VLAN管理

この章は、次の項で構成されています。

VLAN 設定

VLANを作成すると、スイッチ上に個別のブロードキャストドメインを作成できます。ブロードキャストドメインは、ルータなどのレイヤ3デバイスを介して、互いに通信できます。VLANは主に、物理的な場所に関係なく、ホスト間のグループを形成するために使用されます。VLANはホスト間でグループを形成することでセキュリティを向上させます。VLANを作成しても、その VLAN が少なくとも 1 つのポートに手動で、または動的に接続されるまでは何の効果もありません。VLAN を確立する最も一般的な理由の 1 つは、音声用とデータ用に別の VLAN を作成するためです。これにより、両方のタイプのパケットが送信されます。

VLAN の作成または構成

スイッチで VLAN を作成または構成するには、次の手順を実行します。

手順

ステップ1 [VLAN Management] > [VLAN Settings] をクリックします。

ステップ2 [Add] をクリックして、1 つ以上の新しい VLAN を追加します。

ステップ3 単一の VLAN を作成するには、[VLAN] オプション ボタンを選択して [VLAN ID] を入力し、必要に応じて [VLAN Name] を入力します。

ステップ4 新しい VLAN に次のフィールドを追加します。

- [VLAN Interface State]：VLAN を有効にする場合にオンにします。
- [Link Status SNMP Traps]：SNMP トラップのリンクステータス生成を有効にする場合にオンにします。

（注）
VLAN テーブルには、VLAN の作成方法を示す [Originators] という用語が表示されます。

ステップ5 VLAN の範囲を追加するには、[Range] チェックボックスをオンにし、[VLAN range] フィールドに VLAN 範囲（2 ～ 4094）を入力します。

ステップ6 [Apply] をクリックして、VLAN を作成します。

レイヤ3スイッチング

レイヤ 3 スイッチは、スイッチとルータの機能を組み合わせたものです。IP ルーティング インテリジェンスが組み込まれていて、ルータとして機能するほか、同じサブネットまたは仮想 LAN 上にあるデバイスをすばやくリンクするためのスイッチとして機能します。着信パケットを検査し、送信元アドレスと宛先アドレスに応じてルーティングを決定し、ルーティングプロトコルを処理できます。レイヤ3スイッチは、次のようにスイッチとルータの両方として機能します。

デバイスをレイヤ 3 スイッチとしてセットアップするには、次の手順に従います。

手順

ステップ1 [VLAN Management] > [VLAN Settings] をクリックします。

ステップ2 [Add] をクリックします。

ステップ3 VLAN ID と VLAN 名を入力します。

ステップ4 [Apply] をクリックして、VLAN を作成します。

ステップ5 次に、[IPv4 Configuration] > [IPv4 Interface] に移動します。

ステップ6 [Enable] をオンにして、IPv4 ルーティングを有効にします。これにより、すべてのレイヤ 3 インターフェイス間のルーティングが可能になり、あるVLANからのトラフィックを別のVLANに転送できるようになります。

ステップ 7 [Apply] をクリックして、すべてのレイヤ 3 インターフェイス間のルーティングを有効にします。これにより、ある VLAN からのトラフィックを別の VLAN に転送できるようになります。

インターフェイスの設定

VLANが構成されている物理ネットワークポートまたはボンドに接続されている仮想インターフェイスは、VLANインターフェイスと呼ばれます。VLANインターフェイスは、ルーティングされるトラフィックに正しい VLAN ID を自動的に割り当てるために使用されます。

VLAN 関連のパラメータは、[VLAN Interface Settings] ページに表示され、設定が可能になります。VLAN 設定を行うには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [Interface Settings] をクリックします。

ステップ 2 インターフェイス タイプ（ポートまたは LAG）を選択し、[Go] をクリックします。ポートまたは LAG とその VLAN パラメータが表示されます。

ステップ 3 ポートまたは LAG を設定するには、それらを選択して [Edit] をクリックします。

ステップ 4 次のフィールドに値を入力します。

Interface	[Port/LAG] を選択し、ポートを選択または入力します。
Switchport Mode	レイヤ 2 またはレイヤ 3 を選択します。

Interface VLAN Mode	VLANのインターフェイスモードを選択します。次のオプションがあります。 • [Access]：インターフェイスは、1 つの VAN のタグなしメンバになります。このモードで設定されているポートは、アクセス ポートと呼ばれます。 • [Trunk]：インターフェイスは、最大 1 つの VLAN のタグなしメンバと、0 以 上の VLAN のタグ付きメンバになります。このモードで設定されているポートは、トランク ポートと呼ばれます。 • [General]：インターフェイスは、IEEE 802.1q 規格で定義されているすべての機能 をサポートします。インターフェイスは、1 つまたは複数の VLAN のタグ付きまたはタグなしメンバーになれます。 （注） GVRP 対応ポートを使用する場合は、インターフェイス VLAN モードが [全般（General）] に設定されていることを確認します。 • [Customer]：このオプションを選択すると、インターフェイスが Q-in-Q モー ドになります。これにより、プロバイダー ネットワーク全体で独自の VLAN 配置（PVID）が使用できます。デバイスは、1 つ以上の顧客ポートがある場合には Q-in-Q モードです。 • [Private VLAN—Host]：インターフェイスを隔離またはコミュニティとして設定する場合に選択します。この後、[Secondary VLAN - Host] フィールドで、隔離 VLAN またはコミュニティ VLAN のいずれかを選択します。 • [Private VLAN—Promiscuous]：インターフェイスを混合として設定する場合に選択します。 • [VLAN Mapping—Tunnel]：インターフェイスを VLAN トンネルエッジポートとして設定する場合に選択します。 • [VLAN Mapping—One to One]：インターフェイスを VLAN マッピング ワンツーワン エッジ ポートとして使用するように設定する場合に選択します。
Frame Type	（一般モードでのみ使用可能）インターフェイスで受信可能なフレームのタイプを選択します。設定されたフレームタイプではないフレームは、入力時に廃棄されます。値は次のとおりです。 • [Admit All]：インターフェイスは、タグなしフレーム、タグ付きフレーム、優先順位タグ付きフレームのすべての種類のフレームを受信します。 • [Admit Tagged Only]：インターフェイスはタグ付きフレームのみを受け入れます。 • [Admit Untagged Only]：インターフェイスはタグなしおよびプライオリティタグ付 きフレームのみ受け入れます。

Ingress Filtering	入力フィルタリングを有効にする場合に選択します。入力フィルタリングが有効になると、インターフェイスは、そのインターフェイスがメンバーになっていない VLAN に分類されるすべての着信フレームを破棄します。入力のフィルタリングは全般ポートで無効または有効にできます。アクセスポートとトランクポートでは常に有効になっています。

ステップ 5 [Apply] をクリックします。

VLANへのポート

[Port to VLAN] セクションには、ポートの VLAN メンバーシップがさまざまな方法で表示されます。これらを使用して、VLANにメンバーを含めたり、VLANからメンバーを除外したりできます。デフォルトの VLAN メンバーシップが禁止されている場合、ポートに対して他の VLAN メンバーシップは許可されません。そのポートに内部 VID として 4095 が割り当てられます。

エンドノード間のパスでパケットを転送するには、VLAN対応デバイスを手動で設定するか、VLAN とそのポートメンバーシップを Generic VLAN Registration Protocol（GVRP）から動的に学習する必要があります。

2 つの VLAN 対応デバイス間に仲介する VLAN 対応デバイスがない場合、それらのタグなしポートメンバーシップは、同じ VLAN に属している必要があります。2 つのデバイス間にあるポートが、そのポートと VLAN 間でタグなしパケットの送受信を行う場合、それらのポートの PVID が一致する必要があります。これがないと、トラフィックが 1 つの VLAN から別の VLAN にリークする可能性があります。

VLAN 対応や VLAN 非対応のその他のネットワークデバイスは、VLAN タグ付きフレームを通過させることができます。宛先エンドノードが VLAN 未対応なのに、VLAN からのトラフィックを受信する必要がある場合、最後の VLAN 対応デバイスが、宛先 VLAN のタグなしフレームをエンドノードに転送する必要があります。

特定の VLAN 内のポートを表示および構成するには、[Port to VLAN] ページを使用して、以下の手順に従います。

手順

ステップ 1 [VLAN Management] > [Port to VLAN] をクリックします。

ステップ 2 VLAN とインターフェイスの種類（ポートまたはLAG）を選択し、[Go] をクリックして、VLAN に関するポートの特性を表示または変更します。

各ポートまたは LAG のポートモードは、インターフェイスの設定 （3 ページ）で設定されている現在のポートモードとともに表示されます。

各ポートまたは LAG には、VLAN への現在の登録が表示されます。

次のフィールドが表示されます。

- [VLAN Mode]：VLAN のポートの種類が表示されます。
- [Membership Type]：次のいずれかのオプションを選択できます。
  - [Forbidden]：このインターフェイスは、GVRP 登録からであってもVLANに参加できません。ポートが他の VLAN のメンバーではない場合、ポートでこのオプションを有効にすると、内部 VLAN 4095 のポート部分（予約済み VID）になります。
  - [Excluded]：インターフェイスは現在 VLAN のメンバーではありません。VLAN の新規作成時には、すべてのポートおよびLAG でこれがデフォルトで設定されます。
  - [Tagged]：インターフェイスは、VLAN のタグ付きメンバーになります。
  - [Untagged]：インターフェイスは、VLANのタグなしメンバーになります。VLANのフレームはタグなしでインターフェイス VLAN に送信されます。
  - [Multicast TV VLAN]：マルチキャスト IP を使用してデジタル TV に使用されるインターフェイス。ポートは、マルチキャスト TV VLAN の VLAN タグを使用して VLAN に参加します。
- [PVID]：インターフェイスの PVID を VLAN の VID に設定します。PVID はポート単位の設定です。

ステップ 3 [Apply]をクリックします。インターフェイスはVLANに割り当てられ、同時に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。

別の VLAN ID を選択すれば、続けて別の VLAN のポート メンバーシップを表示または設定できます。

ポートVLANメンバシップ

アクセスレイヤスイッチで VLAN が使用可能になった場合、エンドユーザーはそれに参加できる必要があります。その結果、[Port VLAN Membership] ページには、デバイスのすべてのポートとともに、各ポートが所属する VLAN が表示されます。

[VLAN to Port] ページでは、ポートは大文字の P で示されます。ポートを 1 つ以上の VLAN に割り当てるには、次の手順に従います。

手順

ステップ 1 [VLAN Management] > [Port VLAN Membership] をクリックします。

ステップ 2 インターフェイスの種類（ポートまたはLAG）を選択し、[Go]をクリックします。選択した種類のすべてのインターフェイスに対して、次のフィールドが表示されます。

- [Interface]：ポート /LAG ID。
- [Mode]：インターフェイスの設定 （3 ページ）で選択されたインターフェイス VLAN モード。

- [Administrative VLANs]：インターフェイスがメンバになる可能性のあるすべてのVLANが表示されるドロップダウン リスト。
- [Operational VLANs]：インターフェイスが現在メンバになっているすべての VLAN が表示 されるドロップダウン リスト。
- [LAG]：選択したインターフェイスが [Port] の場合、このインターフェイスがメンバーになっている LAG が表示されます。

ステップ 3 ポートを選択し、[Join VLAN] ボタンをクリックします。

ステップ 4 次のフィールドに値を入力します。

- [Interface]：ポートまたは LAG を選択します。
- [Current VLAN Mode]：インターフェイスの設定 （3 ページ）で選択したポート VLAN モードが表示されます。
- **[Access Mode Membership (Active)]**
  - [Access VLAN ID]：ドロップダウンリストから、VLAN を選択します。
- **[Trunk Mode Membership]**
  - [Native VLAN ID]：ポートがトランクモードになっている場合は、この VLAN のメンバーになります。
  - [Tagged VLANs]：ポートがトランクモードになっている場合は、これらの VLAN のメンバーになります。次のオプションがあります。

    [All VLANs]：ポートがトランクモードになっている場合は、すべてのVLANのメンバーになります。

    [User Defined]：ポートがトランクモードになっている場合は、ここに入力された VLAN のメンバーになります。
- [General Mode Membership]
  - [Untagged VLANs]：ポートが一般モードになっている場合は、この VLAN のタグなしメンバーになります。
  - [Tagged VLANs]：ポートが一般モードになっている場合は、これらの VLAN のタグ付きメンバーになります。
  - [Forbidden VLANs]：ポートが一般モードになっている場合は、インターフェイスが GVRP 登録からであってもVLANに参加できません。ポートが他のVLANのメンバーではない場合、ポートでこのオプションを有効にすると、内部 VLAN 4095 のポート部分（予約済み VID）になります。
  - [General PVID]：ポートが一般モードになっている場合は、これらの VLAN のメンバーになります。
- **[Customer Mode Membership]**

- [Customer VLAN ID]：ポートがカスタマーモードになっている場合は、この VLAN のメンバーになります。

ステップ 5 [Apply] をクリックします。

ステップ 6 ポートを選択して、[Details] をクリックすると、次のフィールドが表示されます。

- [Interface]：ポートまたは LAG を選択します。
- [Administrative VLANs]：ポートはこれらの VLAN に対して設定されています。
- [Operational VLANs]：ポートは現在これらの VLAN のメンバーです。

VLAN 変換

VLAN 変換では、入力タグを別のタグに置き換えたり、その逆の pn 出力を行ったりします。これは、一連の VLAN 変換ルールを構成するためにインターフェイスで使用されます。これらのルールが適用されると、そのインターフェイスの着信および発信パケットのVLAN-IDは、変換ルールからの適切な VLAN-ID にマッピングされます。この構成は、フレームの VLAN 識別子をインターフェイスで変更する必要がある場合に役立ちます。

ワンツーワンの VLAN トンネリング

VLAN トンネリングは、QinQ/Nested VLAN/カスタマーモード VLAN 機能を拡張する機能です。この機能は、サービスプロバイダーが単一の VLAN を使用して複数の VLAN を所有しているお客様をサポートできるようにします。カスタマー VLAN ID を保護しながら、複数のカスタマー VLAN でトラフィックを分離します。サービスプロバイダー エッジ スイッチのトンネル ポートに着信するパケット（適切な VLAN ID ですでに 802.1Q タグ付けされている）は、カスタマーに一意である VLAN ID を含む 802.1Q タグの別のレイヤでカプセル化されます。元々のカスタマーの802.1Qタグは、カプセル化されたパケットの中に維持されます。したがって、サービスプロバイダーインフラストラクチャに着信するパケットは二重にタグ付けされます。

この機能は、スイッチがネットワーク経由でトラフィックを転送するために、通常の 802.1Q タグ（カスタマー VLAN/C-VLAN）に加えてサービスタグ（S-VLAN）と呼ばれる第 2 の ID タグが追加されるため、「ダブルタギング」またはQinQと呼ばれます。カスタマーネットワークがプロバイダーエッジスイッチに接続されるインターフェイスであるエッジインターフェイスでは、C-VLAN が S-VLAN にマッピングされ、オリジナルの C-VLAN タグがペイロードの一部として維持されます。タグなしフレームは除去されます。

フレームの最初の C-VLAN-ID は、非エッジのタグ付きインターフェイスを介して配信されるときに、S-VLAN タグの別のレイヤにマッピングされます。その結果、非エッジのインターフェイスを持つフレームでブロードキャストされるパケットには、外部 S-VLAN タグと内部 C-VLAN タグの 2 つのタグが付けられます。トラフィックがネットワーク サービス プロバイダーのインフラストラクチャ経由で転送されている間は、サービス VLAN タグがそのまま保

持されます。フレームが出力デバイスのエッジインターフェイスから送信されるときにS-VLANタグが除去されます。タグのないフレームはドロップされます。

VLAN トンネリング機能では、基本的な QinQ/Nested VLAN 実装に加えて、個別のコマンドセットを使用して次の機能が提供されます。

- エッジ インターフェイスごとに、S-VLAN を分離するためのさまざまな C-VLAN のマッピングを複数提供
- エッジ インターフェイスで受信された特定の C-VLAN に対してドロップ アクションの設定が可能
- S-VLANに明確にマッピングされていないC-VLANに対してアクションの設定が可能（ドロップまたは特定の S-VLAN へのマッピング）
- グローバルまたは NNI インターフェイス（ネットワーク ノード インターフェイス - バックボーン ポート）ごとに、S-VLAN タグの EtherType が設定可能以前の QinQ の実装では、S-VLAN タグには EtherType 0x8100 のみがサポートされていました。

インターフェイスでデバイスを S-VLAN として設定するまえに、ユーザ指定の S-VLAN を作成しておく必要があります。この VLAN が存在しない場合、コマンドは失敗します。

IPv4/IPv6 転送と、VLAN トンネリングは同時には使用できません。つまり、IPv4 転送または IPv6 転送のいずれかが有効になっている場合、インターフェイスを VLAN トンネリング モードに設定することはできません。また、任意のインターフェイスを VLAN トンネリング モードに設定すると、そのデバイスで IPv4 転送および IPv6 転送を有効にすることはできません。

次の機能も、VLAN トンネリング機能と同時には使用できません。

- 自動音声 VLAN
- Auto Smartport
- 音声 VLAN

エッジインターフェイスを含む VLAN では、IPv4 と IPv6 のインターフェイスを定義することができません。

VLAN 変換

エッジ インターフェイスを含む VLAN では、次のレイヤ 2 の機能はサポートされません。

- IGMP/MLD スヌーピング
- DHCP スヌーピング
- IPv6 ファースト ホップ セキュリティ

エッジ インターフェイス（UNI - ユーザ ネットワーク インターフェイス）では、次のプロトコルを有効にすることができません。

- STP
- GVRP

エッジ インターフェイス（UNI - ユーザ ネットワーク インターフェイス）では、次の機能はサポートされません。

- RADIUS VLAN 割り当て
- 802.1x VLAN
- SPAN/RSPAN：ネットワーク キーワードを使用する宛先ポート、またはネットワーク キーワードまたはリフレクタ ポートを使用するリフレクタ ポート宛先ポートとして。

インターフェイスで VLAN トンネリングを適用するには、ルータの TCAM ルールを使用する必要があります。ルータに十分な TCAM 用リソースがない場合、コマンドは失敗します。ユーザーは、[Administration] > [Routing Resources] 経由で、VLAN トンネリング（およびマッピング）用のルータ TCAM リソース割り当てを追加および削除できます（システムの再起動が必要）。

元の QinQ 実装（顧客モードに関連するコマンド）もまた、新しい VLAN トンネリング実装で維持されています。顧客ポート モードは、VLAN マッピング トンネル ポート モードにおいては特殊なケースであり、TCAM リソースの割り当てを必要としません。

レイヤ 2 制御プロトコル（L2CP）の BPDU トンネリング

デフォルトでは、下記 MAC アドレス宛ての入力 L2 PDU は、VLAN トンネル エッジ ポートでドロップされます（処理されません）。

- 01:80:C2:00:00:00-01:80:C2:00:00:FF（ただし、処理が行われてドロップされない LACP フレーム（宛先 MAC 01:80:C2:00:00:02）は除きます）
- 01:00:0C:00:00:00-01:00:0C:FF:FF:FF

VLAN トンネル設定の一部として、ドロップと転送のどちらを実施するか定義して、レイヤ 2 制御プロトコル PDU（CDP、LLDP、VTP、STP）をカプセル化することができます。これを L2CP トンネリングと呼びます。この機能では、特定のタグなしレイヤ 2 プロトコル フレームをプロバイダ ネットワークで転送できるトンネルが作成されます（タグ付きフレームはドロップされます）。この機能は、VLAN マッピング インターフェイスで設定します。L2CP トンネリング機能は、プロバイダ ネットワーク内のそれぞれ異なった側にある 2 つのカスタマーサイトを接続する際に有用です。この機能により、2 つのサイト間で、ISP クラウドを介したサポート対象プロトコルのパケットの転送が可能になります。

そのようなフレームをトンネリングするには、PDU をプロバイダ ネットワークで転送する際に VLAN ID（第 2 のタグ）として使用される VLAN を定義する必要があります。リモート カスタマー サイトで PDU が受信されると、外側の VLAN が除去され、PDU は、リモート カスタマー ネットワークにおいて、そのネットワークからの発信データと同様の処理を施されます。この機能では、インターフェイスごとの L2CP トンネル転送が可能になることに加え、カプセル化に使用する S-VLAN を割り当てたり、このトラフィック用の事前定義済み CoS を割り当てたり、インターフェイスによって転送される L2CP PDU のレートを制限したりすることもできます。

ワンツーワンの VLAN マッピング

VLANトンネリングに加えて、デバイスはVLANワンツーワンマッピングをサポートします。VLANワンツーワンマッピングでは、エッジインターフェイス（カスタマーネットワークがプロバイダーエッジスイッチに接続されるインターフェイス）上で、C-VLANがS-VLANにマッピングされ、オリジナルのC-VLANタグが指定されたS-VLANに置き換えられます。タグなしフレームは除去されます。フレームが非エッジのタグ付きインターフェイス上で送信される場合、単一の VLAN タグ、つまり、指定された S-VLAN のタグが付けられます。トラフィックがサービスプロバイダーのインフラストラクチャネットワーク経由でルーティングされている間は、サービス VLAN タグが保持されます。フレームがエッジインターフェイスに送信されるときに、出力デバイスの S-VLAN タグが C-VLAN タグに置き換えられます。ワンツーワン VLAN マッピングモードでは、インターフェイスは出力タグ付きインターフェイスとして定義されるマッピングを持つすべてのS-VLANに属します。インターフェイスのPVIDは4095に設定されます。

VLAN マッピング

バックボーンネットワークは、同じ VLAN 内の 2 つのレイヤ 2 ユーザーネットワークを接続できます。2 つのユーザーネットワークは、ユーザー間のレイヤ 2 接続を確保し、レイヤ 2 プロトコルを均一に展開するために、シームレスに相互運用する必要があります。ただし、バックボーンネットワークとユーザーネットワークの VLAN プランが異なるため、バックボーンネットワークはユーザーネットワークからの VLAN パケットを直接送信できません。この問題を解決するには、VLAN マッピングを構成します。ユーザーネットワークからの VLAN パケットがバックボーンネットワークに入ると、バックボーンネットワークのエッジデバイスはカスタマー VLAN（C-VLAN）ID をサービス VLAN（S-VLAN ID）に変更します。

パケットが送信された後、デバイスは VLAN ID の変更を元に戻します。これにより、2 つのユーザーネットワークがシームレスに通信できます。

VLAN マッピングを設定するには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [VLAN Translation] > [VLAN Mapping] の順にクリックします。

定義済みの VLAN マッピング設定のテーブルが表示されます。

ステップ 2 次のいずれかのマッピングタイプを選択します。

- [One to One]：1 対 1 VLAN マッピング モードに設定されたインターフェイスの設定を表示および編集するには、このオプションを選択します。
- [Tunnel Mapping]：トンネル VLAN マッピング モードに設定されたインターフェイスの設定を表示および編集するには、このオプションを選択します。

ステップ 3 [Add] をクリックして、次のフィールドに入力します。

- [Interface]：ポートを選択します。
- [Interface VLAN Mode]：現在のインターフェイス モードが表示されます。
- [Mapping Type]：次のいずれかを選択します。
  - [One to One]：1 対 1 VLAN マッピング設定を定義する場合には、このオプションを選択します。
  - [Tunnel Mapping]：このオプションは、トンネル VLAN マッピング設定を定義する場合に選択します。
- [One to One Translation]：このオプションは、[Mapping Type] の選択時に [one-to-one] オプションが選択された場合に表示されます。次のいずれかを選択します。
  - [Source VLAN]：S-VLAN（変換後の VLAN）に変換される顧客 VLAN（C-VLAN）の ID を設定します。
  - [Translated VLAN]：指定された C-VLAN を置き換える S-VLAN を設定します。
- [Tunnel Mapping]：このオプションは、[Mapping Type] の選択時に [Tunnel Mapping] オプションが選択された場合に表示されます。次のいずれかを選択します。
  - [Customer VLAN]：指定されていない C-VLAN に必要なアクションを定義する場合は [Default] を選択します。または、一覧表示された VLAN の VLAN トンネル動作を明示的に定義する場合は [VLAN List] を選択します。
  - [Tunneling]：[Drop] または [Outer VLAN ID] を選択します。[Outer VLAN ID] を選択した場合は、VLAN を入力します。

ステップ 4 [Apply] をクリックします。パラメータが、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。

プロトコル処理

各種のレイヤ2プロトコルは、トポロジを拡張し、ローカルサイトとリモートサイトの両方を組み込むために、サービス プロバイダー ネットワークを通して接続された各サイトのカスタマーが使用する必要があります。すべての VLAN は、サービス プロバイダー ネットワーク上のローカルサイトとリモートサイトを含む適切なスパニングツリーを確立する必要があり、STP は正しく機能する必要があります。近くにあるシスコの機器は、ローカルサイトとリモートサイトの両方から Cisco Discovery Protocol（CDP）によって検出される必要があります。VTP に参加しているカスタマーネットワークのすべてのサイトでは、VLAN トランキングプロトコル（VTP）を利用して矛盾しない VLAN 設定を提供する必要があります。

プロトコルトンネリングが有効の場合、インバウンド側のサービスプロバイダースイッチは、レイヤ 2 プロトコルパケットを特別な MAC アドレスを使用してカプセル化し、サービス プロバイダーネットワーク経由で送信します。このパケットはネットワークのコアスイッチでは処理されずに通常のパケットとして転送されます。CDP、STP、VTP のレイヤ 2 プロトコルデー

タユニット（PDU）は、サービスプロバイダーネットワークを通過し、サービスプロバイダーネットワークのアウトバウンド側のカスタマースイッチに配信されます。

VLAN 変換トンネルエッジポートで受信される L2CP PDU の処理を設定するには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [VLAN Translation] > [Protocol Handling] の順にクリックします。

各種のレイヤ 2 プロトコルは、トポロジを拡張し、ローカルサイトとリモートサイトの両方を組み込むために、サービスプロバイダーネットワークを通して接続された各サイトのカスタマーが使用する必要があります。すべての VLAN は、サービス プロバイダー ネットワーク上のローカルサイトとリモートサイトを含む適切なスパニングツリーを確立する必要があり、STP は正しく機能する必要があります。近くにあるシスコの機器は、ローカルサイトとリモートサイトの両方から Cisco Discovery Protocol（CDP）によって検出される必要があります。VTP に参加しているカスタマーネットワークのすべてのサイトでは、VLAN トランキングプロトコル（VTP）を利用して矛盾しない VLAN 設定を提供する必要があります。

（注）
インターフェイスごとにプロトコル処理動作を設定するには、ハードウェアリソースを VLAN マッピング機能に割り当てる必要があります。

ステップ 2 [Default Tunneling CoS] を設定します。0 ～ 7 の値（デフォルト = 5）を入力して、VLAN トンネリングエッジポートで転送およびカプセル化される L2CP PDU に適用するグローバル CoS 値を定義します。この値は、特定のユーザー CoS 設定を持たないすべてのインターフェイスに使用されます。

ステップ 3 リスト内のいずれか 1 つのエントリを選択して [Copy Settings] をクリックすると、選択したエントリの設定が、1つまたは複数のエントリにコピーされます。選択したエントリを編集するには[Edit]をクリックします。

ステップ 4 次のフィールドを入力します。

- [Interface]：ポートを選択します。
- [Interface VLAN Mode]：現在のインターフェイス VLAN モードが表示されます。
- [BPDU VLAN ID]：次のいずれかを選択します。
  - [None]：L2CP BPDU トンネリングのために選択されている VLAN はありません。このオプションは、L2CP PDU のトンネリングを無効にする場合に使用します。
  - [VLAN ID]：このインターフェイスで L2CP PDU をトンネリングする際に使用する VLAN ID を選択します。
- [CoS]：次のいずれかを選択します。
  - [Use Default]：グローバルなデフォルト値を使用する場合に選択します。
  - [User defined]：このオプションを選択し、0 ～ 7 の範囲で値を設定します。

- [Drop threshold]：次のいずれかを選択します。
  - [None]：ドロップしきい値を無効にする場合に選択します。
  - [User defined]：しきい値を 8 ～ 256 Kbps に設定する場合に選択します（デフォルトは 32 Kbps）。
- [Protocol Forwarding]：デバイスで転送およびカプセル化するプロトコルを選択します。
  - [CDP]：このプロトコルの転送およびカプセル化を有効にする場合に選択します。
  - [LLDP]：このプロトコルの転送およびカプセル化を有効にする場合に選択します。
  - [STP]：このプロトコルの転送およびカプセル化を有効にする場合に選択します。
  - [VTP]：このプロトコルの転送およびカプセル化を有効にする場合に選択します。

ステップ 5 [Apply] をクリックします。パラメータが、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。

プライベートVLAN設定

スイッチ上のポートを互いに分離するために、プライベート VLAN は VLAN のイーサネット ブロードキャスト ドメインをサブドメインに分割します。プリンシパル VLAN と 1 つ以上のサブ VLAN がサブドメインを構成します。プライベート VLAN ドメインにあるすべての VLAN によって、プライマリ VLAN が共有されます。あるサブドメインは、セカンダリ VLAN ID を使用して別のサブドメインと区別できます。

プライベート VLAN 機能は、ポート間でのレイヤ 2 の分離を提供します。つまり、IP ルーティングとは異なり、ブリッジングトラフィックのレベルで、同じブロードキャストドメイン内のポートが相互に通信することはできません。プライベート VLAN 内のポートは、レイヤ 2 ネットワークの任意の場所に配置できます。よって、これらのポートは同じスイッチ上にある必要はありません。プライベート VLAN は、タグなしのトラフィックかプライオリティタグ付きのトラフィックを受信して、タグなしのトラフィックを送信することを目的としています。

新しいプライベート VLAN を作成するには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [Private VLAN Settings] をクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 次のフィールドに値を入力します。

- [Primary VLAN ID]：プライベート VLAN でプライマリ VLAN として定義する VLAN を選択します。プライマリ VLAN は、無差別ポートから隔離ポートおよびコミュニティ ポートにレイヤ 2 で接続できるようにするために使用します。

- [Isolated VLAN ID]：隔離 VLAN は、隔離ポートがプライマリ VLAN にトラフィックを送信する場合に使用します。
- [Available Community VLANs]：コミュニティ VLAN にする VLAN を [Selected Community VLANs] リストに移動します。コミュニティ VLAN により、コミュニティポートからプロミスキャスポートや同じコミュニティのコミュニティポートへのレイヤ 2 接続が可能になります。これはメイン ページでは [Community VLAN Range] と表示されます。

ステップ 4 [Apply] をクリックします。設定が変更され、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。

GVRP設定

Generic VLAN Registration Protocol（GVRP）は、大規模なネットワーク内で VLAN を制御できるようにする標準ベースのプロトコルです。GVRP は IEEE 802.1Q 仕様に準拠しています。IEEE 802.1Q 仕様は、ネットワーク トランク インターコネクト上でフレームに VLAN 構成データをタグ付けする方法を定義しています。これにより、ネットワークデバイスは VLAN 構成情報を他のデバイスとその場で交換できます。

GVRP は、各ポート上だけでなくグローバルに有効化する必要があります。オンにすると、GVRP によって GARP パケットデータ単位（GPDU）が送受信されます。定義済みであってもまだ非アクティブな VLAN の情報は伝達されません。伝達するには、VLAN が少なくとも 1 つのポートでアクティブになっている必要があります。デフォルトでは、GVRPはグローバルでも、ポートでも無効になっています。

インターフェイスの GVRP 設定を定義するには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [GVRP Settings] をクリックします。

ステップ 2 [GVRP Global Status] を選択して、GVRP をグローバルで有効にします。

ステップ 3 [Apply] をクリックして、グローバル GVRP ステータスを設定します。

ステップ 4 インターフェイスの種類（ポートまたは LAG）を選択して [Go] をクリックし、その種類のすべてのインターフェイスを表示します。

ステップ 5 ポートの GVRP 設定を定義するには、ポートを選択して [Edit] をクリックします。

ステップ 6 次のフィールドに値を入力します。

- [Interface]：編集するインターフェイス（ポートまたは LAG）を選択します。
- [GVRP State]：インターフェイスで GVRP を有効にする場合に選択します。
- [Dynamic VLAN Creation]：このインターフェイスで動的な VLAN の作成を有効にする場合に選択します。

- [GVRP Registration]：このインターフェイスで GVRP を使用した VLAN の登録を有効にする場合に選択します。

ステップ 7 [Apply]をクリックします。GVRP設定が変更され、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。

VLAN グループ

VLAN グループは、タグ付きまたはタグなしの VLAN の論理グループです。VLAN がタグ付けされている場合、その VLAN との間で送受信される各パケットには VLAN ID が含まれます。ネットワークトラフィックには、タグ付きパケットとタグなしパケットの両方を含めることができます。パケットに VLAN タグがない場合、パケットはタグなし VLAN に送信されます。

VLAN グループは、レイヤ 2 ネットワークでのトラフィックのロード バランシングに使用されます。パケットは、さまざまな分類に従って VLAN に割り当てられます。分類スキームを複数定義した場合は、次の順序で VLAN にパケットが割り当てられます。

- タグ：パケットがタグ付きの場合、VLAN はタグから取得されます。
- MAC ベースの VLAN：MAC ベースの VLAN が定義されている場合、VLAN は入力インターフェイスの送信元 MAC から VLAN へのマッピングにより取得されます。
- サブネットベースの VLAN：サブネットベースの VLAN が定義されている場合、VLAN は入力インターフェイスの送信元 IP から VLAN へのマッピングにより取得されます。
- プロトコルベースの VLAN：プロトコルベースの VLAN が定義されている場合、VLAN は入力インターフェイスの（イーサネットの種類）プロトコルから VLAN へのマッピングにより取得されます。
- PVID：VLAN は、ポートのデフォルト VLAN ID から取得されます。

MACベースグループ

MAC ベースの VLAN 分類を使用すると、パケットを送信元 MAC アドレスによって分類できます。この場合、インターフェイスごとに MAC から VLAN へのマッピングを定義できます。また、それぞれが独自の MAC アドレスのセットを持つ複数の MAC ベースの VLAN グループを定義することもできます。特定のポートや LAG をこれらの MAC ベースグループに割り当てることができます。MAC ベース VLAN グループには、同じポート上の重複する MAC アドレス範囲を含めることはできません。

デバイスの MAC アドレスに基づいてパケットを転送するには、MAC アドレスのグループを作成し、VLAN にマッピングする必要があります。最大 256 個の MAC アドレス（ホストまたは範囲）を構成し、1 つまたは複数の MAC ベースの VLAN グループにマッピングできます。

VLAN グループに MAC アドレスを割り当てるには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [VLAN Groups] > [MAC-Based Groups] をクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 次のフィールドに値を入力します。

- [MAC Address]：VLAN グループに割り当てる MAC アドレスを入力します。

  （注）
  この MAC アドレスを他の VLAN グループに割り当てることはできません。

- [Prefix Mask]：次のいずれかを入力します。
  - [Host(48)]：プレフィックス マスク（48 ビット）に MAC アドレスのすべてのビットを含める場合
  - [Length]：MAC アドレスのプレフィックス

- [Group ID]：ユーザ作成の VLAN グループ ID 番号を入力します。

ステップ 4 [Apply] をクリックします。MAC アドレスが VLAN グループに割り当てられます。

VLANに対するMACベースグループ

インターフェイス上の VLAN に MAC ベース VLAN グループを割り当てるには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [VLAN Groups] > [MAC-Based Groups to VLAN] をクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 次のフィールドに値を入力します。

- [Group Type]：グループが MAC ベースであることが表示されます。
- [Interface]：トラフィックを受信する全般インターフェイス（ポートまたは LAG）を入力します。
- [Group ID]：VLAN グループを選択します。
- [VLAN ID]：VLAN グループからのトラフィックを転送する VLAN を選択します。

ステップ 4 [Apply] をクリックして、VLAN グループから VLAN へのマッピングを設定します。このマッピングはインターフェイスを VLAN に動的にバインドしないため、インターフェイスを VLAN に手動で追加する必要があります。

サブネットベースグループ

サブネットベース グループの VLAN 分類により、サブネットに基づいてパケットを分類することができます。その後、インターフェイスごとにサブネットから VLAN へのマッピングを定義することができます。複数の異なるサブネットを含むサブネットベース VLAN グループが複数定義できます。

これらのグループは、特定のポートまたはLAGに割り当てることができます。サブネットベース VLAN グループ間では、同一ポートでサブネット範囲を重複させることはできません。

サブネットベースのグループを追加するには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [VLAN Groups] > [Subnet-Based Groups] の順にクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 次のフィールドに入力します。

- [IP Address]：サブグループの元になる IP アドレスを入力します。
- [Prefix Mask]：サブネットを定義するプレフィックス マスクを入力します。
- [Group ID]：グループ ID を入力します。

ステップ 4 [Apply] をクリックします。グループが追加され、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。

VLANに対するサブネットベースグループ

サブネット グループをポートにマッピングするには、ポート上で DVA を設定しないようにする必要があります（インターフェイスの設定 （3 ページ）を参照）。複数のグループを単一ポートに結合でき、各ポートがそれぞれ独自の VLAN に関連付けられています。複数のグループを単一の VLAN にマッピングすることもできます。

サブネットグループを VLAN にマッピングするには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [VLAN Groups] > [Subnet-Based Groups to VLAN] の順にクリックします。

ステップ 2 インターフェイスをプロトコルベース グループと VLAN に関連付けるには、[Add] をクリックします。

[Group Type] フィールドには、マッピングされているグループの種類が表示されます。

ステップ 3 次のフィールドに入力します。

- [Interface]：プロトコルベース グループに従って VLAN に割り当てられるポートまたは LAG 番号。
- [Group ID]：プロトコルグループ ID。
- [VLAN ID]：このインターフェイスに指定したグループを、ユーザ定義の VLAN ID に結びつけます。

ステップ 4 [Apply] をクリックします。サブネットベース グループのポートが VLAN にマッピングされ、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。

プロトコルベースグループ

プロトコルのグループを定義し、ポートにバインドできます。プロトコル グループをポートにバインド後、グループ内のプロトコルに基づいて生成されたすべてのパケットが、プロトコルベース グループ ページで設定された VLAN に割り当てられます。一連のプロトコルを定義するには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [VLAN Groups] > [Protocol-Based Groups] をクリックします。

ステップ 2 [Add] をクリックして、プロトコルベース VLAN グループを追加します。

ステップ 3 次のフィールドに入力します。

- [Encapsulation]：プロトコルパケットタイプ。次のオプションを使用できます。
  - [Ethernet V2]：これを選択した場合には、[Ethernet Type] を選択します。
  - [LLC-SNAP（rfc1042]：これを選択した場合には、[Protocol Value] を入力します。
  - [LLC]：これを選択した場合には、[DSAP-SSAP Values] を選択します。
- [Ethernet Type]：イーサネット V2 カプセル化のイーサネットの種類を選択します。これは、VLAN グループのイーサネットパケットのペイロード内にカプセル化されているプロトコルを示すために使用される、イーサネットフレーム内の 2 オクテットのフィールドです。
- [Protocol Value]：LLC-SNAP（rfc 1042）カプセル化のプロトコルを入力します。

• [Group ID]：プロトコル グループ ID を入力します。

ステップ 4 [Apply] をクリックします。プロトコル グループが追加され、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。

VLANに対するプロトコルベースグループ

プロトコルベースの VLAN は、物理ネットワークを各プロトコルの論理 VLAN グループに分割します。フレームがポートで受信されると、その VLAN メンバーシップはプロトコルタイプに基づいて決定されます。複数のグループを単一ポートに結合でき、各ポートがそれぞれ独自の VLAN に関連付けられています。いくつかのグループを単一のポートにマッピングすることもできます。

プロトコルポートを VLAN にマッピングするには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [VLAN Groups] > [Protocol-Based Groups to VLAN] をクリックします。

ステップ 2 インターフェイスをプロトコルベース グループと VLAN に関連付けるには、[Add] をクリックします。

[Group Type] フィールドには、マッピングされているグループの種類が表示されます。

ステップ 3 次のフィールドに入力します。

• [Interface]：プロトコルベース グループに従って VLAN に割り当てられるポートまたは LAG 番号。

• [Group ID]：プロトコルグループ ID。

• [VLAN ID]：インターフェイスを、ユーザ定義の VLAN ID に結びつけます。

ステップ 4 [Apply] をクリックします。プロトコル ポートが VLAN にマッピングされ、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。

Voice VLAN

音声 VLAN 機能を使用すると、IP フォンからの IP 音声トラフィックをアクセスポートで伝送できます。IP フォンがスイッチに接続されると、その IP フォンはレイヤ 3 IP プレシデンス値およびレイヤ 2 サービスクラス（CoS）値として 5（どちらの値もデフォルトの設定値）を使用して、音声トラフィックを送信します。データ伝送が均質性に欠ける場合、IP フォンの音質が劣化することがあります。そのため、このスイッチでは、IEEE 802.1p CoS に基づく Quality of Service（QoS）をサポートしています。スイッチからのネットワークトラフィックを予測可能な方法で送信するため、QoS は分類およびスケジューリングを使用します。

音声 VLAN は、LLDP-MED ネットワークルールを使用して CoS/802.1p 設定や DSCP 設定を伝達できます。アプライアンスが LLDP-MED パケットを送信する場合、LLDP-MED はデフォルトでは音声 QoS オプションを使用して応答するように設定されます。MED をサポートするデバイスが送信する音声トラフィックは、LLDP-MED 応答で受け取ったものと同じ CoS/802.1p パラメータおよび DSCP パラメータを使用する必要があります。ユーザーは、独自のネットワーク設定を使用したり、音声 VLAN と LLDP-MED の間の自動更新を無効にしたりできます。OUIモードで使用する場合、デバイスはさらに、OUIに基づく音声トラフィックのマッピングと検知（CoS/802.1p）を設定できます。

デフォルトでは、すべてのインターフェイスはCoS/802.1pで信用されます。デバイスは、音声ストリームで検出された CoS/802.1p 値に基づいて QoS を適用します。テレフォニー OUI 音声ストリームでは、QoS をオーバーライドでき、必要に応じて、必要なCoS/802.1p値を指定し、テレフォニー OUI の検知オプションを使用することで、音声ストリームの 802.1p を検知できます。

プロパティ

音声 VLAN のプロパティ ページを使用して、次が行えます。

- 音声 VLAN の現在の設定内容を表示します。
- 音声 VLAN の VLAN ID を設定します。
- 音声 VLAN の QoS を設定します。
- 音声 VLAN のモード（テレフォニー OUI または自動音声 VLAN）を設定します。
- 自動音声 VLAN のトリガー方法を設定します。

音声 VLAN のプロパティを表示および設定するには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [Voice VLAN] > [Properties] をクリックします。

- デバイスに設定されている音声 VLAN の設定が、[Voice VLAN Settings (Administrative Status)] ブロックに表示されます。
- 音声 VLANの導入に対して実際に適用されている音声 VLAN設定が、[Voice VLAN Settings (Operational Status)] ブロックに表示されます。

（注）
Auto SmartportとテレフォニーOUIを同時に使用することはできません。CoS/802/1p および DSCP の値は、LLDP MED ネットワークポリシーと自動音声 VLAN に対してのみ使用されます。

ステップ 2 次の [Administrative Status] フィールドに値を入力します。

- [Voice VLAN ID]：音声 VLAN にする VLAN を入力します。

（注）
音声 VLAN ID、CoS/802.1p、DSCP を変更すると、デバイスは、管理音声 VLAN をスタティック音声 VLAN としてアドバタイズします。外部音声 VLAN によってトリガーされる [Auto Voice VLAN Activation] オプションを選択した場合は、デフォルト値のままにしておく必要があります。

- [CoS/802.1p]：音声ネットワークポリシーとして LLDP-MED の CoS/802.1p 値を選択します。詳細については、[Administration] > [Discovery] > [LLDP] > [LLDP MED Network Policy] を参照してください。
- [DSCP]：音声ネットワークポリシーとして LLDP-MED の DSCP 値を選択します。詳細については、[Administration] > [Discovery] > [LLDP] > [LLDP MED Network Policy] を参照してください。

  次の [Operational Status] フィールドが表示されます。
- [Voice VLAN ID]：音声 VLAN。
- [CoS/802.1p]：LLDP-MED により音声ネットワーク ポリシーとして使用されている値。詳細については、[Administration] > [Discovery] > [LLDP] > [LLDP MED Network Policy] を参照してください。
- [DSCP]：音声ネットワーク ポリシーとして LLDP-MED で使用される値。

  次の [Dynamic Voice VLAN Settings] フィールドが表示されます。
- [Dynamic Voice VLAN]：次のいずれかの方法で音声 VLAN 機能を無効または有効にするにはこのフィールドを選択します。
  - [Enable Auto Voice VLAN]：ダイナミック音声 VLAN を自動音声 VLAN モードで有効にします。
  - [Enable Telephony OUI]：テレフォニー OUI モードでダイナミック音声 VLAN を有効化します。
  - [Disable]：自動音声 VLAN またはテレフォニー OUI を無効にします
- [Auto Voice VLAN Activation]：自動音声 VLAN が有効な場合は、自動音声VLAN をアクティブ化するために、次のいずれかのオプションを選択します。
  - [Immediate]：有効にすると、デバイスでただちに自動音声 VLAN がアクティブになり、動作状態になります。
  - [By external Voice VLAN trigger]：音声 VLAN をアドバタイズするデバイスをデバイスが検出した場合にのみ、デバイス上の自動音声 VLAN がアクティブになり、動作状態になります。

    （注）
    音声 VLAN ID、CoS/802.1p、DSCP のすべて、またはいずれかを手動でデフォルト値から再設定すると、自動音声 VLAN よりもプライオリティが高いスタティック音声 VLAN になります。

ステップ 3 [Apply] をクリックします。VLAN のプロパティが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。

自動音声 VLAN

自動音声 VLAN は音声 VLAN を維持しますが、音声 VLAN ポートのメンバーシップの維持は Auto Smartport に依存します。自動音声 VLAN は動作時には次の機能を実行します。

アクティブにすると、自動音声 VLAN は次のタスクを実行します。

- 直接接続されたネイバーデバイスからの CDP アドバタイズメントで、音声 VLAN の情報を検索します。
- 複数のネイバースイッチやルータ（Cisco Unified Communications（UC）デバイスなど）がそれぞれの音声 VLAN をアドバタイズしている場合、MAC アドレスが最も小さいデバイスからの音声 VLAN が使用されます。

自動音声 VLAN モードが有効になっている場合は、自動音声 VLAN ページを使用して、関連するグローバルおよびインターフェイスのパラメータを表示します。

また、このページを使用して、[Restart Auto Voice VLAN] をクリックして自動音声 VLAN を手動で再起動することができます。これにより、短い遅延の後、音声 VLAN がデフォルトの音声 VLAN にリセットされ、自動音声 VLAN 検出が再起動されて、自動音声 VLAN が有効な LAN 内のすべてのスイッチで同期プロセスが再実行されます。

（注） [Source Type] が [Inactive] の状態の場合、音声 VLAN をデフォルトの音声 VLAN にリセットする処理のみが実行されます。

自動音声 VLAN パラメータを表示するには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [音声 VLAN（Voice VLAN] > [Auto Voice VLAN] をクリックします。

このページの [Operational Status] ブロックに、現在の音声 VLAN およびそのソースに関する情報が表示されます。

- [Auto Voice VLAN Status]：自動音声 VLAN が有効か無効かを表示します。
- [Voice VLAN ID]：現在の音声 VLAN の ID。
- [Source Type]：ルート デバイスで音声 VLAN を検出する送信元の種類が表示されます。
- [CoS/802.1p]：LLDP-MED により音声ネットワーク ポリシーとして使用される CoS/802.1p 値を表示します。
- [DSCP]：LLDP-MED により音声ネットワーク ポリシーとして使用される DSCP 値を表示します。
- [Root Switch MAC Address]：自動音声 VLAN ルート デバイスの MAC アドレ ス。ルート デバイスは、この音声 VLAN の学習元となった音声 VLAN によって検出 または設定されたものです。

- [Switch MAC Address]：デバイスの基本 MAC アドレス。デバイスのスイッチ MAC アドレスがルートスイッチ MAC アドレスの場合、デバイスは自動音声 VLAN のルート デバイスです。
- [Voice VLAN ID Change Time]：音声 VLAN が更新された最後の時刻。

ステップ 2 [Restart Auto Voice VLAN] をクリックすると、音声 VLAN がデフォルトの音声 VLAN にリセットされ、自動音声 VLAN が有効な、LAN 内のすべてのスイッチの自動音声 VLAN 検出が再起動されます。

[Voice VLAN Local Source Table] には、デバイスで設定されている音声 VLAN、および直接接続されたネイバーデバイスによってアドバタイズされた音声 VLAN の設定が表示されます。ファイルには、次のフィールドがあります。

- [Interface]：音声 VLAN 設定を受信または設定されたインターフェイスが表示されます。[N/A] が表示された場合には、デバイス自身に設定が行われています。インターフェイスが表示された場合には、ネイバーから受信した音声設定が使用されています。
- [Source MAC Address]：音声設定の受信元 UC の MAC アドレス。
- [Source Type]：音声設定の受信元 UC のタイプ。次のオプションを使用できます。
  - [Default]：デバイスのデフォルトの音声 VLAN 設定。
  - [Static]：デバイス上に定義されているユーザー定義の音声 VLAN 設定。
  - [CDP]：音声 VLAN 設定が CDP を実行していることをアドバタイズした UC。
  - [LLDP]：音声 VLAN 設定が LLDP を実行していることをアドバタイズした UC。
  - [Voice VLAN ID]：アドバタイズまたは設定された音声 VLAN の識別子。
- [Voice VLAN ID]：現在の音声 VLAN の識別子。
- [CoS/802.1p]：LLDP-MED により音声ネットワーク ポリシーとして使用される、アドバタイズまたは設定された CoS/802.1p 値。
- [DSCP]：LLDP-MED により音声ネットワーク ポリシーとして使用される、アドバタイズまたは設定された DSCP 値。
- [Best Local Source]：この音声 VLAN がデバイスにより使用されたかどうかが表示されます。次のオプションを使用できます。
  - [Yes]：デバイスはこの音声 VLAN を使用して、自動音声 VLAN が有効な他のスイッチと同期します。より優先順位の高い送信元からの音声 VLAN が検出されない限り、この音声 VLAN がネットワークの音声 VLAN です。最適なローカル送信元はただ 1 つだけです。
  - [No]：この音声 VLAN は最適なローカルソースではありません。

ステップ 3 ページ上の情報を更新するには、[Refresh] をクリックします。

テレフォニー OUI

Voice over Internet Protocol（VoIP）機器からのトラフィックが、IP 電話、VoIP エンドポイント、音声システムなどの音声デバイスで構成される特定の VLAN に割り当てられている場合、音声仮想ローカルエリアネットワーク（VLAN）が使用されます。スイッチでは、ポートメンバーを検出して音声 VLAN に自動的に追加し、設定された Quality of Service（QoS）を音声 VLAN からのパケットに割り当てます。音声デバイスが別々の音声 VLAN 内にある場合、音声デバイス間で通信を行うには IP ルータが必要です。

組織固有識別子（OUI）を使用して、特定の製造者の Media Access Control（MAC）アドレスを OUI テーブルに追加できます。MAC アドレスの最初の 3 バイトには製造者 ID が含まれ、最後の 3 バイトには一意のステーション ID が含まれています。OUI がテーブルに追加されると、IP 電話が OUI テーブルにリストされている場合、音声 VLAN ポートのポートで特定の IP 電話から受信した音声は音声 VLAN に転送されます

受信したパケットの送信元 MAC アドレスは、スイッチによってチェックされ、音声パケットであるかどうかが判断されます。VoIP トラフィックの送信元 MAC アドレスには、事前構成済みの OUI プレフィックスが含まれています。特定の製造者の MAC アドレスと説明を OUI テーブルに手動で入力できます。OUI がリストされている特定の IP 電話から音声 VLAN ポートで受信したすべてのトラフィックは、音声 VLAN にルーティングされます。

テレフォニー OUI を設定したり、新しい音声 VLAN OUI を追加したりするには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [Voice VLAN] > [Telephony OUI] をクリックします。

テレフォニー OUI ページには次のフィールドがあります。

- [Telephony OUI Operational Status]：OUI が音声トラフィックの識別に使用されて いるかどうかを表示します。
- [CoS/802.1p]：音声トラフィックに割り当てる CoS キューを選択します。
- [Remark CoS/802.1p]：出トラフィックをリマークするかどうかを選択します。
- [Auto Membership Aging Time]：ポートで検出された電話の MAC アドレスす べてが期限切れになった後、音声 VLAN からそのポートを削除するまでの遅延時間 を入力します。

ステップ 2 [Apply] をクリックして、デバイスの実行コンフィギュレーションをこれらの値で更新します。

ステップ 3 [Restore Default OUIs] をクリックすると、ユーザーが作成した OUI はすべて削除され、デフォルトの OUI のみがテーブルに残ります。次のメッセージを含むポップアップが表示されます。「ユーザー定義の OUI がすべて消去されます。続行しますか?（All User-defined OUIs will be erased. Do you want to continue?）」[OK] をクリックします。

すべての OUI を削除するには、上部のチェックボックスをオンにします。すべての OUI が選択され、[Delete] をクリックすることで削除できます。その後、[Restore Default OUIs] をクリックすると、既知の OUI が復元されます。

ステップ 4 新しい OUI を追加する場合には、[Add] をクリックします。

ステップ 5 次のフィールドに値を入力します。

- [Telephony OUI]：新しい OUI を入力します。
- [Description：OUI 名を入力します。

ステップ 6 [Apply] をクリックします。OUI がテレフォニー OUI テーブルに追加されます。

電話機 OUI インターフェイス

QoS 属性は、次のいずれかのモードで、ポートごとに音声パケットに割り当てることができます。

- [All]：そのインターフェイスで受信され、音声 VLAN に分類されるすべての着信フレームに、その音声 VLAN に設定されている Quality of Service（QoS）値が適用されます。
- [Telephony Source MAC Address (SRC)]：音声 VLAN に設定された QoS 値は、音声 VLAN へと分類されるすべての受信フレームに適用され、設定したテレフォニー OUI と一致する送信元 MAC アドレスの OUI が含まれます。

テレフォニー OUI インターフェイス ページを使用して、OUI 識別子に基づいて音声 VLAN にインターフェイスを追加し、音声 VLAN の OUI QoS モードを設定します。

インターフェイスでテレフォニー OUI を設定するには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [Voice VLAN] > [Telephony OUI Interface] をクリックします。

テレフォニー OUI インターフェイス ページには、すべてのインターフェイスの音声 VLAN OUI パラメータが表示されます。

ステップ 2 インターフェイスをテレフォニー OUI ベース音声 VLAN の候補ポートに設定するには、[Edit] をクリックします。

ステップ 3 次のフィールドに値を入力します。

- [Interface]：ポートまたは LAG インターフェイスを選択します。
- [Telephony OUI VLAN Membership]：有効にすると、インターフェイスは、テ レフォニー OUI ベースの音声 VLAN の候補ポートになります。設定されているテレフォニー OUI のいずれかと一致するパケットを受信すると、ポートは音声 VLAN に追加されます。

- [Voice VLAN QoS Mode]（メイン ページでは [Telephone OUI QoS Mode]）：次のオプションのいずれかを選択します。
  - [All]：QoS 属性は音声 VLAN へと分類されるすべてのパケットに適用されます。
  - [Telephony Source MAC Address]：IP 電話からのパケットのみに QoS 属性が適用されます。

ステップ 4 [Apply] をクリックします。OUI が追加されます。

自動監視 VLAN

多くの場合、カメラや監視機器などの監視デバイス間のネットワーク通信には、より高い優先順位を与える必要があり、組織内の監視インフラストラクチャを構成するさまざまなデバイスが相互に到達可能であることが重要です。通常、ネットワーク管理者は、すべての監視デバイスが同じ VLAN に接続されていることを確認し、この優先度の高いトラフィックを許可するようにこの VLAN とそのインターフェイスを設定する必要があります。

自動監視 VLAN（ASV）機能は、ネットワーク上の監視デバイスを検出して VLAN に割り当て、それらのトラフィックの優先順位を設定することにより、このセットアップを自動化します。

ASV の一般設定

ユーザーは、OUI と MAC アドレスのリストを作成して、ネットワーク上の監視トラフィックを定義します。この機能が有効になっているインターフェイス上で、OUI または MAC アドレスのいずれかに送信元が一致するトラフィックは、監視トラフィックと見なされます。MAC と OUI の任意の組み合わせで、監視トラフィックに最大 32 の送信元を定義できます。

ASV の構成

この機能をアクティブにする場合、ユーザーは既存の静的 VLAN を選択して ASV VLAN として指定する必要があります。次に、ユーザーは、この VLAN のトラフィックの CoS と、VLAN メンバーシップのエージングタイムを設定します。最後に、監視トラフィックを受信すると予想されるインターフェイスで ASV 機能をアクティブにする必要があります。

ASV の一般的な設定を行うには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [Auto-Surveillance VLA] > [ASV General Settings] をクリックします。

ステップ 2 ドロップダウンメニューから、自動監視 VLAN の ID を選択します。この設定は、ASV VLAN ID を選択するために使用されます。[None] を選択すると、機能は無効になります。

ステップ 3 CoS を入力します。この設定は、ASV の監視トラフィックに適用されるサービスクラス（CoS）を選択するために使用されます。指定できる範囲は 0 ～ 7 です。デフォルト値は 5 です。

ステップ 4 [Membership Aging Time] には、日、時間、分を入力します（範囲：1 分～ 30 日、デフォルトは 1 日）。この設定は、ASV メンバーシップのエージングタイムを構成するために使用されます。このエージングタイム内にインターフェイスで監視トラフィックが受信されない場合、そのインターフェイスはASVから削除されます。

ステップ 5 [Add] をクリックして監視トラフィック送信元を追加し、以下を構成します。

- [Source Type]：次のいずれかを選択します。
  - OUI Prefix
  - MAC Address
- [Source]：送信元を入力します。このフィールドの検証とヒントは、選択した送信元タイプに基づいて変わります。タイプが [OUI Prefix] の場合、値はユニキャスト MAC アドレスの 3 オクテットのプレフィックスである必要があります。

  タイプが [MAC Address] の場合、値はユニキャスト MAC アドレスである必要があり、ヒントは表示されません。
- [Description]：送信元の説明を入力します

ステップ 6 [Apply] をクリックして設定を保存します。

ASV インターフェイス設定

ユーザーは、選択したインターフェイスで自動監視機能をアクティブにします。この機能は、一般またはアクセス VLAN モードのポートまたは LAG でアクティブにできます。

ASVが有効になっているインターフェイスで監視トラフィックが検出されると、このトラフィックは ASV にルーティングされます。一般 VLAN モードのインターフェイスでは、各監視トラフィックは、ACLおよびQoSルールと共有されるリソーステーブルのエントリを消費します。このテーブルの消費されたエントリの数を表示するには、[Hardware Resource Utilization] ページに移動します。

ASV インターフェイス設定を行うには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [Auto-Surveillance VLAN] > [ASV Interface Settings] をクリックします。

ステップ 2 インターフェイスタイプとしてポートまたは LAG を選択し、[Go] をクリックします。

ステップ 3 ASV インターフェイス設定を編集するには、[Edit] をクリックします。

ステップ 4 次にインターフェイス（ポートまたは LAG）を選択します。

ステップ 5 [Enable] をオンにして、自動監視 VLAN メンバーシップを有効にします。

ステップ 6 [Apply] をクリックして設定を保存します。

アクセスポートマルチキャストTV VLAN

マルチキャスト TV VLAN では、同じデータ VLAN（レイヤ 2 隔離）ではないサブスクライバに対して、サブスクライバ VLAN ごとにマルチキャスト伝送フレームを複製せずに、マルチキャスト伝送が行えます。

同じデータ VLAN（レイヤ 2 隔離）ではなく、異なる VLAN ID メンバーシップでデバイスに接続しているサブスクライバは、同じマルチキャスト VLAN ID へのポートに参加することで、同じマルチキャスト ストリームを共有できます。

マルチキャスト サーバに接続しているネットワーク ポートは、マルチキャスト VLAN ID のメンバーとして静的に設定されます。

サブスクライバが（IGMP メッセージの送信による）マルチキャスト サーバとの通信に使用するネットワーク ポートは、マルチキャスト パケット ヘッダーにマルチキャスト TV VLAN を含んだマルチキャスト ストリームを、マルチキャスト サーバから受信します。このため、ネットワーク ポートは静的に次のように設定する必要があります。

- ポートの種類はトランクまたは全般（「インターフェイスの設定 （3 ページ）」を参照）
- マルチキャスト TV VLAN のメンバー

アクセス ポートとして定義されている場合にのみ、サブスクライバの受信者ポートはマルチキャスト TV VLAN と関連付けることができます。

1 つまたは複数の IP マルチキャスト アドレスのグループを、同じマルチキャスト TV VLAN に関連付けることができます。

すべての VLAN がマルチキャスト TV VLAN として設定できます。マルチキャスト TV VLAN に割り当てられたポートは、次のようになります。

- マルチキャスト TV VLAN に参加します。
- マルチキャスト TV VLAN の出力ポートを通過するパケットは、タグなしです。
- ポートのフレームタイプパラメータは [Admit All] に設定され、タグなしパケットが許可されます（インターフェイスの設定 （3 ページ）を参照）。

マルチキャスト TV VLAN の設定は、ポートごとに定義されます。顧客ポートは、[Port Multicast VLAN Membership] ページを使用してマルチキャスト TV VLAN のメンバーに設定されます。

VLANに対するマルチキャストグループ

最大 256 組の IPv4 アドレス範囲がマルチキャスト TV VLAN にマッピングできます。範囲ごとに、マルチキャストアドレスの全範囲を設定できます。

（注） *は、関連するマルチキャストTV VLANが存在しなくなったため、対応するマルチキャストグループが非アクティブであることを示します。VLAN 設定 （1 ページ）に進んで、VLAN を作成します。

マルチキャスト TV VLAN 設定を定義するには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [Access Port Multicast TV VLAN] > [Multicast Group to VLAN] の順にクリックします。

ステップ 2 [Add] をクリックして、マルチ キャスト グループを VLAN に関連付けます。任意の VLAN が選択できます。

次のフィールドに入力します。

- [Multicast TV VLAN]：マルチキャスト パケットが割り当てられている VLAN。ここで選択した VLAN がマルチキャスト TV VLAN になります。
- [Multicast Group Start]：マルチキャスト グループ範囲の最初の IPv4 アドレス。
- [Group Definition]：次の範囲オプションのいずれかを選択します。
  - [By group size]：グループ範囲のマルチキャスト アドレスの数を指定します。
  - [By range]：[Multicast Group Start] フィールドのアドレスよりも大きい IPv4 マルチキャスト アドレスを指定します。これが範囲内の最後のアドレスです。

ステップ 3 [Apply] をクリックします。マルチキャスト TV VLAN 設定が変更され、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。

ポートマルチキャスト TV VLAN メンバーシップ

マルチキャスト TV VLAN では、同じデータ VLAN 上に存在しない（レイヤ 2 隔離）のサブスクライバへのマルチキャスト伝送が可能で、その際、サブスクライバ VLAN ごとにマルチキャスト伝送フレームを複製する必要はありません。マルチキャスト TV VLAN の設定を定義するには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [Access Port Multicast TV VLAN] > [Port Multicast VLAN Membership] の順にクリックします。

ステップ 2 [Multicast TV VLAN] から VLAN を選択します。

ステップ 3 [Interface Type] からインターフェイスを選択します。

ステップ 4 [Candidate Access Ports] リストには、デバイスに設定されているすべてのアクセス ポートが含まれています。必要なポートを、[Member Access Ports] フィールドに移動します。

ステップ 5 [Apply] をクリックします。マルチキャスト TV VLAN 設定が変更され、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。

カスタマーポートマルチキャストTV VLAN

トリプル プレイ サービスでは、1 つのブロードバンド接続で次の 3 つのブロード バンド サービスをプロビジョニングします。

- 高速なインターネット アクセス
- ビデオ
- 音声

トリプル プレイ サービスはサービス プロバイダーのサブスクライバに対してプロビジョニングされ、サブスクライバはレイヤ 2 での分離が維持されます。

各サブスクライバには、CPE MUX ボックスがあります。MUX には、サブスクライバのデバイス（PC、電話機など）に接続されている複数のアクセス ポートと、アクセス デバイスに接続されている 1 つのネットワーク ポートがあります。

ボックスは、パケットの VLAN タグに基づいて、パケットをネットワーク ポートからサブスクライバのデバイスに転送します。各 VLAN は MUX アクセス ポートのいずれかにマッピングされています。

サブスクライバからサービス プロバイダー ネットワークへのパケットは、サービスの種類を区別するために、VLAN タグ付きフレームとして転送されます。つまり、各サービスの種類に対して一意の VLAN ID が CPE ボックスにあります。

サブスクライバからサービスプロバイダー ネットワークへのすべてのパケットは、顧客VLANとして設定されているサブスクライバの VLAN を使用してアクセス デバイスによりカプセル化されます（外部タグまたは S-VID）。ただし、マルチキャスト TV VLAN に関連付けられている TV 受信者からの IGMP スヌーピング メッセージは除きます。TV 受信者からも送信される VOD 情報は、その他の種類のトラフィックと同様にして送信されます。

ネットワーク ポートでパケットを受信したサービス プロバイダー ネットワークからサブスクライバへのパケットは、サービス プロバイダー ネットワークで二重タグ パケットとして送信されます。外部タグ（サービス タグまたは S タグ）は、次のようにして、2 種類の VLAN の 1 つを置き換えます。

- サブスクライバの VLAN（インターネットと IP フォンを含む）
- マルチキャスト TV VLAN

内部 VLAN（C タグ）は、サブスクライバのネットワークでの宛先を決定するために（CPE MUX により）使用されるタグです。

VLANへのCPE VLAN

CPE VLAN のマルチキャスト TV VLAN へのマッピング

サブスクライバの VLAN で CPE MUX をサポートするには、サブスクライバに、複数のビデオプロバイダー（各々が異なる外部 VLAN に割り当てられたもの）が必要となることがあります。CPE マルチキャスト VLAN（内部）は、マルチキャストプロバイダー（外部）VLAN にマッピングする必要があります。CPE VLAN をマルチキャスト VLAN にマッピングすると、IGMP スヌーピングに参加できます。

CPE VLAN をマッピングするには、次の手順を実行します。

手順

ステップ 1 [VLAN Management] > [Customer Port Multicast TV VLAN] > [CPE VLAN to VLAN] をクリックします。

ステップ 2 [Add] をクリックします。

ステップ 3 次のフィールドに入力します。

- [CPE VLAN]：CPE ボックスで定義した VLAN を入力します。
- [Multicast TV VLAN]：CPE VLAN にマッピングするマルチキャスト TV VLAN を選択します。

ステップ 4 [Apply] をクリックします。CPE VLAN マッピングが変更され、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。

ポートマルチキャストVLANメンバシップ

マルチキャスト VLAN が関連付けられているポートは、顧客ポートとして設定する必要があります（「インターフェイスの設定 （3 ページ）」を参照）。

ポートをマルチキャスト TV VLAN にマッピングするには、以下の手順を実行します。

手順

ステップ 1 [VLAN Management] > [Customer Port Multicast TV VLAN] > [Port Multicast VLAN Membership] の順にクリックします。

ステップ 2 [Multicast TV VLAN] から VLAN を選択します。

ステップ 3 [Interface Type] からインターフェイスを選択します。

ステップ 4 [Candidate Customer Ports] リストには、デバイスに設定されているすべてのアクセス ポートが含まれています。必要なポートを、[Member Customer Ports] フィールドに移動します。

ステップ 5 [Apply] をクリックします。新しい設定が変更され、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.

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。