CHAPTER 11

VLAN の設定

この章では、Catalyst 3750 Metro スイッチに、標準範囲の VLAN（VLAN ID が 1 ～ 1005）および拡張範囲の VLAN（VLAN ID が 1006 ～ 4094）を設定する方法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。

（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。

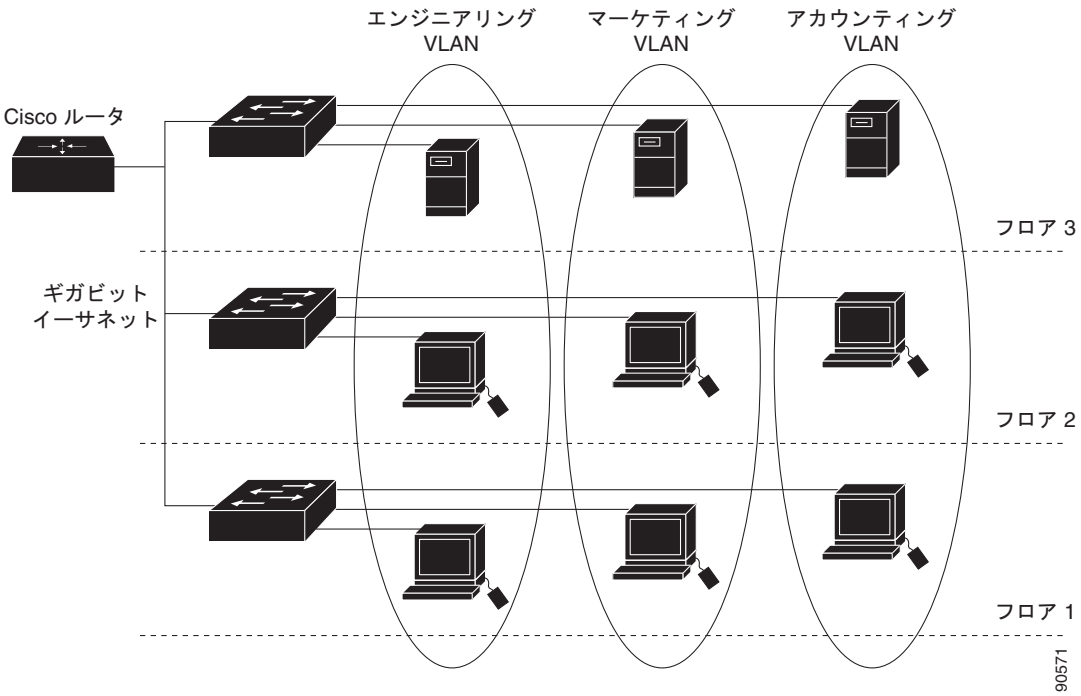
VLAN の概要

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 と同じアトリビュート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されます。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する必要があります（図 11-1 を参照）。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 MIB 情報があり、それぞれが独自にスパニング ツリーの実装をサポートします。第 16 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 12 章「VTP の設定」を参照してください。

図 11-1 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 11-1　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 ステーションは同じ VLAN に属します。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 ブリッジング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、「スイッチ仮想インターフェイス」（P.9-5）および「レイヤ 3 インターフェイスの設定」（P.9-19）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）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 6 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、および透過の各モードで 1005 の VLAN をサポートしています。VLAN は 1 ～ 4094 の数で識別されます。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 用に予約され

ています。VTP は、VLAN ID が 1 ～ 1005 の標準範囲 VLAN だけを学習します。1005 を超える VLAN ID は拡張範囲 VLAN と呼ばれ、VLAN データベースにはストアされません。1006 ～ 4094 の VLAN ID を作成する場合は、スイッチを VTP 透過モードにする必要があります。

スイッチは合計 1005（標準範囲および拡張範囲）の VLAN をサポートしますが、ルーテッド ポート、SVI、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は左右されます。

スイッチは、最大 128 のスパニング 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 つずつスパニング ツリー インスタンスを使用できます。スパニング 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.11-6）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 に属するポートは、メンバシップ モードを指定して設定します。メンバシップ モードにより、各ポートが搬送できるトラフィックの種類、および属することができる VLAN の数が決まります。表 11-1 に、各種メンバシップ モード、メンバシップ、VTP 特性を示します。

表 11-1　ポート メンバシップ モード

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.11-10）を参照してください。	VTP は必須ではありません。VTP にグローバルに情報を伝播させないようにする場合は、VTP モードを透過モードに設定して VTP をディセーブルにします。VTP に加入するには、あるスイッチのトランク ポートに接続した別のスイッチ上に 1 つまたは複数のトランク ポートが必要です。
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 へのフラッディング 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.11-19）を参照してください。 **（注）** Cisco IOS リリース 12.2(22)EY 以降のリリースでは、ISL トランキングは enhanced-services（ES）ポートではサポートされません。ES ポートは IEEE 802.1Q カプセル化だけをサポートします。	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 11-1　ポート メンバシップ モード （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	ダイナミック アクセス ポートは 1 つの VLAN（VLAN ID が 1 ～ 4094）だけに所属し、VMPS によってダイナミックに割り当てられます。たとえば、Catalyst 5000 または Catalyst 6500 シリーズ スイッチは VMPS として使用できますが、Catalyst 3750 Metro スイッチは VMPS として使用できません。Catalyst 3750 Metro スイッチは、VMPS クライアントです。 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。 設定の詳細については、「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.11-31）を参照してください。	VTP は必須です。 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。 VTP に加入するには、あるスイッチのトランク ポートに接続した別のスイッチ上に 1 つまたは複数のトランク ポートが必要です。
プライベート VLAN	プライベート VLAN ポートは、プライベート VLAN のプライマリまたはセカンダリ VLAN に属するホストまたは混合ポートです。この機能を使用するには、Enhanced Multilayer Image（EMI; 拡張マルチレイヤ イメージ）がスイッチ上で稼動している必要があります。 プライベート VLAN の詳細については、第 13 章「プライベート VLAN の設定」を参照してください。	プライベート VLAN を設定する場合は、スイッチが VTP 透過モードになっている必要があります。プライベート VLAN がスイッチに設定されている場合、VTP モードを透過モードからクライアント モードやサーバ モードに変更しないでください。
音声 VLAN	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。音声 VLAN ポートの詳細については、第 14 章「音声 VLAN の設定」を参照してください。	VTP は必須ではなく、音声 VLAN には影響しません。
トンネル（**dot1q-tunnel**）	トンネル ポートは、サービスプロバイダー ネットワーク上でカスタマー VLAN の整合性を保つための IEEE 802.1Q トンネリングに使用されます。トンネル ポートは、サービスプロバイダー ネットワークのエッジ スイッチ上に設定し、カスタマー インターフェイスの IEEE 802.1Q トランク ポートに接続して、非対称リンクを作成します。トンネル ポートは、トンネリング専用の単一の VLAN に属します。 トンネル ポートの詳細については、第 15 章「IEEE 802.1Q 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。	VTP は必須ではありません。**switchport access vlan** インターフェイス コンフィギュレーション コマンドを使用して、手動で VLAN にトンネル ポートを割り当てます。

モードおよびその機能の詳細については、表 11-4（P.11-16）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.5-19）を参照してください。

標準範囲 VLAN の設定

標準範囲の VLAN とは、VLAN ID が 1 ～ 1005 の VLAN のことです。スイッチが VTP サーバ モードまたは透過モードにある場合は、VLAN データベース内の VLAN 2 ～ 1001 について設定を追加、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）。

（注） スイッチが VTP 透過モードの場合、拡張範囲 VLAN（ID が 1006 ～ 4094 の VLAN）も作成できます。ただし、これらの拡張範囲 VLAN は VLAN データベースに格納されません。「拡張範囲 VLAN の設定」（P.11-11）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、NVRAM にストアされます。

注意 *vlan.dat* ファイルを手動で削除しようとすると、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。VTP 設定の変更手順については、第 12 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）、Token Ring Bridge Relay Function（TrBRF; トークンリング ブリッジ リレー機能）または 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）、トークンリング、トークンリング Net）
- VLAN ステート（アクティブまたは一時停止）
- VLAN の Maximum Transmission Unit（MTU; 最大伝送ユニット）
- Security Association Identifier（SAID）
- TrBRF VLAN のブリッジ識別番号
- FDDI および TrCRF VLAN のリング番号
- TrCRF 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 について説明します。内容は次のとおりです。

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、および透過の各モードで 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 FDDI 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 モードが透過モードの場合、VTP と VLAN の設定もスイッチの実行コンフィギュレーション ファイルに保存されます。
- スイッチは VTP 透過モード（VTP はディセーブル）で、VLAN ID 1006 ～ 4094 もサポートします。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。拡張範囲 VLAN は VLAN データベースには格納されません。「拡張範囲 VLAN の設定」（P.11-11）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 透過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 数がサポートされるスパニング ツリー インスタンス数を超える場合は、IEEE 802.1s Multiple STP（MSTP）をスイッチに設定して、複数の VLAN を単一の STP 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 17 章「MSTP の設定」を参照してください。

- VLAN コンフィギュレーション モードにアクセスするには、VLAN ID を指定して **vlan** グローバル コンフィギュレーション コマンドを入力します。VLAN を新規に作成するには新しい VLAN ID を、既存の VLAN を変更するには、その VLAN ID を入力します。デフォルトの VLAN 設定を使用するか（表 11-2 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 モードが透過モードの場合は、スイッチの実行コンフィギュレーション ファイルへの保存も行われるため、**copy running-config startup-config** 特権 EXEC コマンドを入力して設定をスタートアップ コンフィギュレーション ファイルに保存できます。**show running-config** 特権 EXEC コマンドを使用して、スイッチの実行コンフィギュレーション ファイルを表示できます。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。

スタートアップ コンフィギュレーション ファイルに VLAN および VTP 情報（拡張範囲 VLAN 設定も含む）を保存してスイッチを再起動すると、スイッチの設定が次のように決定されます。

- 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 モードが透過で、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、最初の 1005 の VLAN 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 モードがサーバの場合、最初の 1005 の VLAN のドメイン名および VLAN 設定には VLAN データベース情報が使用されます。

注意　起動時に VLAN データベース コンフィギュレーションが使用され、スタートアップ コンフィギュレーション ファイルに拡張範囲 VLAN 設定が含まれていた場合、システムのブート時にこの情報は失われます。

イーサネット VLAN のデフォルト設定

表 11-2 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ので、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だけに設定します。

表 11-2　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	範囲
VLAN ID	1	1 ～ 4094 （注）　拡張範囲 VLAN（VLAN ID 1006 ～ 4094）は VLAN データベースには保存されません。
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
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、一時停止
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	未設定	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 の ID は 4 桁の一意の数字で、1 ～ 1001 を指定できます。VLAN ID 1002 ～ 1005 は、トークンリングおよび FDDI VLAN 用に予約されています。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）　スイッチが VTP 透過モードの場合、1006 を超える VLAN ID を割り当てることができますが、それらは VLAN データベースには追加されません。「拡張範囲 VLAN の設定」（P.11-11）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.11-5）を参照してください。

イーサネット VLAN を作成および変更するには、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	**vlan** *vlan-id*	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。VLAN を新規に作成するには新しい VLAN ID を、既存の VLAN を変更するには、その VLAN ID を入力します。 **（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.11-11）を参照してください。
ステップ 3	**name** *vlan-name*	（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 *vlan-id* 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	**mtu** *mtu-size*	（任意）MTU サイズ（または他の VLAN 特性）を変更します。
ステップ 5	remote-span	（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 の詳細は、第 28 章「SPAN および RSPAN の設定」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** {**name** *vlan-name* | **id** *vlan-id*}	設定を確認します。
ステップ 8	**copy running-config startup config**	（任意）スイッチが VTP 透過モードである場合、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** VLAN コンフィギュレーション 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 透過モードのスイッチから VLAN を削除した場合、そのスイッチ上にかぎり VLAN が削除されます。

それぞれのメディア タイプのデフォルト VLAN（イーサネット VLAN 1、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 モードでグローバル コンフィギュレーション モードを使用して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** *vlan-id*	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 透過モードである場合、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 透過モード）、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.11-8）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** *interface-id*	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** *vlan-id*	VLAN にポートを割り当てます。指定できる 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** *interface-id*	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。

	コマンド	目的
ステップ 7	**show interfaces** *interface-id* **switchport**	表示された *Administrative Mode* および *Access Mode VLAN* 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 gigabitethernet1/0/1
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

スイッチが VTP 透過モード（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。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、多数のカスタマーに対応できます。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。

拡張範囲 VLAN の設定は VLAN データベースにはストアされません。ただし、VTP モードが透過であるため、スイッチの実行コンフィギュレーション ファイルにストアされます。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。

（注） スイッチは 4094 個の 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.11-2）を参照してください。

ここでは拡張範囲 VLAN について説明します。内容は次のとおりです。

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 11-2（P.11-8）を参照してください。拡張範囲 VLAN については MTU サイズとリモート SPAN 設定ステートしか変更できません。残りの特性はデフォルト状態のままにしておく必要があります。

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。

- 拡張範囲 VLAN を追加するには、**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、VLAN コンフィギュレーション モードを開始する必要があります。VLAN データベース コンフィギュレーション モード（開始するには **vlan database** 特権 EXEC コマンドを入力）では、拡張範囲 VLAN を追加できません。
- 拡張範囲の VLAN ID は、VLAN データベースに保存されず、VTP で認識されません。
- 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。
- 拡張範囲 VLAN を作成するときは、スイッチを VTP 透過モードにする必要があります。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。
- グローバル コンフィギュレーション モードまたは VLAN データベース コンフィギュレーション モードで、VTP モードを透過に設定できます。「VTP のディセーブル化（VTP 透過モード）」（P.12-11）を参照してください。VTP 透過モードでスイッチが始動するように、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。
- 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（128）のスパニング ツリー インスタンスが存在している場合、新たに作成されるどの VLAN でもスパニング ツリーはディセーブルになります。スイッチ上の VLAN 数がサポートされるスパニング ツリー インスタンスの最大数を超える場合は、IEEE 802.1s Multiple STP（MSTP）をスイッチに設定して、複数の VLAN を単一の STP 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 17 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 を作成して使用します。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 は拡張範囲の下部にあるため、拡張範囲 VLAN を作成する場合は、最大番号（4094）から始めて最小番号（1006）へと移り、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.11-14）を参照してください。
- スイッチは合計 1005（標準範囲および拡張範囲）の VLAN をサポートしますが、ルーテッド ポート、SVI、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。

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。このコマンドによって VLAN コンフィギュレーション モードが開始されます。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 11-2 を参照）、変更できるパラメータは MTU サイズと RSPAN 設定だけです。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。スイッチが VTP 透過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。

拡張範囲 VLAN は VLAN データベースに保存されずに、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。

（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.11-14）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 透過モードに設定し、VTP をディセーブルにします。
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）** VLAN コンフィギュレーション モードでは Command Line Interface（CLI; コマンドライン インターフェイス）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* コマンドと **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.28-17）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 透過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。

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.11-10）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	**show vlan internal usage**	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	**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 3	**interface** *interface-id*	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 を入力します。
ステップ 4	**shutdown**	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	**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	**vtp mode transparent**	VTP モードを透過に設定して拡張範囲 VLAN を作成します。
ステップ 7	**vlan** *vlan-id*	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	**exit**	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	**interface** *interface-id*	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 を入力します。
ステップ 10	**no shutdown**	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	**end**	特権 EXEC モードに戻ります。
ステップ 12	**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、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 透過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。

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。スイッチ上の VLAN ID 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。

表 11-3 に、VLAN を監視するための特権 EXEC コマンドを示します。

表 11-3　VLAN モニタリング コマンド

コマンド	目的
show interfaces [**vlan** *vlan-id*]	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** *vlan-id*]	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、スイッチ上の VLAN トランクの機能について説明します。

トランキングの概要

トランクは、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、ルータやスイッチといった他のネットワーキング デバイス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 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。

トランキング カプセル化方式は、802.1Q イーサネット インターフェイスで使用できます。802.1Q は、業界標準のトランキング カプセル化方式です。

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 35 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 11-4 に示すトランキング モードをサポートしています。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、ネイバー 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、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 dot1q** 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、トランク ポートのカプセル化タイプを選択します。

（注） Cisco IOS リリース 12.2(22)EY 以降のリリースでは、ES ポートは 802.1 カプセル化だけをサポートします。ES ポートではカプセル化を設定できません。

また、標準 DTP インターフェイスで、トランクでの ISL または 802.1Q カプセル化の使用、あるいはカプセル化タイプの自動ネゴシエーションを指定できます。DTP は、802.1Q トランク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。

（注） トンネル ポートは DTP をサポートしません。トンネル ポートの詳細については、第 15 章「IEEE 802.1Q 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。

表 11-4　レイヤ 2 インターフェイス モード

モード	機能
switchport mode access	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ションします。インターフェイスは、ネイバー 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。
switchport mode dynamic auto	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、ネイバー 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、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。
switchport mode dynamic desirable	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、ネイバー 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、トランク インターフェイスになります。
switchport mode trunk	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、ネイバー リンクのトランク リンクへの変換をネゴシエーションします。インターフェイスは、ネイバー 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。

表 11-4　レイヤ 2 インターフェイス モード （続き）

モード	機能
switchport nonegotiate	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、手動でネイバー 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。
switchport mode dot1q-tunnel	802.1Q トランク ポートと非対称リンクで接続するトンネル（非トランキング）ポートとして、インターフェイスを設定します。802.1Q トンネリングは、サービスプロバイダー ネットワーク上でカスタマー VLAN の整合性を保つために使用します。トンネル ポートの詳細については、第 15 章「IEEE 802.1Q 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 11-5 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。

（注）　Cisco IOS リリース 12.2(22)EY 以降のリリースでは、ES ポートで ISL トランクはサポートされません。**encapsulation** キーワードは、ES ポートには認識されなくなっています。

表 11-5　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
switchport trunk encapsulation dot1q	トランク リンクに 802.1Q カプセル化を指定します。
switchport trunk encapsulation isl	トランク リンクに ISL カプセル化を指定します。
switchport trunk encapsulation negotiate	インターフェイスがネイバー インターフェイスとネゴシエーションを行い、ネイバー 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 802.1Q トランクになるように指定します。これは、スイッチの標準ポートのデフォルトです。
switchport trunk dot1q ethertype *value*	802.1Q カプセル化の ethertype 値を設定します。802.1Q タグ付きフレームを識別する、標準外（非デフォルト）の 2 バイトの ethertype を選択する場合に使用します。デフォルトの ethertype 値は 0x8100 です。 このオプションは、Enhanced-Services（ES）ポート上にかぎりサポートされます。

（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。

IEEE 802.1Q の設定に関する考慮事項

（注）　Cisco IOS リリース 12.2(22)EY 以降のリリースでは、ES ポートは IEEE 802.1Q トランキングだけをサポートします。

802.1Q トランクでは、ネットワークのトランキング方式に次の制約があります。

- 802.1Q トランクを使用して接続した 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可された 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他社製のデバイスに Cisco スイッチを接続する場合、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 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 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 802.1Q スイッチ クラウドは、スイッチ間の 1 つのトランク リンクとして取り扱われます。

- 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る必要があります。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に、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。802.1Q トランクのネイティブ VLAN 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、ネットワーク内のすべての VLAN でスパニング ツリーをディセーブルにしてください。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。

- ES ポート上では、**switchport trunk dot1q ethertype** *value* 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、インターフェイス用のカスタムの ethertype 値を設定できます。この機能を使用すると、スイッチは 802.1Q タグ付きフレームを識別するために標準の 0x8100 ethertype を使用しないサードパーティ ベンダー製スイッチと相互運用できるようになります。たとえば、トランク ポートでカスタムの IEEE 802.1Q ethertype として 0x1234 を設定すると、この ethertype を含む着信フレームは、標準 802.1Q トランクの場合と同じように、ethertype の後ろのタグに含まれる VLAN に割り当てられます。標準 ethertype（0x8100）またはカスタム ethertype 値を設定したトランク ポートに着信するフレームは、有効な IEEE 802.1Q トラフィックとして取り扱われます。それ以外の ethertype を含むフレームは、そのトランクのネイティブ VLAN に割り当てられます。ethertype 値 0x8100 を持った出力トラフィックは、カスタマー ethertype にマッピングされます。

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 11-6 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 11-6　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** （注）　Cisco IOS リリースでは、これは標準ポートだけに適用されます。ES ポートは 802.1Q カプセル化だけをサポートします。
802.1Q カプセル化の ethertype 値	0x8100
VLAN 許容範囲	VLAN 1 ～ 4094
プルーニングに適格な 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（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、スイッチ上でイーサネット インターフェイスをトランク ポートとして設定する手順について説明します。

- 「他の機能との相互作用」（P.11-19）
- 「トランクでの許可 VLAN の定義」（P.11-21）
- 「プルーニング適格リストの変更」（P.11-23）
- 「タグなしトラフィック用ネイティブ VLAN の設定」（P.11-23）

（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。ネイバー 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、標準ポート トランク（またはリリース 12.1(14)AX の ES ポート トランク）はカプセル化をネゴシエーションします。ネイバー インターフェイスが ISL および 802.1Q カプセル化の両方をサポートし、両方のインターフェイスがカプセル化タイプをネゴシエーションするように設定されている場合は、トランクは ISL カプセル化を使用します。Cisco IOS リリース 12.2(22)EY 以降のリリースでは、ES ポートは 802.1Q カプセル化だけをサポートします。

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 ポートにはできません。
- トランク ポートは、トンネル ポートにはできません。
- トランク ポートは EtherChannel ポート グループにまとめることができますが、グループ内のすべてのトランクは同じ設定にしておく必要があります。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 ポートの数は 24 まで、Multiple Spanning-Tree（MST）モードで設定するトランク ポートの数は 40 までにすることを推奨します。
- トランク ポートで 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、802.1x はイネーブルになりません。802.1x 対応ポートのモード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、トランク ポートへの変更をネイバーとネゴシエーションする場合があります。ダイナミック ポートで 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、802.1x はイネーブルになりません。802.1x 対応ポートのモードをダイナミッ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。

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	**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*	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、トランキング用に設定するポートを入力します。
ステップ 3	**switchport trunk encapsulation** {**isl** | **dot1q** | **negotiate**} （ES ポートでは認識できなくなりました）	ISL または 802.1Q カプセル化をサポートするように、またはカプセル化タイプについてネイバー インターフェイスとネゴシエーションする（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。 **（注）** Cisco IOS リリース 12.2(22)EY 以降のリリースでは、**encapsulation** キーワードは ES ポートではサポートされません。ES ポートは 802.1Q カプセル化だけをサポートします。

	コマンド	目的
ステップ 4	**switchport mode** {**dynamic** {**auto** | **desirable**} | **trunk**}	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 ポートである場合、またはトランキング モードを設定する場合にかぎり必要となります）。 • **dynamic auto**：ネイバー 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**：ネイバー 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**：ネイバー 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ションします。
ステップ 5	**switchport access vlan** *vlan-id*	（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	**switchport trunk native vlan** *vlan-id*	802.1Q トランク用にネイティブ VLAN を指定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show interfaces** *interface-id* **switchport**	インターフェイスのスイッチポート設定を表示します。*Administrative Mode* および *Administrative Trunking Encapsulation* フィールドに表示されます。
ステップ 9	**show interfaces** *interface-id* **trunk**	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	**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。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、標準ポートを IEEE 802.1Q トランクとして設定する例を示します。この例では、ネイバー 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 上でユーザ トラフィック（スパニング ツリー アドバタイズメントを含む）が送受信されないように、VLAN 1 最小化機能を使用して、任意の個々の VLAN トランク リンクで VLAN 1 をディセーブルにすることができます。

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 を削除しても、インターフェイスは、たとえば、Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、Port Aggregation Protocol（PAgP; ポート集約プロトコル）、Link Aggregation Control Protocol（LACP）、ダイナミック トランキング プロトコル（DTP）、VLAN 1 内の VLAN トランキング プロトコル（VTP）などの管理トラフィックの送受信を続けます。

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。

ISL トランクまたは 802.1Q 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。 *vlan-list* 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。
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 *Trunking VLANs Enabled* 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。

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 ポートにだけ適用されます。トランク ポートごとに独自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.12-12）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	**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*	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、VLAN プルーニングを適用するトランク ポートを選択します。
ステップ 3	**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan-list* [,*vlan*[,*vlan*[,,,]]	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.12-4）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 は、2 ～ 1001 です。**拡張範囲 VLAN（VLAN ID が 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、フラッディング 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	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id* **switchport**	表示された *Pruning VLANs Enabled* フィールドの設定を確認します。
ステップ 6	**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。

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

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。

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.11-18）を参照してください。

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	**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*	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、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ます。
ステップ 3	**switchport trunk native vlan** *vlan-id*	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。 *vlan-id* では、指定できる範囲は 1 ～ 4094 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id* **switchport**	*Trunking Native Mode VLAN* フィールドの設定を確認します。
ステップ 6	**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。

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 16 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、STP ポート プライオリティの設定により、イネーブルになるポートとブロッキング ステートになるポートが決まります。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 11-2 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 11-2　STP ポート プライオリティによるロード シェアリング

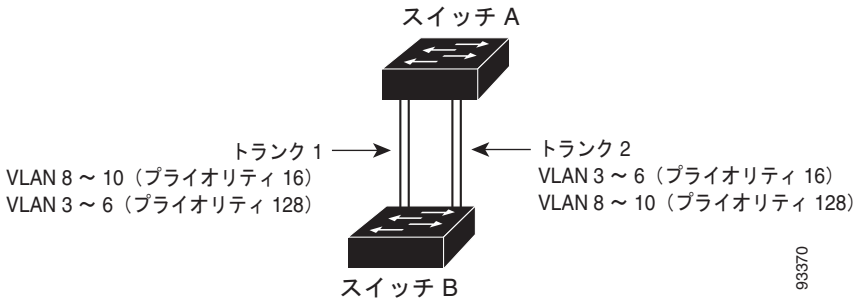


図 11-2 のようにネットワークを設定するには、特権 EXEC モードで次の手順を実行します。

	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。
ステップ 3	**vtp mode server**	スイッチ A を VTP サーバとして設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show vtp status**	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 *VTP Operating Mode* および *VTP Domain Name* フィールドをチェックします。
ステップ 6	**show vlan**	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	**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 8	**interface gigabitethernet1/ 0/1**	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、トランクに設定するインターフェイスとしてギガビット イーサネット ポート 1 を定義します。

	コマンド	目的
ステップ 9	**switchport trunk encapsulation** {**isl** | **dot1q** | **negotiate**}	ISL カプセル化または 802.1Q カプセル化をサポートするように、またはネイバー インターフェイスとネゴシエーション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。 （注）　Cisco IOS リリース 12.2(22)EY 以降のリリースでは、ES ポートは 802.1Q トランキングだけをサポートします。そのため、これらのキーワードは標準ポートだけで認識されます。
ステップ 10	**switchport mode trunk**	ポートをトランク ポートとして設定します。
ステップ 11	**end**	特権 EXEC モードに戻ります。
ステップ 12	**show interfaces gigabitethernet1/ 0/1 switchport**	VLAN 設定を確認します。
ステップ 13		スイッチの 2 番めのインターフェイスに対して、スイッチ A 上でステップ 7 ～ 11 を繰り返します。
ステップ 14		スイッチ A に設定されたトランク ポートに接続するトランク ポートを設定するため、スイッチ B でステップ 7 ～ 11 を繰り返します。
ステップ 15	**show vlan**	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	**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 17	**interface gigabitethernet1/ 0/1**	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、STP 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ます。
ステップ 18	**spanning-tree vlan 8-10 port-priority 16**	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	**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 20	**interface gigabitethernet1/0/2**	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、STP 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ます。
ステップ 21	**spanning-tree vlan 3-6 port-priority 16**	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	**end**	特権 EXEC モードに戻ります。
ステップ 23	**show running-config**	設定を確認します。
ステップ 24	**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。

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 11-3 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 11-3　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

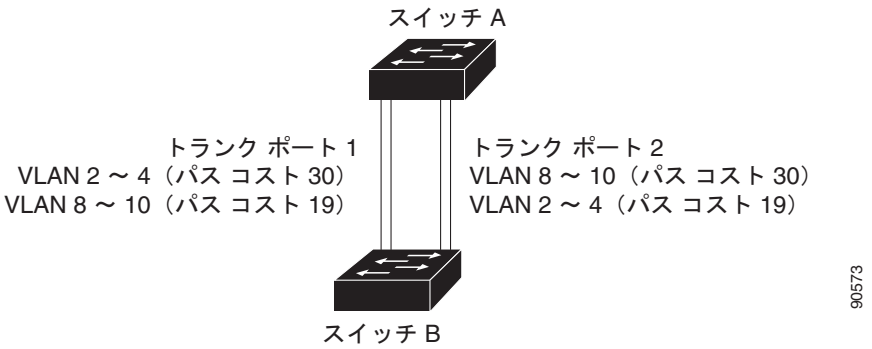


図 11-3 のようにネットワークを設定するには、特権 EXEC モードで次の手順を実行します。

	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	**interface gigabitethernet1/0/1**	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、トランクに設定するインターフェイスとしてギガビット イーサネット ポート 1 を定義します。
ステップ 3	**switchport trunk encapsulation {isl | dot1q | negotiate}**	ISL カプセル化または 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。 **（注）** Cisco IOS リリース 12.2(22)EY 以降のリリースでは、ES ポートは 802.1Q トランキングだけをサポートします。そのため、これらのキーワードは標準ポートだけで認識されます。
ステップ 4	**switchport mode trunk**	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	**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。

	コマンド	目的
ステップ 6		スイッチ A の 2 番めのインターフェイスについて、ステップ 2 ～ 4 を繰り返します。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	設定を確認します。ステップ 2 ～ 6 で設定したインターフェイスがトランク ポートになっていることを出力で確認します。
ステップ 9	**show vlan**	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。
ステップ 10	**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 11	**interface gigabitethernet1/0/1**	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、STP コストを設定するインターフェイスとしてギガビット イーサネット ポート 1 を定義します。
ステップ 12	**spanning-tree vlan 2-4 cost 30**	VLAN 2 ～ 4 のスパニング ツリー パス コストを 30 に設定します。
ステップ 13	**end**	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 ～ 11 を繰り返し、VLAN 8、9、および 10 のスパニング ツリー パス コストを 30 に設定します。
ステップ 15	**exit**	特権 EXEC モードに戻ります。
ステップ 16	**show running-config**	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	**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。

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ために使用します。ダイナミック アクセス ポートは、永続的に VLAN に割り当てられるのではなく、ポート上で認識された MAC 送信元アドレスに基づいて VLAN に割り当てられます。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し、VQP を介して通信することは可能です。

ここでは VMPS の設定について説明します。

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。このポートは、CLI または Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を使用して、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 つだけですが、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 11-7 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 11-7　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 リトライ回数	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。
- 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 802.1x をイネーブルにしようとすると、エラー メッセージが表示され、802.1x はイネーブルになりません。802.1x 対応ポートをダイナミック VLAN 割り当てに変更しようとすると、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、あとでアクセス 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 ポートにはできません。
- セキュア ポートは、ダイナミック アクセス ポートにはできません。ポートをダイナミックにするには、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 ポートにはできません。
- 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はなれません。
- ポート チャネルはダイナミック アクセス ポートとしては設定できません。

- 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ある必要があります。
- 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。スイッチを VMPS クライアントにすることは可能ですが、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	**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 server** *ipaddress* **primary**	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	**vmps server** *ipaddress*	（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	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show vmps**	表示された *VMPS Domain Server* フィールドの設定を確認します。
ステップ 6	**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。

（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 接続できる必要があります。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場合は、最初に **rcommand** 特権 EXEC コマンドを使用してクラスタ 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	**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*	エンド ステーションに接続しているスイッチ ポートのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**switchport mode access**	ポートをアクセス モードにします。
ステップ 4	**switchport access vlan dynamic**	ポートをダイナミック VLAN メンバシップ適格として設定します。 ダイナミック 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 *Operational Mode* 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 から受信したダイナミック 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**	ダイナミック 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**	ダイナミック 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 から受信した VLAN メンバシップ情報を定期的に再確認します。この再確認を行う間隔を分単位で設定できます。

クラスタのメンバー 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にする必要があります。この場合もまた、**rcommand** 特権 EXEC コマンドを使用してメンバー スイッチにログイン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*	ダイナミック 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 *Reconfirm Interval* フィールドのダイナミック 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。

リトライ回数の変更

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	**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 retry** *count*	リトライ回数を変更します。リトライ回数は 1 ～ 10 回の範囲で指定できます。デフォルトは 3 回です。
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 *Server Retry Count* フィールドの設定を確認します。
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 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 vmps 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 リトライ回数：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として設定された時間が経過すると自動的に行われます。また、**vmps reconfirm** 特権 EXEC コマンドを入力するか、SNMP の同等のコマンドを使用することによって、強制的に再確認できます。

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

```
Switch# show vmps

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 11-4 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 Trivial File Transfer Protocol（TFTP）サーバに保存されています。

図 11-4　ダイナミック ポート VLAN メンバシップの構成例