



VLAN、VTP、および VMPS の設定

この章では、Catalyst 4500 シリーズ スイッチの Virtual LAN (VLAN; 仮想 LAN) について説明します。また、VLAN トランッキング プロトコル (VTP) をイネーブルにする方法、および Catalyst 4500 シリーズ スイッチを VLAN メンバーシップ ポリシー サーバ (VMPS) クライアントとして設定する方法についても説明します。

この章の主な内容は、次のとおりです。

- 「VLAN」 (P.16-1)
- 「VLAN トランッキング プロトコル」 (P.16-8)
- 「VLAN メンバーシップ ポリシー サーバ」 (P.16-22)



(注)

この章で使用するスイッチ コマンドの構文および使用方法の詳細については、次の URL で『Cisco Catalyst 4500 Series Switch Command Reference』と関連資料を参照してください。

<http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html>

『Catalyst 4500 Series Switch Command Reference』に掲載されていないコマンドについては、より詳細な Cisco IOS ライブラリを参照してください。次の URL で『Cisco IOS Command Reference』と関連資料を参照してください。

<http://www.cisco.com/en/US/products/ps6350/index.html>

VLAN

ここでは、主に次の内容について説明します。

- 「VLAN について」 (P.16-2)
- 「VLAN 設定時の注意事項および制約事項」 (P.16-3)
- 「VLAN のデフォルト設定」 (P.16-5)
- 「VLAN の設定」 (P.16-5)

VLAN について

VLAN は、1 つまたは複数の LAN 上のデバイス グループで、実際には複数の異なる LAN セグメント上にある場合でも、同じワイヤに接続するように通信設定されています。VLAN は、物理接続ではなく論理接続に基づいているため、非常に柔軟です。



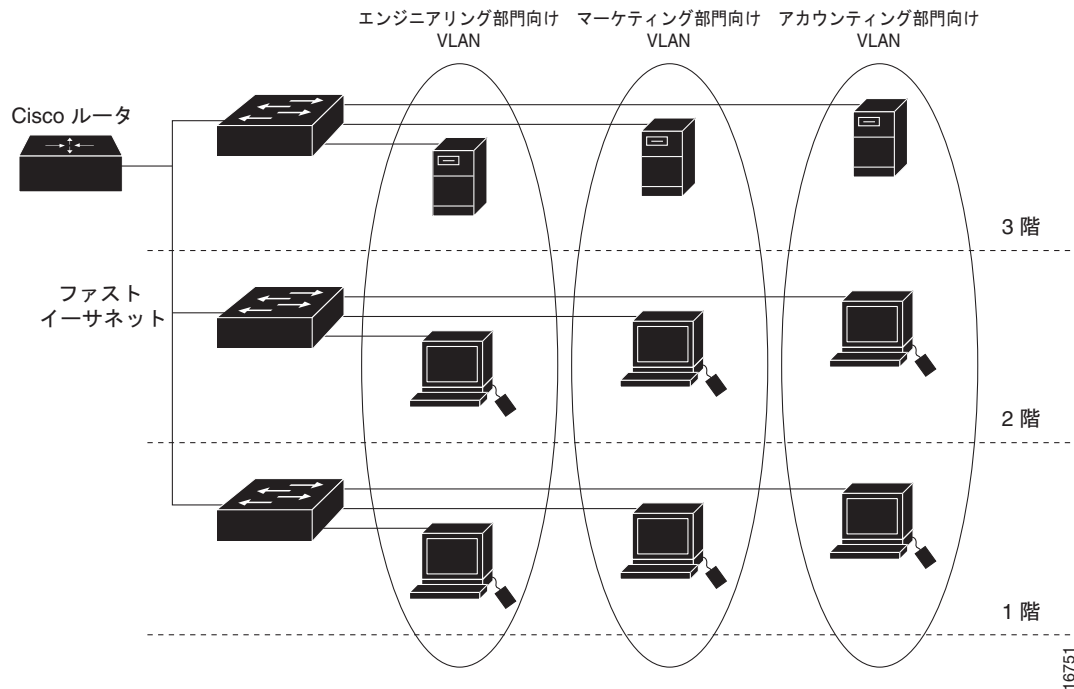
(注) VTP バージョン 3 アップデートは無差別トランク ポートを通しません。

VLAN は、レイヤ 2 ネットワークのブロードキャスト ドメインを決定します。ブロードキャスト ドメインは、設定内のいずれかのデバイスから発信されたブロードキャスト フレームを受信するすべてのデバイス セットです。ブロードキャスト ドメインは、通常、スイッチによって分割されます。これはスイッチがブロードキャスト フレームを転送しないためです。レイヤ 2 スイッチは、スイッチの設定に基づいてブロードキャスト ドメインを作成します。スイッチは、複数のブロードキャスト ドメイン作成を可能にするマルチポートブリッジです。ブロードキャスト ドメインは、スイッチ内の個々の仮想ブリッジのように機能します。

スイッチ内で 1 つまたは複数の仮想ブリッジを定義できます。スイッチ内で作成した仮想ブリッジは、新しいブロードキャスト ドメイン (VLAN) を定義します。スイッチ内、または 2 つのスイッチ間で、トラフィックが直接別の VLAN (ブロードキャスト ドメイン間) に接続されることはありません。2 つの異なる VLAN を相互接続するには、スイッチまたはレイヤ 3 スイッチを使用する必要があります。Catalyst 4500 シリーズ スイッチの VLAN 間ルーティングの詳細については、「[レイヤ 3 インターフェイスについて](#)」(P.33-1) を参照してください。

図 16-1 に、論理的に定義されたネットワークを作成する 3 つの VLAN の例を示します。

図 16-1 VLAN の例



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を同じ VLAN に所属させる場合などです。VLAN 間のトラフィックは、ルーティングする必要があります。LAN インターフェイスの VLAN メンバーシップは、インターフェイス別に割り当てする必要があります（インターフェイスベースまたはスタティックな VLAN メンバーシップと呼ばれます）。

管理ドメイン内に VLAN を作成する場合、次のパラメータを設定できます。

- VLAN 番号
- VLAN 名
- VLAN タイプ
- VLAN 状態（アクティブまたは中断）
- VLAN の Maximum Transmission Unit (MTU; 最大伝送単位)
- セキュリティアソシエーション ID (SAID)
- 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)

ソフトウェアを使用して VLAN のタイプを変換する場合は、各メディアタイプごとに異なる VLAN 番号が必要になります。

VLAN 設定時の注意事項および制約事項

ネットワーク上で VLAN を作成および変更するときは、次の注意事項および制約事項に従ってください。

- VLAN を作成する前に、Catalyst 4500 シリーズスイッチを VTP サーバモードまたは VTP トランスペアレントモードに変更してください。Catalyst 4500 シリーズスイッチが VTP サーバであれば、VTP ドメインを定義する必要があります。VTP の設定については、「[VLAN トランッキング プロトコル](#)」(P.16-8) を参照してください。
- VLAN データベースモードでは、**end** コマンドを使用できません。
- Ctrl+Z を押して、VLAN データベースモードを終了することはできません。
- マルチスパンニングツリープロトコル (MSTP) が稼働し、使用可能なすべての VLAN (4094) が設定されている Catalyst 4948 スイッチが、タイムアウトが 500 ms 未満に設定された 2 つのホットスタンバイルータープロトコル (HSRP) ピアのパスにある場合、HSRP がフラップします。

回避策：

- 使用する VLAN の数を減らします。
- 600 ms を超えるタイマーを設定します。
- **no igmp snooping** (グローバル) および **access-list hardware capture mode VLAN** コマンドを入力します。

VLAN の範囲



(注)

4094 の VLAN を使用するには、拡張システム ID をイネーブルにする必要があります。「[ブリッジ ID の概要](#)」(P.21-2) を参照してください。

Cisco IOS Release 12.2(25)EWA 以降では、Catalyst 4500 シリーズ スイッチは IEEE 802.1Q 規格に準拠し、4096 の VLAN をサポートしています。これらの VLAN は、予約、標準、拡張の 3 つの範囲に分けられます。

VLAN Trunking Protocol (VTP; VLAN トランッキング プロトコル) を使用している場合、これらの VLAN の一部はネットワーク内の他のスイッチに伝播されます。拡張範囲 VLAN は伝播されないため、ネットワーク デバイスごとに手動で設定する必要があります。

表 16-1 で、VLAN 範囲の使い方について説明します。

表 16-1 VLAN の範囲

VLAN	範囲	使用状況	VTP に よって 伝播される
0、4095	予約済み	システム専用です。これらの VLAN は参照または使用できません。	—
1	標準	シスコ システムズのデフォルトです。この VLAN は削除できません。	Yes
2 ~ 1001	標準	イーサネット VLAN 用。ユーザはこれらの VLAN を作成、使用、削除できます。	Yes
1002 ~ 1005	標準	FDDI およびトークンリング用のシスコ システムズのデフォルトです。VLAN 1002 ~ 1005 は削除できません。	Yes
1006 ~ 4094	拡張	イーサネット VLAN 専用です。拡張範囲 VLAN を設定する場合、次の点に注意してください。 <ul style="list-style-type: none"> レイヤ 3 ポートおよび一部のソフトウェア機能には、内部 VLAN が必要です。内部 VLAN は 1006 以上から割り当てます。このような用途にすでに割り当てられている VLAN を使用できません。内部で使用されている VLAN を表示するには、show vlan internal usage コマンドを入力します。 Catalyst オペレーティング システムを実行しているスイッチは、VLAN 1006 ~ 1024 の設定をサポートしません。VLAN 1006 ~ 1024 を設定する場合は、Catalyst オペレーティング システム ソフトウェアが稼働しているスイッチにその VLAN が拡張されないようにしてください。 拡張範囲 VLAN を使用するには、拡張システム ID をイネーブルにする必要があります。 	No

標準範囲の VLAN で設定できるパラメータ



(注) イーサネット VLAN 1 および 1006 ~ 4094 で使用するのは、デフォルト値だけです。

VLAN 2 ~ 1001 では、次のパラメータを設定できます。

- VLAN 名
- VLAN タイプ
- VLAN 状態 (アクティブまたは中断)

- SAID
- VLAN のスパニングツリー プロトコル (STP) タイプ

VLAN のデフォルト設定

表 16-2 に、VLAN のデフォルト設定の値を示します。

表 16-2 イーサネット VLAN のデフォルトおよび範囲

パラメータ	デフォルト	有効な値
VLAN ID	1	1 ~ 4094
VLAN 名	VLANx。x はソフトウェアで割り当てられた番号です。	範囲なし
802.10 SAID	100,001	1 ~ 4,294,967,294
MTU サイズ	1500	1500 ~ 18,190
トランスレーショナルブリッジ 1	1002	0 ~ 1005
トランスレーショナルブリッジ 2	1003	0 ~ 1005
VLAN ステート	active	active、suspend、shutdown



(注)

Catalyst 4500 シリーズ 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、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)、または Token Ring Bridge Relay Function (TrBRF; トークンリングブリッジ リレー機能) トラフィックを転送しませんが、VTP を使用して VLAN 設定を伝播します。ソフトウェアはこれらのメディア タイプのパラメータを保存しますが、これらはサポートされていません。

VLAN の設定



(注)

VLAN を設定する前に、VLAN トランキンング プロトコル (VTP) を使用して、ネットワークのグローバル VLAN 設定情報を維持する必要があります。VTP については、「[VLAN トランキンング プロトコル](#)」(P.8) を参照してください。



(注)

VLAN は、ここで紹介されている以外にも多くのパラメータをサポートしています。詳細については、『*Cisco IOS Command Reference*』を参照してください。



(注)

VLAN の設定は **vlan.dat** ファイルに保存され、vlan.dat ファイルは不揮発性メモリに保存されます。vlan.dat ファイルを手動で削除すると、VLAN データベースに矛盾が生じる可能性があります。VLAN の設定または VTP を変更する場合は、ここに記載されているコマンドおよび『*Cisco IOS Command Reference*』に記載されているコマンドを使用してください。

ここでは、VLAN の設定手順について説明します。

- 「グローバル コンフィギュレーション モードでの VLAN の設定」(P.16-6)
- 「VLAN へのレイヤ 2 LAN インターフェイスの割り当て」(P.16-8)

グローバル コンフィギュレーション モードでの VLAN の設定

スイッチが VTP サーバ モードまたはトランスペアレント モードの場合は、「[VLAN トランキンング プロトコル](#)」(P.16-8) を参照)、グローバルおよび VLAN コンフィギュレーション モードで VLAN を設定できます。VLAN をグローバルおよび config-vlan コンフィギュレーション モードで設定した場合、VLAN の設定は **running-config** または **startup-config** ファイルではなく、**vlan.dat** ファイルに保存されます。VLAN の設定を表示するには、**show vlan** コマンドを入力します。

スイッチが VLAN トランスペアレント モードの場合に、**copy running-config startup-config** コマンドを実行すると、VLAN の設定が **startup-config** ファイルに保存されます。実行コンフィギュレーションをスタートアップ コンフィギュレーションとして保存したあとに、**show running-config** コマンドおよび **show startup-config** コマンドを実行すると、VLAN の設定が表示されます。



(注)

スイッチの起動時に、**startup-config** ファイルおよび **vlan.dat** ファイル内の VTP ドメイン名と VTP モードが異なる場合、スイッチは **vlan.dat** ファイル内の設定を使用します。

ポート メンバーシップ モードを定義したり、VLAN のポートを追加および削除するには、インターフェイス コンフィギュレーション コマンド モードを使用します。これらのコマンドの結果は、**running-config** 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** コマンドを使用します。

ユーザ設定 VLAN には 1 ~ 4094 の一意の ID があります。VLAN を作成するには、**vlan** コマンドと使用されていない ID を入力します。特定の ID が使用されているかどうかを確認するには、**show vlan id ID** コマンドを入力します。VLAN を修正する場合は、既存の VLAN に **vlan** コマンドを使用します。

VLAN の作成時に割り当てられるデフォルト パラメータの一覧は、「[VLAN のデフォルト設定](#)」(P.16-5) を参照してください。**media** キーワードを使用しないで VLAN タイプを指定する場合、VLAN はイーサネット VLAN になります。

VLAN を作成する手順は、次のとおりです。

	コマンド	目的
ステップ1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	Switch(config)# vlan <i>vlan_ID</i> Switch(config-vlan)#	イーサネット VLAN を追加します。 (注) イーサネット VLAN 1 および FDDI、またはトークンリング VLAN 1002 ~ 1005 のメディア タイプのデフォルト VLAN は削除できません。 VLAN を削除する場合は、この VLAN に割り当てられたアクセス ポートとして設定された LAN インターフェイスはいずれも、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。 VLAN を削除する場合は no キーワードを使用します。 Switch(config-vlan)# と表示される場合、VLAN コンフィギュレーション モードで実行しています。新しく作成された VLAN のパラメータを変更する場合は、このモードを使用します。
ステップ3	Switch(config-vlan)# end	VLAN コンフィギュレーション モードからイネーブル モードに戻ります。
ステップ4	Switch# show vlan [<i>id</i> <i>name</i>] <i>vlan_name</i>	VLAN の設定を確認します。

イーサネット VLAN を作成または変更する場合は、次の点に注意してください。

- レイヤ 3 ポートおよび一部のソフトウェア機能には、1006 以上から昇順に内部 VLAN を割り当てる必要があるため、拡張範囲 VLAN は 4094 から降順に設定してください。
- 拡張範囲 VLAN が設定できるのはグローバル コンフィギュレーション モードだけです。VLAN データベース モードでは拡張範囲 VLAN を設定できません。
- レイヤ 3 ポートおよび一部のソフトウェア機能は、拡張範囲 VLAN を使用しています。作成または変更対象の VLAN がレイヤ 3 ポートまたはソフトウェア機能によって使用中の場合、スイッチからメッセージが表示され、VLAN 設定は変更されません。
- VLAN コンフィギュレーション コマンドで VLAN を作成すると、既存の VTP ドメインに自動的に追加されます。ユーザのアクションは必要ではありません。

次に、グローバル コンフィギュレーション モードでイーサネット VLAN を作成し、設定を確認する例を示します。

```
Switch# configure terminal
Switch(config)# vlan 3
Switch(config-vlan)# end
Switch# show vlan id 3
VLAN Name                Status    Ports
-----
3    VLAN0003                active
VLAN Type  SAID       MTU    Parent RingNo BridgeNo Stp    BrdgMode Trans1 Trans2
-----
3    enet    100003   1500    -     -     -     -     -     0     0
Primary Secondary Type                Interfaces
-----
Switch#
```

VLAN へのレイヤ 2 LAN インターフェイスの割り当て

管理ドメイン内で作成された VLAN は、VLAN に 1 つまたは複数の LAN インターフェイスを割り当てるまで未使用の状態のままとなります。



(注)

適切なタイプの VLAN に LAN インターフェイスを割り当ててください。イーサネットタイプの VLAN には、ファストイーサネットインターフェイス、ギガビットイーサネットインターフェイス、10 ギガビットイーサネットインターフェイスを割り当てます。

VLAN に 1 つまたは複数の LAN インターフェイスを割り当てるには、「レイヤ 2 スイッチング用のイーサネットインターフェイスの設定」(P.18-5) に記載されている作業を行います。

VLAN トランッキング プロトコル

ここでは、Catalyst 4500 シリーズ スイッチの VLAN トランッキング プロトコル (VTP) と、次の内容について説明します。

- 「VTP について」(P.16-8)
- 「VTP 設定時の注意事項および制約事項」(P.16-13)
- 「VTP のデフォルト設定」(P.16-14)
- 「VTP の設定」(P.16-15)

VTP について

VTP はレイヤ 2 のメッセージング プロトコルであり、VTP ドメインでの VLAN の追加、削除、名前変更などを管理することにより、VLAN 設定の整合性を維持します。VTP ドメイン (別名、VLAN 管理ドメイン) は、同じ VTP ドメイン名を共有し、トランクで相互接続された 1 つ以上のネットワーク デバイスで構成されます。VTP を使用すると、VLAN 名の重複、無効な VLAN タイプの指定、セキュリティ違反などのさまざまな問題によって生じる設定ミスおよび設定の矛盾が最小限に抑えられます。

VLAN を作成する前に、ネットワークで VTP を使用するかどうかを決定する必要があります。VTP を使用すると、1 台または複数のネットワーク デバイス上で中央集約的に設定変更を行い、それらの変更を自動的にネットワーク上の他のネットワーク デバイスに伝達することができます。VLAN の設定の詳細については、「VLAN」(P.16-1) を参照してください。

ここでは、VTP の機能について説明します。

- 「VTP ドメインの概要」(P.16-9)
- 「VTP モードの概要」(P.16-9)
- 「VTP アドバタイズの概要」(P.16-10)
- 「VTP バージョンの概要」(P.16-10)
- 「VTP プルーニングの概要」(P.16-12)

VTP ドメインの概要

VTP ドメインは、同じ VTP ドメイン名を共有し、相互接続された 1 台または複数のネットワーク デバイスで構成されます。1 台のネットワーク デバイスが所属できる VTP ドメインは 1 つだけです。ドメインのグローバル VLAN 設定を変更するには、Command-Line Interface (CLI; コマンドライン インターフェイス) または Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) を使用します。

デフォルトでは、Catalyst 4500 シリーズ スイッチは VTP サーバ モードであり、スイッチがトランク リンクを介してドメインについてのアドバタイズメントを受信するか、ユーザが管理ドメインを設定しない限り、ドメインは NULL に設定されます。管理ドメイン名を指定するか、スイッチがドメイン名を学習するまで、VTP サーバ上での VLAN の作成または変更はできません。

スイッチが、トランク リンクを介して VTP アドバタイズを受信した場合、管理ドメイン名および VTP 設定のリビジョン番号を継承します。スイッチは、別の管理ドメイン名または古い設定のリビジョン番号が指定されたアドバタイズについては無視します。

スイッチを VTP トランスペアレントとして設定した場合、VLAN の作成および変更は可能ですが、その変更が作用するのは個々のスイッチに限られます。

VTP サーバ上の VLAN 設定を変更すると、その変更は VTP ドメイン内のすべてのネットワーク デバイスに伝播されます。VTP アドバタイズメントは、すべてのスイッチ間リンク (ISL) と IEEE 802.1Q トランク接続に伝送されます。

VTP は、一意の名前と内部インデックスの対応によって、複数の LAN タイプに対して VLAN をダイナミックにマッピングします。このマッピングにより、ネットワーク管理者の不要なデバイス管理が軽減されます。

VTP モードの概要

次のいずれかの VTP モードで動作するように Catalyst 4500 シリーズ スイッチを設定できます。

- サーバ: VTP サーバモードでは、VLAN の作成、変更、および削除を行えます。また、VTP ドメイン全体に対して他の設定パラメータ (VTP バージョン、VTP プルーニングなど) を指定できます。VTP サーバは、同一 VTP ドメイン内の他のネットワーク デバイスに、自らの VLAN 設定をアドバタイズし、トランク リンクを介して受信したアドバタイズに基づいて、自らの VLAN 設定を他のネットワーク デバイスと同期させます。VTP サーバがデフォルトのモードです。



(注) VTP バージョン 3 では、VLAN の操作はプライマリ サーバに対してのみ行われます。

- クライアント: VTP クライアントは、VTP サーバと同様に動作しますが、VTP クライアント上で VLAN の作成、変更、または削除を行うことはできません。
- 透過的: VTP 透過ネットワーク装置は、VTP に関与しません。VTP トランスペアレント ネットワーク デバイスは、VLAN 設定をアドバタイズせず、受信したアドバタイズに基づいて同期させることもありません。ただし VTP バージョン 2 では、トランスペアレント ネットワーク デバイスは、トランッキング LAN インターフェイスで受信した VTP アドバタイズメントを転送します。
- オフ: VTP オフ モードでは、ネットワーク デバイス機能は、VTP トランスペアレント デバイスと同じ方法で動作します。ただし、VTP アドバタイズは転送されません。



(注) Catalyst 4500 シリーズ スイッチは、スイッチが Nonvolatile RAM (NVRAM; 不揮発性 RAM) への設定の書き込み中に障害を検出すると、自動的に VTP サーバ モードから VTP クライアント モードに切り替わります。この場合、NVRAM が正常に動作するまで、スイッチを VTP サーバ モードに戻すことはできません。

VTP アドバタイズの概要

VTP ドメインの各ネットワーク デバイスは、予約されたマルチキャスト アドレスに対して、各トランッキング LAN インターフェイスからアドバタイズメントを定期的送信します。VTP アドバタイズを受信した隣接するネットワーク デバイスは、必要に応じて各自の VTP および VLAN 設定を更新します。

VTP アドバタイズでは、次のグローバル設定情報が配信されます。

- VLAN ID (ISL および 802.1Q)
- エミュレートされた LAN 名 (Asynchronous Transfer Mode (ATM; 非同期転送モード) LAN Emulation (LANE; LAN エミュレーション) 用)
- 802.10 SAID 値 (FDDI)
- VTP ドメイン名
- VTP 設定のリビジョン番号
- 各 VLAN の最大伝送単位 (MTU) サイズを含めた VLAN 設定
- フレーム形式

VTP バージョンの概要

VTP バージョン 2

ネットワークで VTP を使用する場合は、VTP バージョン 2 またはバージョン 3 のどちらを使用するかを決定する必要があります。



(注)

Catalyst 4500 シリーズ 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、トークンリング コンセントレータ リレー機能 (TrCRF)、またはトークンリングブリッジリレー機能 (TrBRF) トラフィックを転送しません。VTP を使用して VLAN 設定を伝播します。

VTP バージョン 1 ではサポートされず、バージョン 2 でサポートされる機能は、次のとおりです。

- トークンリングサポート：トークンリング LAN スwitチングと VLAN (TrBRF と TrCRF) をサポートします。
- 認識不能な Type-Length-Value (TLV) のサポート：VTP サーバまたは VTP クライアントは、TLV が解析不能であっても、設定の変更を他のトランクに伝播します。認識不可能な TLV は、NVRAM に保存されます。
- バージョン依存型トランスペアレントモード：VTP バージョン 1 およびバージョン 2 の場合、VTP トランスペアレント ネットワーク デバイスは、バージョンを確認せずに VTP メッセージをトランスペアレントモードで転送します。
- 整合性検査：VTP バージョン 2 の場合、CLI (コマンドライン インターフェイス)、または SNMP (簡易ネットワーク管理プロトコル) を介して新しい情報が入力された場合に限り、VLAN 整合性検査 (VLAN 名、値など) を行います。VTP メッセージから新しい情報を取得した場合、または NVRAM から情報を読み込んだ場合には、整合性検査を行いません。受信した VTP メッセージのダイジェストが正しい場合は、整合性検査を行わずにその情報が受け入れられます。

VTP バージョン 3

VTP バージョン 1 およびバージョン 2 ではサポートされず、バージョン 3 でサポートされる機能は、次のとおりです。

- 非表示のパスワードのサポート：パスワードを **hidden** または **secret** として設定するオプションをサポートします。

hidden キーワードを指定すると、ドメインで **takeover** コマンドが発行された場合、パスワードを再入力する必要があります。パスワード文字列から生成される秘密キーが、**const_nvram:vlan.dat** ファイルに保存されます。このオプションを使用して設定する場合、パスワードは、設定内では普通の文字列としては表示されません。代わりに、パスワードに関連付けられている秘密キーが、実行中の設定で 16 進数の形式で保存されます。**hidden** キーワードが指定されていない場合、VTP バージョン 1 および VTP バージョン 2 のように、**const_nvram:vlan.dat** にクリア テキストとして保存されます。

secret キーワードが指定される場合、パスワードの秘密キーは直接設定できます。

- 拡張 VLAN データベース伝播のサポート：VTP バージョン 2 では、VLAN 番号 1 から 1000 の VLAN 設定情報だけが伝播されます。VTP バージョン 3 では、情報は、VLAN 拡張範囲 (VLAN 番号 1006 から 4094) にも伝播されます。
- VTP バージョン 1、VTP バージョン 2、または VTP バージョン 3 が稼働している Catalyst 4500 シリーズ スイッチでは、デフォルトの VLAN 1 および 1002 ~ 1005 は変更できません。



(注) VTP プルーニングは、VLAN 番号 1 から 1000 だけに、引き続き適用されます。

- ドメイン内のデータベースの伝播：VLAN データベース情報の伝播に加え、VTP では、Multiple Spanning Tree (MST) プロトコル データベース情報も伝播できます。
- VTP のディセーブル化：トランッキング ポートで VTP がディセーブルになっているときには、そのポート上のすべての VTP インスタンスに適用されます。VTP がグローバルにディセーブル化されているときには、システム内のすべてのトランッキング ポートに設定が適用されます。
- VTP バージョン 1 および VTP バージョン 2 では、VTP サーバの役割は、データベースを NVRAM にバックアップすることと、管理者がデータベース情報を変更できるようにすることです。VTP バージョン 3 では、VTP プライマリ サーバと VTP セカンダリ サーバの役割が導入されました。VTP プライマリ サーバは、データベース情報をアップデートするために使用されます。送信されたアップデートは、システム内のすべてのデバイスで受け取られます。VTP セカンダリ サーバは、VTP 設定を VTP プライマリ サーバからのアップデートを使用して受信した NVRAM にバックアップできます。

プライマリ サーバとセカンダリ サーバのステータスは、実行時のステータスで、設定可能なオプションではありません。デフォルトでは、すべてのデバイスがセカンダリ サーバに割り当てられます。プライマリ サーバのステータスが必要になるのは、データベースのアップデートが必要な場合だけです。また、プライマリ サーバのステータスは、管理者がドメインから **takeover** メッセージを発行したときに取得されます。「[テイクオーバーの起動](#)」(P.16-20) を参照してください。

デバイスのリロードのときか、スイッチオーバー パラメータまたはドメイン パラメータが変更されるときに、プライマリ サーバのステータスが失われます。セカンダリ サーバでは、設定がバックアップされ、その伝播が継続されます。このため、プライマリ サーバがなくても VTP ドメインが機能する場合があります。

VTP プルーニングの概要

VTP プルーニングは、ブロードキャスト パケット、マルチキャスト パケット、ユニキャスト パケットなど、不要なフラッディング トラフィックを削減することにより、ネットワークの帯域幅を拡張します。VTP プルーニングを使用すると、トラフィックがネットワーク デバイスにアクセスするために使用しなければならない トランク リンクへのフラッディング トラフィックが制限されるので、使用可能な帯域幅が増えます。VTP プルーニングは、デフォルトではディセーブルに設定されています。

VTP プルーニングを有効にするには、管理ドメイン内のすべてのデバイスが VTP プルーニングをサポートする必要があります。VTP プルーニングをサポートしないデバイスについては、トランク上で VLAN を使用できるように手動で設定する必要があります。

図 16-2 に、VTP プルーニングを使用しない場合のスイッチド ネットワークを示します。スイッチ 1 のインターフェイス 1 およびスイッチ 4 のインターフェイス 2 は、Red という VLAN に割り当てられています。スイッチ 1 に接続されたホストから、ブロードキャストが送信されます。スイッチ 1 は、このブロードキャストをフラッディングします。Red VLAN にインターフェイスを持たないスイッチ 3、5、6 も含めて、ネットワーク内のすべてのネットワーク デバイスがこのブロードキャストを受信します。

プルーニングの設定は、Catalyst 4500 シリーズ スイッチ上でグローバルに行います（「VTP プルーニングのイネーブル化」(P.16-17) を参照）。

図 16-2 VTP プルーニングを使用しない場合のフラッディング トラフィック

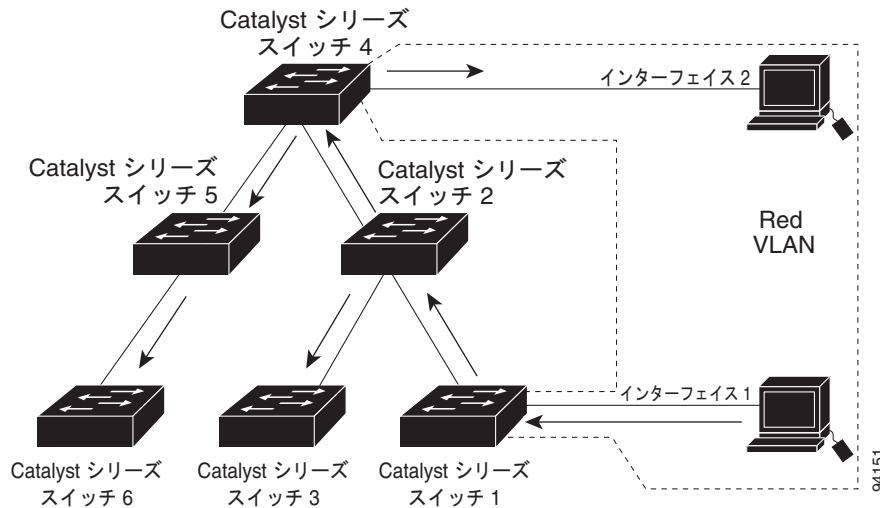
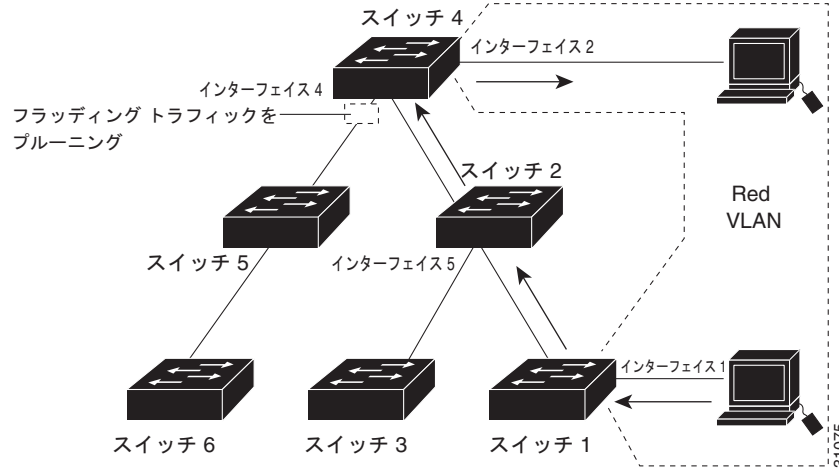


図 16-3 は、VTP プルーニングをイネーブルにした場合と同じスイッチド ネットワークを示しています。Red VLAN へのトラフィックは指定されたリンク（スイッチ 2 のインターフェイス 5 およびスイッチ 4 のインターフェイス 4）でプルーニングされるので、スイッチ 1 からのブロードキャスト トラフィックは、スイッチ 3、5、6 に転送されません。

図 16-3 VTP プルーニングを使用した場合のフラッディング Traffic



VTP サーバで VTP プルーニングをイネーブルにすると、管理ドメイン全体でプルーニングがイネーブルになります。VTP プルーニングは、イネーブルにしてから数秒後に有効になります。デフォルトでは、VLAN 2 ~ 1000 がプルーニング適格です。VTP プルーニング不適格の VLAN からのトラフィックは、プルーニングの対象になりません。VLAN 1 は常にプルーニング不適格です。VLAN 1 からのトラフィックはプルーニングできません。

トランキング LAN インターフェイスに VTP プルーニングを設定するには、**switchport trunk pruning vlan** コマンドを使用します。VTP プルーニングは、LAN インターフェイスがトランキングを実行している場合に作用します。VTP ドメインで VTP プルーニングがイネーブルまたはディセーブルのどちらかに設定されているか、特定の VLAN が存在するかどうか、および LAN インターフェイスが現在トランキングを実行しているかどうかにかかわらず、VLAN プルーニングを設定できます。

VTP 設定時の注意事項および制約事項

ネットワークに VTP を実装する場合、次の注意事項および制約事項に従ってください。

- スーパーバイザ エンジンの冗長構成は、デフォルト以外の VLAN データ ファイル名または場所をサポートしません。冗長スーパーバイザ エンジンが搭載されたスイッチ上で、**vtp file file_name** コマンドを入力しないでください。
- 冗長スーパーバイザ エンジンを搭載する前に、デフォルト設定に戻るには **no vtp file** コマンドを入力します。
- トランク ポート上の VTP バージョン 3 デバイスで、VTP バージョン 2 デバイスからのメッセージを受信すると、その特定のトランク上の VLAN データベースのスケール ダウン バージョンを VTP バージョン 2 の形式で送信します。VTP バージョン 3 デバイスは、トランクで最初に VTP バージョン 2 パケットを受信しない限り、そのトランク ポートで VTP バージョン 2 形式のパケットを送信しません。
- VTP バージョン 3 デバイスはトランク ポートで VTP バージョン 2 デバイスを検出しても、VTP バージョン 2 パケットに加えて VTP バージョン 3 パケットを引き続き送信して、トランク外で 2 種類のネイバーが共存できるようにします。
- VPT バージョン 3 デバイスは、VTP バージョン 2 またはバージョン 1 デバイスからの設定情報は受け入れません。
- VPT バージョン 2 とは異なり、VTP がバージョン 3 として設定されても、ドメイン内のすべてのバージョン 3 対応デバイスは VPT バージョン 3 システムとしての動作を開始するように設定されません。

- バージョン 2 またはバージョン 3 の機能をサポートする VTP バージョン 1 デバイスで、VTP バージョン 3 パケットを受信すると、VTP バージョン 2 の機能との矛盾が存在しない場合は、このデバイスは VTP バージョン 2 として設定されます。
- VTP バージョン 1 にだけ対応するデバイスは、VTP バージョン 3 デバイスとの相互運用はできません。
- トークンリング環境では、トークンリング VLAN スイッチング機能を正常に動作させるために、VTP バージョン 2 またはバージョン 3 をイネーブルにする必要があります。
- 2 つの VTP バージョン 3 の領域は、VTP バージョン 1 または VTP バージョン 2 の領域を介して、トランスペアレント モードでのみ通信が可能です。
- VTP ドメイン内のすべてのネットワーク デバイスで、同じ VTP バージョンを実行する必要があります。
- VTP がセキュア モードの場合、管理ドメイン内の各ネットワーク デバイスにパスワードを設定する必要があります。

**注意**

セキュア モードで VTP を設定し、ドメイン内の各ネットワーク デバイスに管理ドメイン パスワードを割り当てなかった場合、管理ドメインは正常に動作しません。

- VTP バージョン 2 対応のネットワーク デバイス上で VTP バージョン 2 をディセーブルに設定している場合、その VTP バージョン 2 対応ネットワーク デバイスは、同一 VTP ドメイン内で VTP バージョン 1 が稼働しているネットワーク デバイスとして動作します (VTP バージョン 2 は、デフォルトでディセーブルに設定されています)。
- 同一 VTP ドメイン内のすべてのネットワーク デバイスがバージョン 2 に対応する場合を除き、ネットワーク デバイス上で VTP バージョン 2 をイネーブルにしないでください。1 台のサーバ上で VTP バージョン 2 をイネーブルにすると、ドメイン内のすべてのバージョン 2 対応ネットワーク デバイスで VTP バージョン 2 がイネーブルになります。
- VTP サーバ上で VTP プルーニングをイネーブルまたはディセーブルにすると、管理ドメイン全体で VTP プルーニングがイネーブルまたはディセーブルになります。
- Catalyst 4500 シリーズ スイッチ上で VLAN をプルーニング適格または不適格として設定する場合、設定が有効なのは、そのスイッチ上の VLAN のプルーニングだけです。VTP ドメイン内のすべてのネットワーク デバイスに対して有効となるわけではありません。
- VLAN データベースは、システム上で実行中の VTP バージョンに準拠する形式で、NVRAM ファイルに保存されます。VTP バージョン 2 だけをサポートする古いイメージでは、VTP バージョン 3 ファイル形式は認識されないため、VTP がサポートされる新しいイメージからサポートされないイメージにシステムがダウングレードされた場合、NVRAM VLAN データベースの情報は失われます。

VTP のデフォルト設定

表 16-3 に、VTP のデフォルト設定を示します。

表 16-3 VTP のデフォルト設定

機能	デフォルト値
VTP ドメイン名	スル
VTP モード	サーバ
VTP バージョン 2 のイネーブル ステータス	バージョン 2 はディセーブル

表 16-3 VTP のデフォルト設定 (続き)

機能	デフォルト値
VTP パスワード	なし
VTP プルーニング	ディセーブル

新たに出荷された Catalyst 4500 スーパーバイザ エンジン、Catalyst 4900 シリーズ スイッチ、および Cisco ME 4924-10GE スイッチのデフォルト VTP モードはトランスペアレントです。vlan.dat を削除するか、**erase cat4000_flash:** コマンドを発行して、スイッチをリセットすると、VTP モードがサーバモードに変わります。

VTP の設定

ここでは、VTP の設定手順について説明します。

- 「VTP グローバル パラメータの設定」(P.16-15)
- 「VTP モードの設定」(P.16-18)
- 「テイクオーバーの起動」(P.16-20)
- 「VTP 統計情報の表示」(P.16-21)
- 「ドメイン内の VTP デバイスの表示」(P.16-21)

VTP グローバル パラメータの設定

ここでは、VTP グローバル パラメータの設定について説明します。

- 「VTP パスワードの設定」(P.16-16)
- 「VTP プルーニングのイネーブル化」(P.16-17)
- 「VTP バージョン番号のイネーブル化」(P.16-17)



(注)

VTP グローバル パラメータは、グローバル コンフィギュレーション モード、または EXEC モードで入力できます。

VTP パスワードの設定

VTP グローバル パラメータを設定するには、次のコマンドを使用します。

コマンド	目的
Switch(config)# vtp password <i>password_string</i> [hidden secret]	VTP ドメインのパスワード (8 ~ 64 文字) を設定します。 VTP バージョン 3 では、 hidden キーワードおよび secret キーワードを使用できます。 <ul style="list-style-type: none"> hidden キーワードが使用される場合、パスワード文字列から生成される秘密キーが、<code>const_nvram:vlan.dat</code> ファイルに保存されません。<code>takeover</code> コマンドを使用すると、パスワードを再入力する必要があります。 secret キーワードが使用される場合、パスワードの秘密キーは直接設定できます。secret パスワードには 32 文字の 16 進文字を設定する必要があります。
Switch(config)# no vtp password	パスワードを消去します。

次に、グローバル コンフィギュレーション モードで VTP パスワードを設定する例を示します。

```
Switch# configure terminal
Switch(config)# vtp password WATER
Setting device VLAN database password to WATER.
Switch#
```

次に、EXEC モードで VTP パスワードを設定する例を示します。

```
Switch# vtp password WATER
Setting device VLAN database password to WATER.
Switch#
```



(注)

パスワードは実行コンフィギュレーション ファイルには保存されません。

次に、**hidden** パスワードを設定する例を示します。

```
Switch# configure terminal
Switch(config)# vtp password WATER hidden
Generating the secret associated to the password.
Switch(config)#
```

この例では、**hidden** キーワードを指定して設定したときに、パスワード WATER が表示される方法を示します。

```
Switch# show vtp password
VTP Password: 89914640C8D90868B6A0D8103847A733
Switch#
```


VTP プルーニングのイネーブル化

管理ドメイン内で VTP プルーニングをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ1	Switch(config)# vtp pruning	管理ドメイン内で VTP プルーニングをイネーブルにします。
ステップ2	Switch# show vtp status include pruning	(任意) 設定を確認します。

次に、VTP プルーニングを管理ドメイン内でイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# vtp pruning
Pruning switched ON
```

次に、リリースに関係なく、管理ドメイン内で VTP プルーニングをイネーブルにする例を示します。

```
Switch# vtp pruning
Pruning switched ON
```

次に、設定を確認する例を示します。

```
Switch# show vtp status | include Pruning
VTP Pruning Mode: Enabled
Switch#
```

プルーニング適格性の設定については、「[VTP プルーニングの概要](#)」(P.16-12) を参照してください。

VTP バージョン番号のイネーブル化

VTP バージョン 2 対応のネットワーク デバイスでは、デフォルトで VTP バージョン 2 がディセーブルに設定されています。1 台のネットワーク デバイス上で VTP バージョン 2 をイネーブルにすると、VTP ドメイン内のすべての VTP バージョン 2 対応ネットワーク デバイスでバージョン 2 がイネーブルになります。



注意

同一 VTP ドメイン内のネットワーク デバイスに関して、VTP バージョン 1 とバージョン 2 の間のインターオペラビリティはありません。VTP ドメイン内のすべてのネットワーク デバイスで、同じ VTP バージョンを使用する必要があります。VTP ドメイン内のすべてのネットワーク デバイスが VTP バージョン 2 をサポートしている場合を除き、VTP バージョン 2 をイネーブルにしないでください。



(注)

トークンリング環境では、トークンリング インターフェイスをサポートするデバイス上でトークンリング VLAN スイッチングを正常に動作させるために、VTP バージョン 2 または VTP バージョン 3 をイネーブルにする必要があります。

VTP バージョンをイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ1	Switch(config)# vtp version {1 2 3}	VTP バージョンをイネーブルにします。
ステップ2	Switch# show vtp status include {v1 v2 v3}	(任意) 設定を確認します。

次に VTP バージョン 2 をイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# vtp version 2
V2 mode enabled.
Switch(config)#
```

次に、リリースに関係なく、VTP バージョン 2 をイネーブルにする例を示します。

```
Switch# vtp version 2
V2 mode enabled.
Switch#
```

次に、設定を確認する例を示します。

```
Switch# show vtp status | include V2
VTP V2 Mode: Enabled
Switch#
```

VTP モードの設定

VTP モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch(config)# vtp mode {client server transparent off}	VTP モードを設定します。
ステップ 2	Switch(config)# vtp domain domain_name	(任意：サーバモード専用) VTP ドメイン名を定義します (最大 32 文字)。VTP サーバモードではドメイン名が必要です。スイッチが VTP ドメインにトランク接続されている場合、スイッチはドメイン内の VTP サーバからドメイン名を取得します。 (注) ドメイン名は消去できません。
ステップ 3	Switch(config)# end	VLAN コンフィギュレーション モードを終了します。
ステップ 4	Switch# show vtp status	(任意) 設定を確認します。



(注)

VTP がディセーブルの場合は、VLAN データベース モードでなく、コンフィギュレーション モードで VLAN コンフィギュレーション コマンドを入力でき、VLAN 設定はスタートアップ コンフィギュレーション ファイルに保存されます。

次に、スイッチを VTP サーバとして設定する例を示します。

```
Switch# configure terminal
Switch(config)# vtp mode server
Setting device to VTP SERVER mode.
Switch(config)# vtp domain Lab_Network
Setting VTP domain name to Lab_Network
Switch(config)# end
Switch#
```

次に、スイッチを VTP クライアントとして設定する例を示します。

```
Switch# configure terminal
Switch(config)# vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)# end
Switch#
```

次に、スイッチ上で VTP をディセーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Switch(config)# end
Switch#
```

次に、スイッチ上で VTP をディセーブルにし、VTP アドバタイズメントの転送をディセーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vtp mode off
Setting device to VTP OFF mode.
Switch(config)# end
Switch#
```

次に、デバイスで VTP バージョン 1 を実行しているときの、VTP 設定パラメータの例を示します。

```
Switch# show vtp status
VTP Version capable           : 1 to 3
VTP version running          : 1
VTP Domain Name               : Lab_Network
VTP Pruning Mode              : Enabled
VTP Traps Generation          : Disabled
Device ID                     : 0016.9c6d.5300
Configuration last modified by 127.0.0.12 at 10-18-07 10:12:42
Local updater ID is 127.00.12 at 10-18-07 10:2:42

Feature VLAN:
-----
VTP Operating Mode            : Server
Maximum number of existing VLANs : 5
Configuration Revision        : 1
MD5 digest                    : 0x92 0xF1 0xE8 0x52 0x2E 0x5C 0x36 0x10 0x70 0x61 0xB8
                                0x24 0xB6 0x93 0x21 0x09

Switch#
```

次に、デバイスで VTP バージョン 2 を実行しているときの、VTP 設定パラメータの例を示します。

```
Switch# show vtp status
VTP Version capable           : 1 to 3
VTP version running          : 2
VTP Domain Name               : Lab_Network
VTP Pruning Mode              : Disabled
VTP Traps Generation          : Disabled
Device ID                     : 0012.44dc.b800
Configuration last modified by 127.0.0.12 at 10-18-07 10:38:45
Local updater ID is 127.0.0.12 on interface EO 0/0 (first interface found)

Feature VLAN:
-----
VTP Operating Mode            : Server
Maximum VLANs supported locally: 1005
Number of existing VLANs      : 1005
Configuration Revision        : 1
MD5 digest                    : 0x2E 0x6B 0x99 0x58 0xA2 0x4F 0xD5 0x150x70 0x61 0xB8
                                0x24 0xB6 0x93 0x21 0x09

Switch#
```

次に、デバイスで VTP バージョン 3 を実行しているときの、VTP 設定パラメータの例を示します。

```
Switch# show vtp status
VTP Version capable      : 1 to 3
VTP version running     : 3
VTP Domain Name         : Lab_Network
VTP Pruning Mode        : Disabled
VTP Traps Generation    : Disabled
Device ID                : 0012.44dc.b800

Feature VLAN:
-----
VTP Operating Mode      : Server
Number of existing VLANs : 1005
Number of existing extended VLANs: 3074
Configuration Revision  : 18
Primary ID              : 0012.4371.9ec0
Primary Description     :
Switch#
```

テイクオーバーの起動

この手順は、VTP バージョン 3 だけに適用されます。テイクオーバーを起動するには、次の作業を行います。

コマンド	目的
Switch# vtp primary-server [vlan mst] [force]	<p>スイッチの動作ステートをセカンダリ サーバからプライマリ サーバに変更し、設定をドメイン全体にアドバタイズします（このデバイスのパスワードが hidden キーワードで設定された場合、ユーザに対し、再入力を促すプロンプトが表示されます）。</p> <p>(注) force キーワードを使用すると、設定が矛盾するすべてのサーバで設定が上書きされます。force キーワードを使用しない場合は、テイクオーバーを続行する前に確認が求められます。</p> <p>適切な機能 (vlan または mst) を選択することによって、テイクオーバーの場所を指定します。機能が選択されていない場合、テイクオーバーは VLAN データベースに対して実行されます。</p>

次に、テイクオーバーを起動し、vlan データベースに対して実行する例を示します。

```
Switch# vtp primary-server vlan
Enter VTP password:password
This system is becoming primary for feature vlan

VTP Feature Conf Revision Primary Server Device ID      Description
-----
MST          Yes  4          0012.4371.9ec0=0012.4371.9ec0 R1
Do you want to continue? (confirm)
Switch#
```

VTP 統計情報の表示

送受信された VTP アドバタイズ、VTP エラーなどの VTP 統計情報を表示するには、次の作業を実行します。

コマンド	目的
Switch# show vtp counters	VTP の統計情報を表示します。

次に、VTP の統計情報を表示する例を示します。

```
Switch# show vtp counters
VTP statistics:
Summary advertisements received      : 7
Subset advertisements received      : 5
Request advertisements received     : 0
Summary advertisements transmitted  : 997
Subset advertisements transmitted   : 13
Request advertisements transmitted  : 3
Number of config revision errors    : 0
Number of config digest errors      : 0
Number of V1 summary errors         : 0

VTP pruning statistics:

Trunk          Join Transmitted Join Received  Summary advts received from
-----          -----
Fa5/8          43071          42766          5
```

ドメイン内の VTP デバイスの表示

ドメイン内のすべての VTP デバイスの情報を表示するには、次の作業を行います。

コマンド	目的
Switch# show vtp devices [conflicts]	ドメイン内のすべての VTP デバイスで情報を収集し、表示します。 (注) 特定の機能について vtp modes off または transparent に設定されているスイッチからは情報は収集および表示されません。 conflicts キーワード (オプション) では、設定が矛盾するプライマリ サーバがあるデバイスの情報が表示されます。

次に、ドメイン内で VTP デバイスの情報を表示する例を示します。

```
Switch# show vtp devices
Retrieving information from the VTP domain, please wait for 5 seconds.
VTP Feature Conf Revision Primary Server Device ID Device Description
-----
VLAN No 18 0016.9c6d.5300 0012.011a.0d00 R2
VLAN No 18 0016.9c6d.5300 0012.4371.9ec0 R1
MST Yes 4 0012.4371.9ec0=0012.4371.9ec0 R1

Switch#
```

VLAN メンバーシップ ポリシー サーバ

ここでは、VLAN Membership Policy Server (VMPS) を使用してダイナミック ポート VLAN メンバーシップを設定する方法について説明します。次のサブセクションで構成されます。

- 「VMPS について」 (P.16-22)
- 「VMPS クライアントの概要」 (P.16-25)
- 「ダイナミック ポート VLAN メンバーシップの設定例」 (P.16-31)
- 「VMPS データベース コンフィギュレーション ファイルの例」 (P.16-34)

VMPS について

ここでは、VMPS サーバの機能と動作を説明します。

- 「VMPS サーバの概要」 (P.16-22)
- 「VMPS サーバのセキュリティ モード」 (P.16-23)
- 「代替 VLAN」 (P.16-24)
- 「不正な VMPS クライアント要求」 (P.16-24)

VMPS サーバの概要

VLAN メンバーシップ ポリシー サーバ (VMPS) は、ポートに接続されたデバイスの MAC アドレスに基づいて、ポート用の VLAN を動的に選択する中央集中型サーバを提供します。ネットワーク内にあるスイッチの 1 つのポートからネットワーク内にある別のスイッチのポートにホストを移動する場合、そのスイッチはそのホストに適切な VLAN に新しいポートを動的に割り当てます。

Cisco IOS ソフトウェアを実行する Catalyst 4500 シリーズ スイッチは、VMPS 機能をサポートしません。このスイッチは VLAN Query Protocol (VQP) クライアントとしてだけ機能し、VQP を介して VMPS と通信します。VMPS 機能については、Catalyst オペレーティング システム ソフトウェアを実行する Catalyst 4500 シリーズ スイッチ (または Catalyst 6500 シリーズ スイッチ) を使用する必要があります。

VMPS はユーザ データグラム プロトコル (UDP) ポートを使用して、クライアントから VQP 要求を待ち受けます。したがって、VMPS がネットワーク上のローカルまたはリモート デバイスに存在するかどうかを VMPS クライアントが知る必要はありません。VMPS サーバは VMPS クライアントから有効な要求を受信すると、データベースで MAC アドレス/VLAN マッピングのエントリを検索します。

要求に対する応答では、VMPS は次のいずれかのアクションを実行します。

- 割り当てられた VLAN がポート グループに限定されている場合、VMPS はこのグループに対する要求ポートを確認し、次のように応答します。
 - VLAN がポートで許可されている場合、VMPS は VLAN 名を応答としてクライアントに送信します。
 - VLAN がポートで許可されておらず、VMPS がセキュア モードでない場合、VMPS は「*access-denied*」応答を送信します。
 - VLAN がポートで許可されておらず、VMPS がセキュア モードの場合、VMPS は「*port-shutdown*」応答を送信します。
- データベース内の VLAN が現在のポートの VLAN と一致せず、またポート上にアクティブ ホストがある場合、VMPS は VMPS のセキュア モード設定に応じて、「*access-denied*」(*open*)、「*fallback VLAN name*」(代替 VLAN 設定で *open*)、「*port-shutdown*」(*secure*)、または「*new VLAN name*」(*multiple*) 応答を送信します。

スイッチは「*access-denied*」応答を VMPS から受信すると、MAC アドレスとポート間のトラフィックをブロックし続けます。スイッチはポート向けの packets をモニタし続け、新しいアドレスを識別すると VMPS にクエリーを送信します。スイッチが VMPS から「*port-shutdown*」応答を受信すると、スイッチはポートをディセーブルにします。CLI、Cisco Visual Switch Manager (CVSM)、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。

また、セキュリティ上の理由から、コンフィギュレーション テーブル内の明示的なエントリを使用して、特定の MAC アドレスへのアクセスを拒否することもできます。VLAN 名に **none** キーワードを入力すると、VMPS は「*access-denied*」または「*port-shutdown*」応答を送信します。

VMPS サーバのセキュリティ モード

VMPS は次の 3 つのモードで動作します。VMPS サーバが不正な要求に応答する方法は、VMPS が設定されているモードによって異なります。

- 「[open モード](#)」(P.16-23)
- 「[Secure モード](#)」(P.16-24)
- 「[multiple モード](#)」(P.16-24)

open モード

このポートに VLAN が割り当てられていない場合、VMPS がこのポートに対する MAC アドレスの要求を確認します。

- この MAC アドレスに関連付けられた VLAN がポートで許可されている場合、VLAN 名はクライアントに返されます。
- この MAC アドレスに関連付けられた VLAN がポートで許可されていない場合、ホストは「*access denied*」応答を受信します。

このポートに VLAN が割り当てられている場合、VMPS がこのポートに対する MAC アドレスの要求を確認します。

- この MAC アドレスに関連付けられたデータベース内の VLAN が現在のポートの VLAN と一致せず、代替 VLAN 名が設定されている場合、VMPS は代替 VLAN 名をクライアントに送信します。
- この MAC アドレスに関連付けられたデータベース内の VLAN が現在のポートの VLAN と一致せず、代替 VLAN 名が設定されていない場合、ホストは「*access denied*」応答を受信します。

Secure モード

このポートに VLAN が割り当てられていない場合、VMPS がこのポートに対する MAC アドレスの要求を確認します。

- この MAC アドレスに関連付けられた VLAN がポートで許可されている場合、VLAN 名はクライアントに返されます。
- この MAC アドレスに関連付けられた VLAN がポートで許可されていない場合、ポートはシャットダウンされます。

このポートに VLAN が割り当てられている場合、VMPS がこのポートに対する MAC アドレスの要求を確認します。

- この MAC アドレスに関連付けられたデータベース内の VLAN が現在のポートの VLAN と一致しない場合、代替 VLAN 名が設定されていてもポートはシャットダウンされます。

multiple モード

複数のホスト (MAC アドレス) がすべて同じ VLAN にある場合、これらをダイナミック ポートでアクティブにできます。ダイナミック ポートでリンクがダウンすると、ポートは割り当てられていない状態に戻ります。ポートを通じてオンラインになるホストは、ポートが VLAN に割り当てられる前に、VMPS ですべて再チェックされます。

ダイナミック ポートに接続された複数のホストが別の VLAN に属する場合、VMPS サーバに multiple モードが設定されていれば、最新の要求での MAC アドレスと一致する VLAN がクライアントに返されます。



(注)

Catalyst オペレーティング システム ソフトウェアを実行する Catalyst 4500 シリーズおよび Catalyst 6500 シリーズ スイッチは、この 3 つの操作モードすべてで VMPS をサポートします。ただし、User Registration Tool (URT) は open モードだけをサポートします。

代替 VLAN

代替 VLAN 名を VMPS サーバで設定できます。

このポートに VLAN が割り当てられていない場合、VMPS がこのポートに対する MAC アドレスの要求を比較します。

- データベースにない MAC アドレスを持つデバイスを接続する場合、VMPS は代替 VLAN 名をクライアントに送信します。
- 代替 VLAN 名が設定されておらず、MAC アドレスがデータベースにない場合、VMPS は「*access-denied*」応答を送信します。

このポートに VLAN が割り当てられている場合、VMPS がこのポートに対する MAC アドレスの要求を比較します。

- VMPS が secure モードの場合、代替 VLAN がサーバに設定されているかどうかに関係なく、VMPS は「*port-shutdown*」応答を送信します。

不正な VMPS クライアント要求

次に、不正な VMPS クライアント要求の例を 2 つ示します。

- MAC アドレス マッピングが VMPS データベースに存在せず、「no fall back」VLAN が VMPS に設定されている場合。

- ポートがすでに VLAN に割り当てられ (VMPS モードは「multiple」でない)、2 番目の VMPS クライアント要求が異なる MAC アドレスの VMPS で受信された場合。

VMPS クライアントの概要

ここでは、VMPS クライアントとしてスイッチを設定する方法、およびそのスイッチのポートをダイナミック VLAN メンバーシップに設定する方法について説明します。

次のトピックについて説明します。

- 「ダイナミック VLAN メンバーシップの概要」 (P.16-25)
- 「デフォルトの VMPS クライアント設定」 (P.16-25)
- 「VMPS クライアントとしてのスイッチの設定」 (P.16-26)
- 「VMPS の管理およびモニタリング」 (P.16-29)
- 「ダイナミック ポート VLAN メンバーシップのトラブルシューティング」 (P.16-30)

ダイナミック VLAN メンバーシップの概要

ポートが「dynamic」として設定されている場合、ポート上の MAC アドレスに基づき VLAN 情報を受信します。VLAN が静的にポートに割り当てられていない場合、ポート上の MAC アドレスに基づき VMPS から動的に取得されます。

ダイナミック ポートは、1 つの VLAN だけに属することができます。リンクがアクティブになる際、ポートが VLAN に割り当てられるまでスイッチはこのポートへトラフィックを転送しません。ダイナミック ポート上にある新規ホストの最初の packets における送信元 MAC アドレスは、VQP 要求の一部として VMPS に送信され、VMPS データベース内で MAC アドレスと VLAN の照合が行われます。一致した場合、VMPS はそのポートの VLAN 番号を送信します。一致しない場合、(VMPS セキュリティ モード設定に応じて) VMPS は要求を拒否するか、またはポートをシャットダウンします。想定される VMPS 応答の詳細については「VMPS について」 (P.16-22) を参照してください。

複数のホスト (MAC アドレス) がすべて同じ VLAN にある場合、これらをダイナミック ポートでアクティブにできます。ダイナミック ポートでリンクがダウンすると、ポートは割り当てられていない状態に戻り、VLAN に属さなくなります。ポートを通じてオンラインになるホストは、ポートが VLAN に割り当てられる前に、VMPS ですべて再チェックされます。

この操作を行うには、クライアントデバイスが VMPS に到達可能である必要があります。VMPS クライアントは UDP パケットとして VQP 要求を送信し、中止する前に複数回試行します。再試行の間隔については、「再試行間隔の設定」 (P.29) を参照してください。

また、VMPS クライアントは定期的に VLAN メンバーシップを再確認します。再確認の回数については、「VMPS の管理およびモニタリング」 (P.29) を参照してください。

最大 50 台のホストは常に特定のポートでサポートされます。最大数を超えると、VMPS サーバの動作モードに関係なくポートをシャットダウンします。



(注) ポートで 50 を超えるホストがアクティブになると、VMPS はダイナミック ポートをシャットダウンします。

デフォルトの VMPS クライアント設定

表 16-4 に、クライアントスイッチのデフォルトの VMPS およびダイナミック ポート設定を示します。

表 16-4 デフォルトの VMPS クライアントおよびダイナミック ポート設定

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 ポート	未設定

VMPS クライアントとしてのスイッチの設定

ここでは、次の項目について説明します。

- 「VMPS サーバの IP アドレスの設定」 (P.16-26)
- 「VMPS クライアントでのダイナミック アクセス ポートの設定」 (P.16-27)
- 「VLAN メンバーシップの再確認」 (P.16-28)
- 「再確認間隔の設定」 (P.16-28)
- 「VLAN メンバーシップの再確認」 (P.16-28)

VMPS サーバの IP アドレスの設定

Catalyst 4500 シリーズ スイッチを VMPS クライアントとして設定するには、VMPS として機能するスイッチの IP アドレスおよびホスト名を入力する必要があります。

Catalyst 4500 シリーズ スイッチ上でプライマリおよびセカンダリ VMPS を定義するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# vmps server {ipaddress hostname} primary	プライマリ VMPS サーバとして機能するスイッチの IP アドレス、またはホスト名を指定します。
ステップ 3	Switch(config)# vmps server {ipaddress hostname}	セカンダリ VMPS サーバとして機能するスイッチの IP アドレス、またはホスト名を指定します。
ステップ 4	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 5	Switch# show vmps	VMPS サーバ エントリを確認します。

次に、プライマリおよびセカンダリ VMPS デバイスを定義する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vmps server 172.20.128.179 primary
Switch(config)# vmps server 172.20.128.178
Switch(config)# end
```



(注) VMPS クライアントでこの CLI を使用して、最大 4 つの VMPS サーバを設定できます。

```
Switch# show vmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.179 (primary, current)
                   172.20.128.178

Reconfirmation status
-----
VMPS Action:          No Dynamic Port
```

VMPS クライアントでのダイナミック アクセス ポートの設定

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、次の作業を行います。

	コマンド	目的
ステップ1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	Switch(config)# interface interface	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、設定するポートを指定します。
ステップ3	Switch(config-if)# switchport mode access	ポートをアクセス モードに設定します。
ステップ4	Switch(config-if)# switchport access vlan dynamic	ダイナミック VLAN アクセスの対象となるようにポートを設定します。
ステップ5	Switch(config-if)# end	特権 EXEC モードに戻ります。
ステップ6	Switch# show interface interface switchport	入力を確認します。

次に、ダイナミック アクセス ポートを設定し、入力を確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fa1/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan dynamic
Switch(config-if)# end

Switch# show interface fa1/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative mode: dynamic auto
Operational Mode: dynamic access
Administrative Trunking Encapsulation: isl
Operational Trunking Encapsulation: isl
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: NONE
Pruning VLANs Enabled: NONE
```

音声ポート

ダイナミック アクセス ポートに Voice VLAN ID (VVID; 音声 VLAN ID) が設定されている場合、ポートはアクセス VLAN および音声 VLAN 両方に属することができます。そのため、IP Phone に接続するよう設定されたアクセス ポートでは、次のために異なる VLAN を指定できます。

- IP Phone のアクセス ポート (アクセス VLAN) を介してスイッチに接続された PC へ、PC からのデータ トラフィック
- IP Phone へ、IP Phone からの音声トラフィック (音声 VLAN)

VLAN メンバーシップの再確認

スイッチが VMPS から受信したダイナミック ポート VLAN メンバーシップの割り当てを確認するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# vmmps reconfirm	ダイナミック ポート VLAN メンバーシップを再確認します。
ステップ 2	Switch# show vmmps	ダイナミック VLAN 再確認ステータスを確認します。

再確認間隔の設定

VMPS クライアントは、VMPS から受信した VLAN メンバーシップ情報を定期的に再確認します。VLAN/MAC アドレス割り当てを再確認するまで VMPS クライアントが待機する時間 (分) を設定できます。

再確認間隔を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# vmmps reconfirm minutes	ダイナミック VLAN メンバーシップの再確認間隔を分単位で指定します。
ステップ 3	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ 4	Switch# show vmmps	ダイナミック VLAN 再確認ステータスを確認します。

次に、再確認間隔を 60 分に変更し、その変更を確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vmmps reconfirm 60
Switch(config)# end
Switch# show vmmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 10
VMPS domain server: 172.20.130.50 (primary, current)

Reconfirmation status
-----
VMPS Action:          No Host
```

再試行間隔の設定

次のサーバにクエリーを実行するまで VMPS クライアントが VMPS に連絡を試行する回数を設定できます。

再試行間隔を設定するには、次の作業を行います。

	コマンド	目的
ステップ1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	Switch(config)# vmmps retry count	VQP クエリーの再試行回数を指定します。デフォルト値は 3 です。指定できる範囲は 1 ~ 10 です。
ステップ3	Switch(config)# end	特権 EXEC モードに戻ります。
ステップ4	Switch# show vmmps	再試行回数を確認します。

次に、再試行回数を 5 回に変更し、その変更を確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# vmmps retry 5
Switch(config)# end

Switch# show vmmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 5
VMPS domain server: 172.20.130.50 (primary, current)

Reconfirmation status
-----
VMPS Action:          No Host
```

VMPS の管理およびモニタリング

show vmmps コマンドを使用することにより、次の VMPS 情報を表示できます。

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 を使用して VMPS にクエリーを実行します。
再確認インターバル	VLAN から MAC アドレスへの割り当てを再確認するまでスイッチが待機する時間 (分)。
サーバ再試行回数	VQP が VMPS へ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 設定された VLAN メンバーシップ ポリシー サーバの IP アドレス。スイッチは、現在「**current**」とマークされたものにクエリーを送信します。「**primary**」とマークされたものは、プライマリ サーバです。

VMPS アクション 最新の再確認試行の結果。再確認間隔が経過した場合に自動的に再確認されるか、**vmips reconfirm** コマンドまたは **CVSM** や **SNMP** の同様のコマンドを入力することで自動的に再確認できます。

次に、VMPS 情報を表示する例を示します。

```
Switch# show vmips
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:

Reconfirmation status
-----
VMPS Action:          other

The following example shows how to display VMPS statistics:
Switch# show vmips statistics
VMPS Client Statistics
-----
VQP Queries:          0
VQP Responses:        0
VMPS Changes:         0
VQP Shutdowns:       0
VQP Denied:           0
VQP Wrong Domain:    0
VQP Wrong Version:   0
VQP Insufficient Resource: 0
```



(注) VMPS 統計情報の詳細については、『Cisco IOS Command Reference』を参照してください。

ダイナミック ポート VLAN メンバーシップのトラブルシューティング

VMPS は次の条件でダイナミック ポートを **errdisable** にします。

- 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、ホストがネットワークに接続しないようにポートを **errdisable** にします。
- 50 以上のアクティブ ホストがダイナミック ポートにある場合。

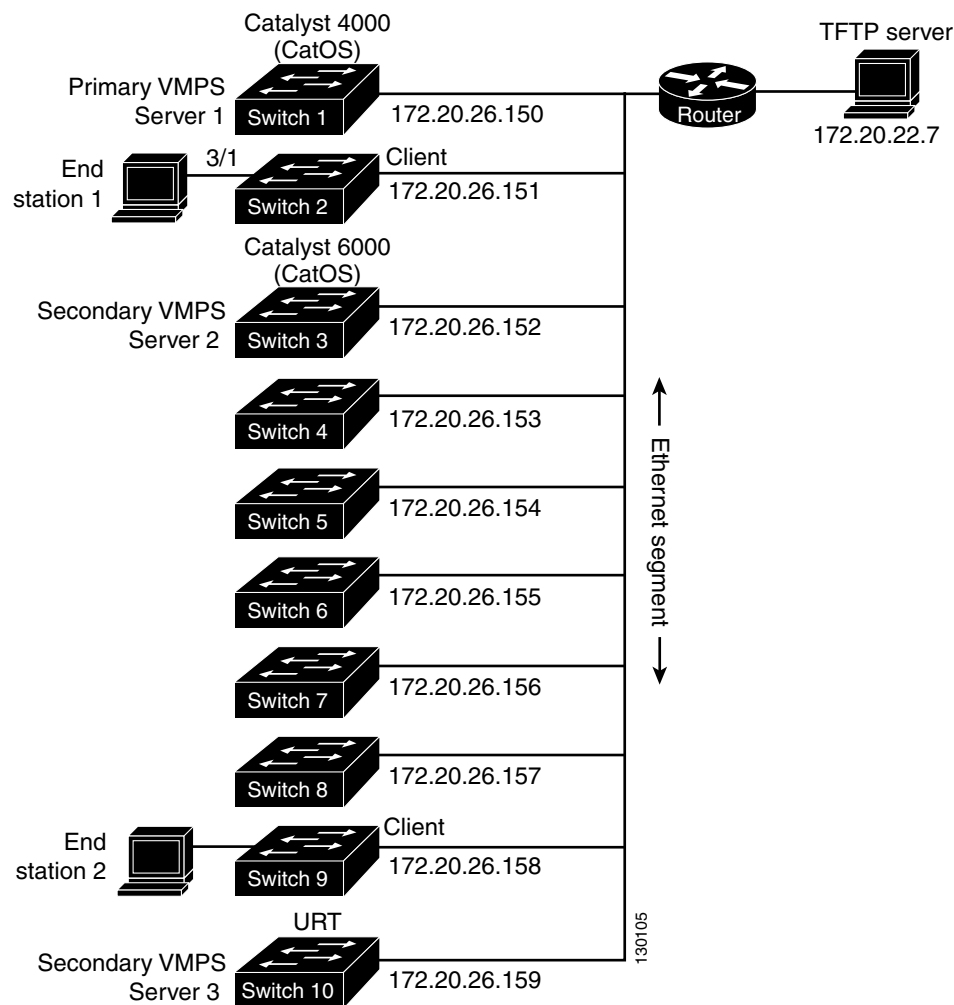
errdisable ステータスのインターフェイスのステータスを表示する方法については、第 9 章「ポートのステータスと接続の確認」を参照してください。**errdisable** ステータスになっているポートを回復するには、**errdisable recovery cause vmips** グローバル コンフィギュレーション コマンドを使用します。

ダイナミック ポート VLAN メンバーシップの設定例

図 16-4 (P.16-31) に、VMPS サーバとダイナミック ポートを持つ VMPS クライアントスイッチで構成されるネットワークを示します。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 4000 ファミリ スイッチ 1 (Catalyst オペレーティング システムを実行する) は、プライマリ VMPS サーバです。
- Catalyst 6000 ファミリ スイッチ 3 (Catalyst オペレーティング システムを実行) および URT は、セカンダリ VMPS サーバです。
- エンドステーションは、次のクライアントに接続されています。
 - Catalyst 4500 シリーズ XL スイッチ 2 (Catalyst Cisco IOS を稼働)
 - Catalyst 4500 シリーズ XL スイッチ 9 (Catalyst Cisco IOS を稼働)
- データベース コンフィギュレーション ファイルは Bldg-G.db という名前で、IP アドレスが 172.20.22.7 の TFTP サーバに保存されています。

図 16-4 ダイナミック ポート VLAN メンバーシップの構成例



可能なトポロジは、2 種類あります。図 16-5 に、1 つのエンドステーションに VMPS クライアントとして稼働する Catalyst 4500 シリーズスイッチが直接接続されたトポロジを示します。図 16-6 に、1 つのエンドステーションに Catalyst 4500 シリーズスイッチと接続する Cisco IP Phone が接続されたトポロジを示します。

図 16-5 1 つのエンドステーションに VMPS クライアントとして動作する Catalyst 4500 シリーズスイッチが直接接続されたトポロジ

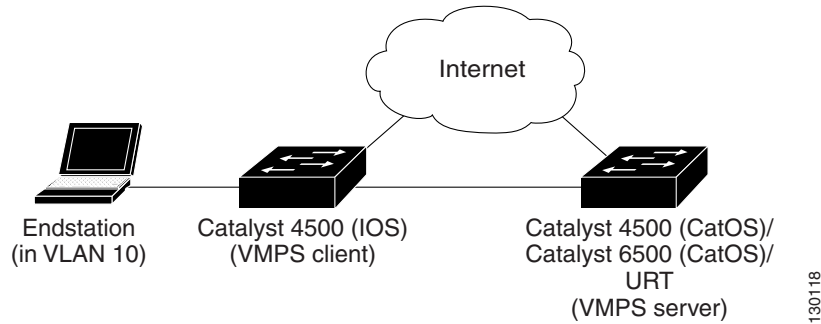
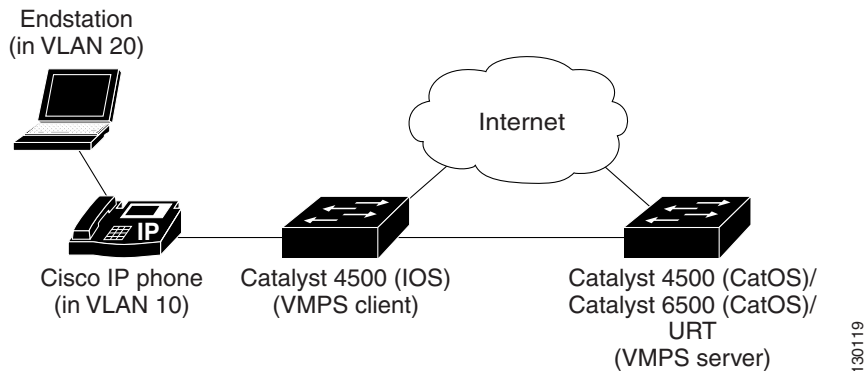


図 16-6 1 つのエンドステーションに Catalyst 4500 シリーズスイッチと接続する Cisco IP Phone が接続されたトポロジ



次の手順では、Catalyst 4500 および Catalyst 6500 シリーズスイッチ（Catalyst オペレーティングシステムを稼働）が VMPS サーバとなります。ネットワーク内の Catalyst 4500 シリーズスイッチのクライアントを設定するには、この手順を実行します。

ステップ 1 クライアントスイッチであるスイッチ 2 の VMPS サーバアドレスを設定します。

- a. 特権 EXEC モードから、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。

```
switch# configuration terminal
```

- b. プライマリ VMPS サーバの IP アドレスを入力します。

```
switch(config)# vmps server 172.20.26.150 primary
```

- c. セカンダリ VMPS サーバの IP アドレスを入力します。

```
switch(config)# vmps server 172.20.26.152
```

- d. VMPS IP アドレスの設定を確認するには、特権 EXEC モードに戻ります。


```
switch(config)# exit
```

- e. スイッチに設定された VMPS 情報を表示します。

```
switch# show vmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.26.152
                    172.20.26.150 (primary, current)
```

- ステップ 2** スイッチ 2 のポート Fa0/1 をダイナミック ポートとして設定します。

- a. グローバル コンフィギュレーション モードに戻ります。

```
switch# configure terminal
```

- b. インターフェイス コンフィギュレーション モードを開始します。

```
switch(config)# interface fa2/1
```

- c. スタティック アクセス ポートの VLAN メンバーシップ モードを設定します。

```
switch(config-if)# switchport mode access
```

- d. ポートのダイナミック VLAN メンバーシップを割り当てます。

```
switch(config-if)# switchport access vlan dynamic
```

- e. 特権 EXEC モードに戻ります。

```
switch(config-if)# exit
switch#
```

- ステップ 3** ポート Fa2/1 のエンド ステーション 2 を接続します。エンド ステーション 2 がパケットを送信すると、スイッチ 2 がプライマリ VMPS サーバであるスイッチ 1 にクエリーを送ります。スイッチ 1 は、ポート Fa2/1 の VLAN ID で応答します。スパニングツリー PortFast モードが Fa2/1 上でイネーブルの場合、ポート Fa2/1 はただちに接続されて転送を開始します。

- ステップ 4** VMPS 再確認間隔を 60 分に設定します。再確認間隔とは、VLAN/MAC アドレス割り当てを再確認するまでスイッチが待機する時間 (分) です。

```
switch# config terminal
switch(config)# vmps reconfirm 60
```

- ステップ 5** 特権 EXEC モードでエントリを確認します。

```
switch# show vmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:

Reconfirmation status
-----
VMPS Action:          No Dynamic Port
```

- ステップ 6** ステップ 1 およびステップ 2 を繰り返して、VMPS サーバアドレスを設定し、各 VMPS クライアントスイッチのダイナミック ポートを割り当てます。

VMPS データベース コンフィギュレーション ファイルの例

次に、VMPS サーバに表示される VMPS データベース コンフィギュレーション ファイルの例を示します。VMPS データベース コンフィギュレーション ファイルは ASCII テキスト ファイルで、VMPS サーバとして機能するスイッチにアクセス可能な TFTP サーバに保存されます。

```
!vmps domain <domain-name>
! The VMPS domain must be defined.
!vmps mode {open | secure}
! The default mode is open.
!vmps fallback <vlan-name>
!vmps no-domain-req {allow | deny}
!
! The default value is allow.
vmps domain WBU
vmps mode open
vmps fallback default
vmps no-domain-req deny
!
!
!MAC Addresses
!
vmps-mac-addr
!
! address <addr> vlan-name <vlan_name>
!
address 0012.2233.4455 vlan-name hardware
address 0000.6509.a080 vlan-name hardware
address aabb.ccdd.eeff vlan-name Green
address 1223.5678.9abc vlan-name ExecStaff
address fedc.ba98.7654 vlan-name --NONE--
address fedc.ba23.1245 vlan-name Purple
!
!Port Groups
!
!vmps-port-group <group-name>
! device <device-id> {port <port-name> | all-ports}
!
vmps-port-group WiringCloset1
  device 198.92.30.32 port Fa1/3
  device 172.20.26.141 port Fa1/4
vmps-port-group "Executive Row"
  device 198.4.254.222 port es5%Fa0/1
  device 198.4.254.222 port es5%Fa0/2
  device 198.4.254.223 all-ports
!
!VLAN groups
!
!vmps-vlan-group <group-name>
! vlan-name <vlan-name>
!
vmps-vlan-group Engineering
vlan-name hardware
vlan-name software
!
!VLAN port Policies
!
```

```
!vmports-policies {vlan-name <vlan_name> | vlan-group <group-name>}
! {port-group <group-name> | device <device-id> port <port-name>}
!
vmports-policies vlan-group Engineering
  port-group WiringCloset1
vmports-policies vlan-name Green
  device 198.92.30.32 port Fa0/9
vmports-policies vlan-name Purple
  device 198.4.254.22 port Fa0/10
  port-group "Executive Row"
```

