAN 3 ~ 6 にポート プライオリティ 16 を割り当てます。
ステップ 22	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 23	<code>show running-config</code>	設定を確認します。
ステップ 24	<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。

STP パス コストによるロード シェアリング

トランクにそれぞれ異なるパス コストを設定し、各パス コストをそれぞれ異なる VLAN 群に対応付け、各 VLAN でポートをブロックすることによって、VLAN トラフィックを分散するパラレル トランクを設定できます。VLAN はトラフィックを分離し、リンクが失われた場合に備えて冗長性を維持します。

図 13-4 で、トランク ポート 1 および 2 は 100BASE-T ポートとして設定されています。次の VLAN パス コストが割り当てられています。

- VLAN 2～4 は、トランク ポート 1 で 30 というパス コストが割り当てられています。
- VLAN 8～10 は、トランク ポート 1 で 100BASE-T のデフォルトのパス コストである 19 のままです。
- VLAN 8～10 は、トランク ポート 2 で 30 というパス コストが割り当てられています。
- VLAN 2～4 は、トランク ポート 2 で 100BASE-T のデフォルトのパス コストである 19 のままです。

図 13-4 パス コストによってトラフィックが分散されるロード シェアリング トランク

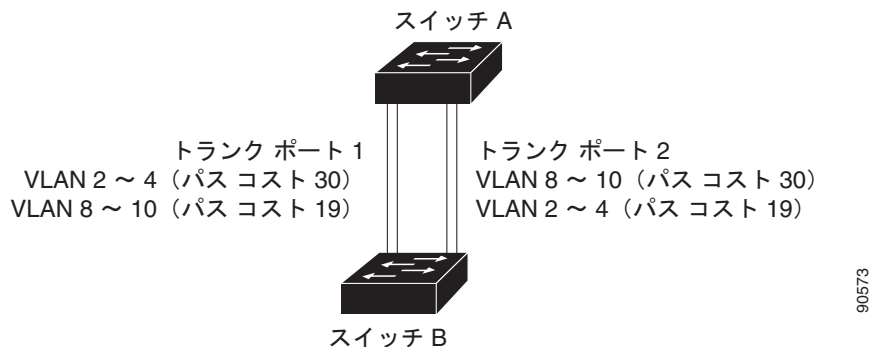


図 13-4 のようにネットワークを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	スイッチ A で、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 gigabitethernet1/0/1</code>	トランクとして設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport trunk encapsulation {isl dot1q negotiate}</code>	ISL または IEEE 802.1Q カプセル化をサポートするようにポートを設定します。同じカプセル化タイプを指定して、リンクの各終端を設定する必要があります。
ステップ 4	<code>switchport mode trunk</code>	ポートをトランク ポートとして設定します。トランクのデフォルトは ISL トランキングです。
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。
ステップ 6		スイッチ A (Catalyst 3560-E スイッチ) またはスイッチ A スタック (Catalyst 3750-E スイッチ) の 2 番目のインターフェイスで、ステップ 2～5 を繰り返します。
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>	設定を確認します。画面で、インターフェイスがトランク ポートとして設定されていることを確認してください。
ステップ 9	<code>show vlan</code>	トランク リンクがアクティブになると、スイッチ A がもう一方のスイッチから VTP 情報を受信します。スイッチ A が VLAN 設定を学習したことを確認します。

	コマンド	目的
ステップ 10	<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 11	<code>interface gigabitethernet1/0/1</code>	STP コストを設定するインターフェイスを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 12	<code>spanning-tree vlan 2-4 cost 30</code>	VLAN 2 ~ 4 のスパンニングツリー パス コストを 30 に設定します。
ステップ 13	<code>end</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 14		スイッチ A に設定したもう一方のトランク インターフェイスでステップ 9 ~ 13 を繰り返し、VLAN 8、9、および 10 のスパンニングツリー パス コストを 30 に設定します。
ステップ 15	<code>exit</code>	特権 EXEC モードに戻ります。
ステップ 16	<code>show running-config</code>	設定を確認します。両方のトランク インターフェイスに対してパス コストが正しく設定されていることを表示で確認します。
ステップ 17	<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。

VMPS の設定

VLAN Query Protocol (VQP) は、ダイナミックアクセス ポートをサポートする場合に使用します。ダイナミックアクセス ポートは VLAN に永続的に割り当てられるのではなく、ポートで認識された MAC 送信元アドレスに基づいて VLAN を割り当てます。未知の MAC アドレスが検出されるたびに、スイッチはリモート VMPS に VQP クエリーを送信します。クエリーには新たに検出された MAC アドレスとそのアドレスを検出したポートが含まれます。VMPS はそのポートの VLAN 割り当てで応答します。このスイッチは、VMPS サーバにはできませんが、VMPS のクライアントとして機能させ、VQP を介して通信できます。

ここでは、次の情報について説明します。

- 「VMPS の概要」 (P.13-27)
- 「VMPS クライアントのデフォルト設定」 (P.13-29)
- 「VMPS 設定時の注意事項」 (P.13-29)
- 「VMPS クライアントの設定」 (P.13-29)
- 「VMPS のモニタリング」 (P.13-32)
- 「ダイナミックアクセス ポート VLAN メンバシップのトラブルシューティング」 (P.13-33)
- 「VMPS の設定例」 (P.13-33)

VMPS の概要

クライアントスイッチは新しいホストの MAC アドレスを受信するたびに、VMPS に VQP クエリーを送信します。このクエリーを受信した VMPS は、データベースで MAC アドレスと VLAN のマッピングを検索します。サーバの応答は、このマッピングと、サーバがオープンモードかセキュアモードかに基づいて行われます。セキュアモードの場合、サーバは不正なホストが検出されると、ポートをシャットダウンします。オープンモードでは、サーバはホストに対してポートアクセスを拒否するだけです。

ポートが未割り当ての場合（つまり、VLAN 割り当てがまだ設定されていない場合）、VMPS は次のいずれかの応答を行います。

- そのポートでホストが許可されている場合、VMPS は割り当てられた VLAN 名を指定し、ホストへのアクセスを許可する VLAN 割り当て応答をクライアントに送信します。
- そのポートでホストが許可されておらず、なおかつ VMPS がオープン モードの場合、VMPS はアクセス拒否応答を送信します。
- そのポートで VLAN が許可されておらず、なおかつ VMPS がセキュア モードの場合、VMPS はポートシャットダウン応答を送信します。

ポートに VLAN 割り当てがすでに設定されている場合、VMPS は次のいずれかの応答を行います。

- データベース内の VLAN がポート上の現在の VLAN と一致した場合、VMPS は成功応答を送信し、ホストへのアクセスを許可します。
- データベース内の VLAN がポート上の現在の VLAN と一致せず、なおかつポート上にアクティブホストが存在する場合、VMPS は VMPS のセキュア モードに応じて、アクセス拒否またはポートシャットダウン応答を送信します。

VMPS からアクセス拒否応答を受信した場合、スイッチはそのホスト MAC アドレスのトラフィックを双方向で引き続きブロックします。スイッチはポート宛てのパケットを引き続き監視し、新しいホストアドレスを検出すると VMPS にクエリーを送信します。VMPS からポートシャットダウン応答を受信した場合、スイッチはそのポートをディセーブルにします。Network Assistant、CLI、または SNMP を使用して、ポートを手動で再びイネーブルにする必要があります。

ダイナミックアクセス ポート VLAN メンバシップ

ダイナミックアクセス ポートが所属できるのは、VLAN ID が 1 ~ 4094 の 1 つの VLAN だけです。リンクがアップになっても、VMPS によって VLAN が割り当てられるまで、このポートとの間でトラフィック転送は行われません。VMPS は、ダイナミックアクセス ポートに接続した新しいホストの最初のパケットから送信元 MAC アドレスを受信し、VMPS データベースの VLAN とその MAC アドレスを照合します。

一致した場合、VMPS はそのポートの VLAN 番号を送信します。クライアント スイッチがまだ設定されていない場合は、スイッチは VMPS からトランク ポートで受信した最初の VTP パケットからのドメイン名を使用します。クライアント スイッチがすでに設定されている場合は、クエリー パケットにスイッチのドメイン名を含めて VMPS に送信し、VLAN 番号を取得します。VMPS はパケット内のドメイン名が自身のドメイン名と一致することを確認したあと、要求を受け入れ、クライアントに割り当てられた VLAN 番号を応答します。一致しない場合、(VMPS セキュア モードの設定に応じて) VMPS は要求を拒否するか、ポートをシャットダウンします。

ダイナミックアクセス ポート上で複数のホスト (MAC アドレス) をアクティブにできますが、それらのホストはすべて同じ VLAN に存在する必要があります。ただし、ポート上でアクティブなホスト数が 20 を超えると、VMPS はダイナミックアクセス ポートをシャットダウンします。

ダイナミックアクセス ポート上でリンクがダウンになると、ポートは切り離された状態に戻り、VLAN の所属から外れます。ポート経由でオンラインになるホストは VMPS によって VQP 経由で再チェックされてから、ポートが VLAN に割り当てられます。

ダイナミックアクセス ポートは、直接ホスト接続に使用したり、ネットワークに接続したりできます。スイッチ上のポートごとに、最大 20 の MAC アドレスを使用できます。ダイナミックアクセス ポートが一度に所属できる VLAN は 1 つですが、VLAN は検出された MAC アドレスに基づいてあとで変更されることがあります。

VMPS クライアントのデフォルト設定

表 13-7 に、クライアント スイッチ上の VMPS およびダイナミックアクセス ポートのデフォルト設定を示します。

表 13-7 VMPS クライアントおよびダイナミックアクセス ポートのデフォルト設定

機能	デフォルト設定
VMPS ドメイン サーバ	なし
VMPS 再確認インターバル	60 分
VMPS サーバ再試行回数	3
ダイナミックアクセス ポート	未設定

VMPS 設定時の注意事項

ダイナミックアクセス ポート VLAN メンバシップには、次の注意事項および制限事項があります。

- VMPS を設定してから、ポートをダイナミックアクセス ポートとして設定する必要があります。
- ポートをダイナミックアクセス ポートとして設定すると、そのポートに対してスパンニングツリーの PortFast 機能が自動的にイネーブルになります。PortFast モードにより、ポートをフォワーディング ステートに移行させるプロセスが短縮されます。
- IEEE 802.1x ポートはダイナミックアクセス ポートとして設定できません。ダイナミックアクセス (VQP) ポートで IEEE 802.1x をイネーブルにしようとする、エラー メッセージが表示され、IEEE 802.1x はイネーブルになりません。IEEE 802.1x 対応ポートを変更してダイナミック VLAN を割り当てようとしても、エラー メッセージが表示され、VLAN 設定は変更されません。
- トランク ポートは、ダイナミックアクセス ポートにはできませんが、トランク ポートに対して **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドを入力することは可能です。その場合、スイッチの設定は維持され、あとにアクセス ポートとして設定された場合には、その設定が適用されます。

ダイナミックアクセス設定を有効にするには、ポート上でトランッキングをオフにしておく必要があります。

- ダイナミックアクセス ポートは、モニタ ポートにできません。
- セキュア ポートは、ダイナミックアクセス ポートにできません。ポートを動的にするには、ポート上でポート セキュリティをディセーブルにしておく必要があります。
- プライベート VLAN ポートは、ダイナミックアクセス ポートにできません。
- ダイナミックアクセス ポートは、EtherChannel グループのメンバーにできません。
- ポート チャネルは、ダイナミックアクセス ポートとして設定できません。
- ダイナミックアクセス ポートは、フォールバック ブリッジングに加入できます。
- VMPS クライアントと VMPS サーバの VTP 管理ドメインは、同じでなければなりません。
- VMPS サーバ上に設定された VLAN を音声 VLAN にしないでください。

VMPS クライアントの設定

ダイナミック VLAN を設定するには、VMPS (サーバ) を使用します。スイッチは、VMPS クライアントにはできますが、VMPS サーバにはできません。

VMPS の IP アドレスの入力

スイッチをクライアントとして設定するには、サーバの IP アドレスを最初に入力する必要があります。



(注) スイッチ クラスタに対して VMPS を定義する場合は、コマンド スイッチにこのアドレスを入力する必要があります。

VMPS の IP アドレスを入力するには、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>vmps server ipaddress primary</code>	プライマリ VMPS サーバとして動作するスイッチの IP アドレスを入力します。
ステップ 3	<code>vmps server ipaddress</code>	(任意) セカンダリ VMPS サーバとして動作するスイッチの IP アドレスを入力します。 セカンダリ サーバのアドレスは、3 つまで入力できます。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show vmps</code>	表示された <i>VMPS Domain Server</i> フィールドの設定を確認します。
ステップ 6	<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。



(注) ダイナミックアクセス ポートを動作させるには、VMPS に IP 接続できなければなりません。IP 接続が可能かどうかをテストするには、VMPS の IP アドレスに `ping` を実行し、応答が得られるかどうかを確認します。

VMPS クライアント上のダイナミックアクセス ポートの設定

クラスタ メンバー スイッチのポートをダイナミックアクセス ポートとして設定するには、最初に `rcommand` 特権 EXEC コマンドを使用して、そのクラスタ メンバー スイッチにログインします。



注意

ダイナミックアクセス ポート VLAN メンバシップはエンドステーション用、またはエンドステーションに接続されたハブ用です。他のスイッチにダイナミックアクセス ポートを接続すると、接続が切断されることがあります。

VMPS クライアント スイッチにダイナミックアクセス 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>	エンドステーションに接続するスイッチ ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>switchport mode access</code>	ポートをアクセス モードにします。

	コマンド	目的
ステップ 4	switchport access vlan dynamic	ポートを動的 VLAN メンバシップ適格として設定します。 動的アクセスポートは、エンドステーションに接続されている必要があります。
ステップ 5	end	特権 EXEC モードに戻ります。
ステップ 6	show interfaces interface-id switchport	表示された <i>Operational Mode</i> フィールドの設定を確認します。
ステップ 7	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。

インターフェイスをデフォルト設定に戻すには、**default interface interface-id** 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。インターフェイスをデフォルトのスイッチポートモード (dynamic auto) に戻すには、**no switchport mode** 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。アクセスモードをスイッチのデフォルト VLAN にリセットするには、**no switchport access vlan** 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。

VLAN メンバシップの再確認

スイッチが VMPS から受信した動的アクセスポート VLAN メンバシップの割り当てを確認するには、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	vmps reconfirm	動的アクセスポート VLAN メンバシップを再確認します。
ステップ 2	show vmps	動的 VLAN の再確認ステータスを確認します。

再確認インターバルの変更

VMPS クライアントは、VMPS から受信する VLAN メンバシップの情報を定期的に再確認します。再確認を実行する間隔は数字を使用して分単位で設定できます。

クラスターのメンバースイッチを設定する場合、このパラメータはコマンドスイッチの再確認インターバルの設定値以上でなければなりません。メンバースイッチにログインするには、最初に **rcommand** 特権 EXEC コマンドを使用する必要があります。

再確認インターバルを変更するには、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	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	vmps reconfirm minutes	動的 VLAN メンバシップの再確認を行う間隔 (分) を入力します。指定できる範囲は 1 ~ 120 です。デフォルト値は 60 分です。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show vmps	表示された <i>Reconfirm Interval</i> フィールドの動的 VLAN の再確認ステータスを確認します。
ステップ 5	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。

スイッチのデフォルト設定に戻すには、**no vmps reconfirm** 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。

再試行回数の変更

スイッチが次のサーバにクエリーを送信する前に、VMPS との接続を試行する回数を変更するには、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>vmpls retry count</code>	再試行の回数を変更します。指定できる再試行回数の範囲は 1 ~ 10 です。デフォルトは 3 です。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show vmpls</code>	表示された <i>Server Retry Count</i> フィールドの設定を確認します。
ステップ 5	<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。

スイッチのデフォルト設定に戻すには、`no vmpls retry` 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。

VMPS のモニタリング

`show vmpls` 特権 EXEC コマンドを使用して、VMPS に関する情報を表示できます。スイッチは VMPS に関する次の情報を表示します。

- VMPS VQP バージョン：VMPS との通信に使用する VQP のバージョン。スイッチは VQP バージョン 1 を使用する VMPS にクエリーを送信します。
- 再確認インターバル：スイッチが VLAN と MAC アドレスの割り当てを再確認する間隔（分）
- サーバ再試行回数：VQP が VMPS にクエリーを再送信する回数。この回数すべてを試行しても応答が得られない場合、スイッチはセカンダリ VMPS へのクエリーを開始します。
- VMPS ドメイン サーバ：設定されている VLAN メンバシップ ポリシー サーバの IP アドレス。スイッチは *current* と表示されているサーバにクエリーを送信します。*primary* と表示されているサーバは、プライマリ サーバです。
- VMPS 動作：最新の再確認の結果。再確認は、再確認インターバルが経過したときに自動的に行われますが、`vmpls reconfirm` 特権 EXEC コマンドを入力するか、Network Assistant または SNMP で同等の操作を行うことによって、強制的に再確認することもできます。

次に、`show vmpls` 特権 EXEC コマンドの出力例を示します。

```
Switch# show vmpls
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
                   172.20.128.87

Reconfirmation status
-----
VMPS Action:          other
```


ダイナミックアクセス ポート VLAN メンバシップのトラブルシューティング

VMPS は次の状況でダイナミックアクセス ポートをシャットダウンします。

- VMPS がセキュア モードであり、なおかつホストのポートへの接続を許可しない場合。VMPS はポートをシャットダウンして、ホストがネットワークに接続できないようにします。
- ダイナミックアクセス ポート上のアクティブ ホストが 20 を超えた場合

ディセーブルにされているダイナミックアクセス ポートを再びイネーブルにするには、**shutdown** インターフェイス コンフィギュレーション コマンドに続けて、**no shutdown** インターフェイス コンフィギュレーション コマンドを入力します。

VMPS の設定例

図 13-5 に、VMPS サーバ スイッチと、ダイナミックアクセス ポートを備えた VMPS クライアント スイッチが含まれるネットワークの例を示します。この例の前提条件は次のとおりです。

- VMPS サーバと VMPS クライアントは、それぞれ別のスイッチです。
- Catalyst 6500 シリーズのスイッチ A が、プライマリ VMPS サーバです。
- Catalyst 6500 シリーズのスイッチ C およびスイッチ J が、セカンダリ VMPS サーバです。
- エンドステーションはクライアント（スイッチ B、スイッチ I）に接続されています。
- データベース コンフィギュレーション ファイルは、IP アドレス 172.20.22.7 の TFTP サーバに保存されています。

図 13-5 ダイナミック ポート VLAN メンバシップの構成例

