有線ダイナミック PVLAN の設定

次のセクションでは、有線動的 PVLAN の設定について説明します。

有線ダイナミック PVLAN の制約事項

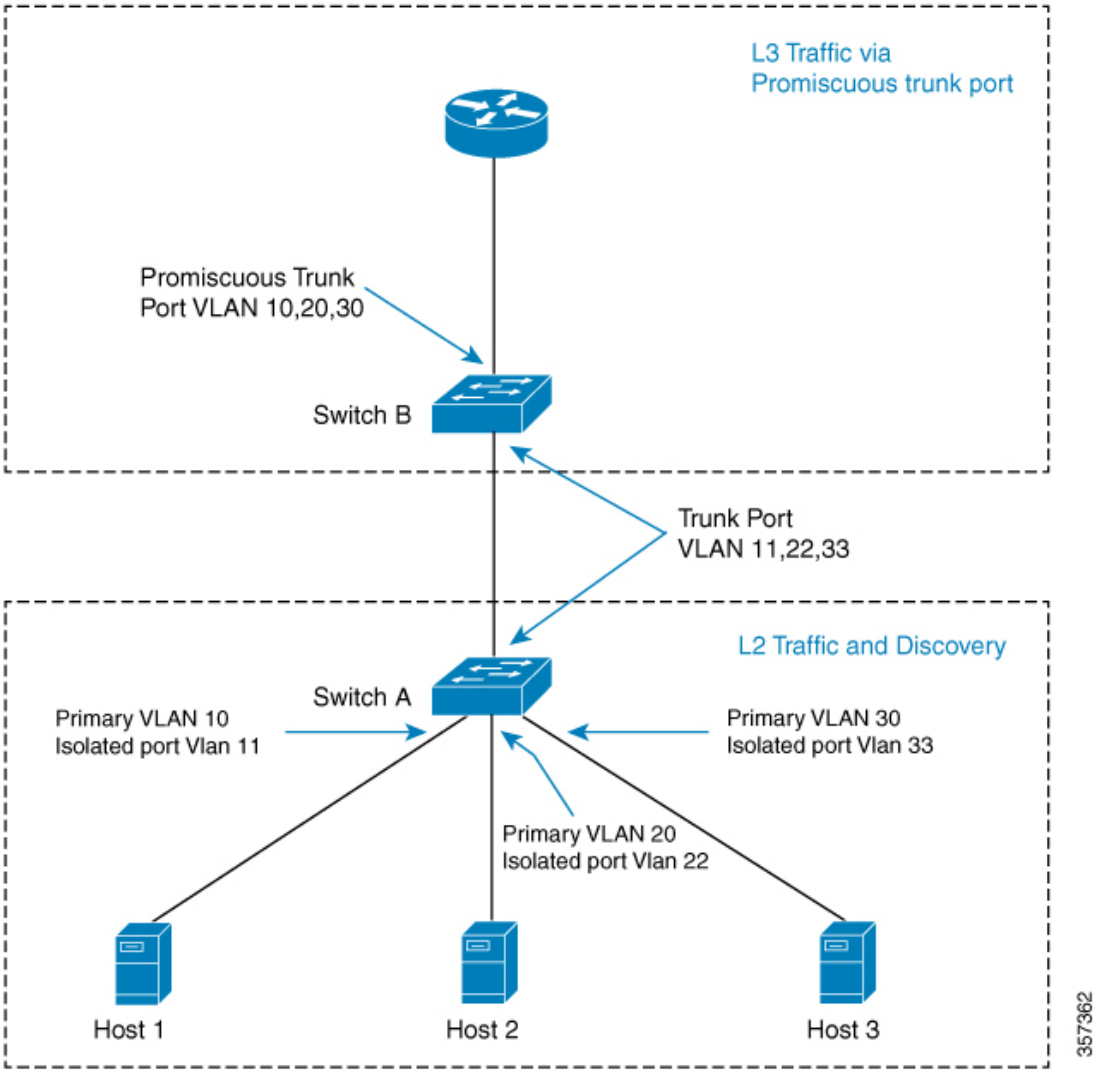
- 有線ダイナミック PVLAN では、ハイアベイラビリティはサポートされません。
- 音声 VLAN 設定は、この機能と共存できません。
- ローカル We b認証（LWA）および中央 Web 認証（CWA）は、この機能では使用できません。
- ダイナミック PVLANインターフェイステンプレートを使用するすべての有線クライアントは、データクライアントとしてプログラムされます。
- PVLAN テンプレートをサポートするのは、既存のアクセスまたは PVLAN ホストスイッチポートモードのインターフェイスのみです。
- ダイナミックテンプレートのサポートには、Identity Based Networking Services 2.0（IBNS 2.0）を使用する必要があります。

有線ダイナミック PVLAN に関する情報

有線ダイナミック PVLAN は、AAA 許可のあるプライベート VLAN を使用してクライアントを分離し、ゼロトラストを提供する機能です。これは、サブネット/VLAN 内のピアツーピア通信をブロックする方法です。ここで、クライアントは PVLAN に割り当てられ、1 つのポートに接続された有線クライアントをレイヤ 2 の他のすべてのポートから分離し、レイヤ 3 通信は無差別ポートを介して行われます。この機能では、ポイントツーポイントブロッキングを保

証するために、ポートインターフェイスごとに単一の有線データクライアントがサポートされます。

（注） 同じインターフェイス上の複数のクライアントからのトラフィックはブロックされません。



このトポロジでは、ホストはスイッチAに接続されており、スイッチの無差別トランクポートとのみ通信できます。PVLANは、中間スイッチを追加することで、複数のスイッチにまたがって拡張できます。上記のトポロジでスイッチ A とスイッチ B の間にスイッチ（スイッチ C）がある場合は、中間リンクにレイヤ 2 トランクポートを設定する必要があります。コミュニティ VLAN の場合、同じコミュニティ VLAN 内の他のホストでパケットを確認できます。

ホストがケーブルでスイッチポートに接続されている場合、そのホストは他のホストを検出できない独立 PVLAN に配置されます。その後、ホストは RADIUS サーバーによって認証されま

有線ダイナミック PVLAN の設定

す。もう 1 つのシナリオは、ポートがクローズモードになり、ポートが認証されていない場合、Extensible Authentication Protocol over LAN（EAPoL）パケットのみが許可される場合です。ポートが認証されると、そのポートは独立 VLAN に動的に配置されます。ホストは最初に RADIUS サーバで認証されるため、ホストのポートに適用されるダイナミック インターフェイス テンプレートの名前を送信します。このインターフェイステンプレートには、ポートで PVLAN プライマリ VLAN とセカンダリ VLAN を有効にするための設定が含まれています。テンプレートがホストに適用されると、スイッチポートモードが変更され、ポートがアクセスモードから PVLAN モードにフラップします。

（注） AAA 許可によって参照されるインターフェイステンプレートと同じ名前のものをスイッチで設定する必要があります。

インターフェイステンプレートが適用されると、スティッキータイマーで設定された時間だけポートは物理的にダウンし、再びアップします。RADIUS サーバーがインターフェイステンプレートを 2 回送信すると、変換が完了したため無視されます。その後、ポートは隔離されたままの PVLAN に割り当てられます。ホストは許可を完了し、準備完了状態になります。

access-session interface-template sticky timer *time* コマンドを使用して、インターフェイス テンプレート情報をポートから削除する前に保持するキープタイムを設定します。

有線ダイナミック PVLAN の設定

有線ダイナミック PVLAN を設定するには、ユーザーデバイス（上記のトポロジのスイッチ A）で次の手順を実行します。

始める前に

ユーザーデバイスで dot1x aaa が設定されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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。

有線ダイナミック PVLAN の設定

	コマンドまたはアクション	目的
ステップ 3	**vlan** *vlan-id* 例： `Device(config)# vlan 200`	（任意）VLAN コンフィギュレーション モードを開始して、独立 VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 4	**private-vlan isolated** 例： `Device(config-vlan)# private-vlan isolated`	VLAN を独立 VLAN として指定します。
ステップ 5	**exit** 例： `Device(config-vlan)# 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	**vlan** *vlan-id* 例： `Device(config)# vlan 100`	VLAN コンフィギュレーション モードを開始して、プライマリ VLAN となる VLAN を指定または作成します。VLAN ID の範囲は 2 ～ 1001 および 1006 ～ 4094 です。
ステップ 7	**private-vlan primary** 例： `Device(config-vlan)# private-vlan primary`	VLAN をプライマリ VLAN として指定します。
ステップ 8	**private-vlan association** [**add** | **remove**] *secondary_vlan_list* 例： `Device(config-vlan)# private-vlan association 200`	セカンダリ VLAN をプライマリ VLAN に関連付けます。単一のプライベート VLAN ID でも、またはハイフンで連結したプライベート VLAN ID でもかまいません。 • *secondary_vlan_list* パラメータには、スペースを含めないでください。カンマで区切った複数の項目を含めることができます。各項目として入力できるのは、単一のプライベート VLAN ID またはハイフンで連結したプライベート VLAN ID です。

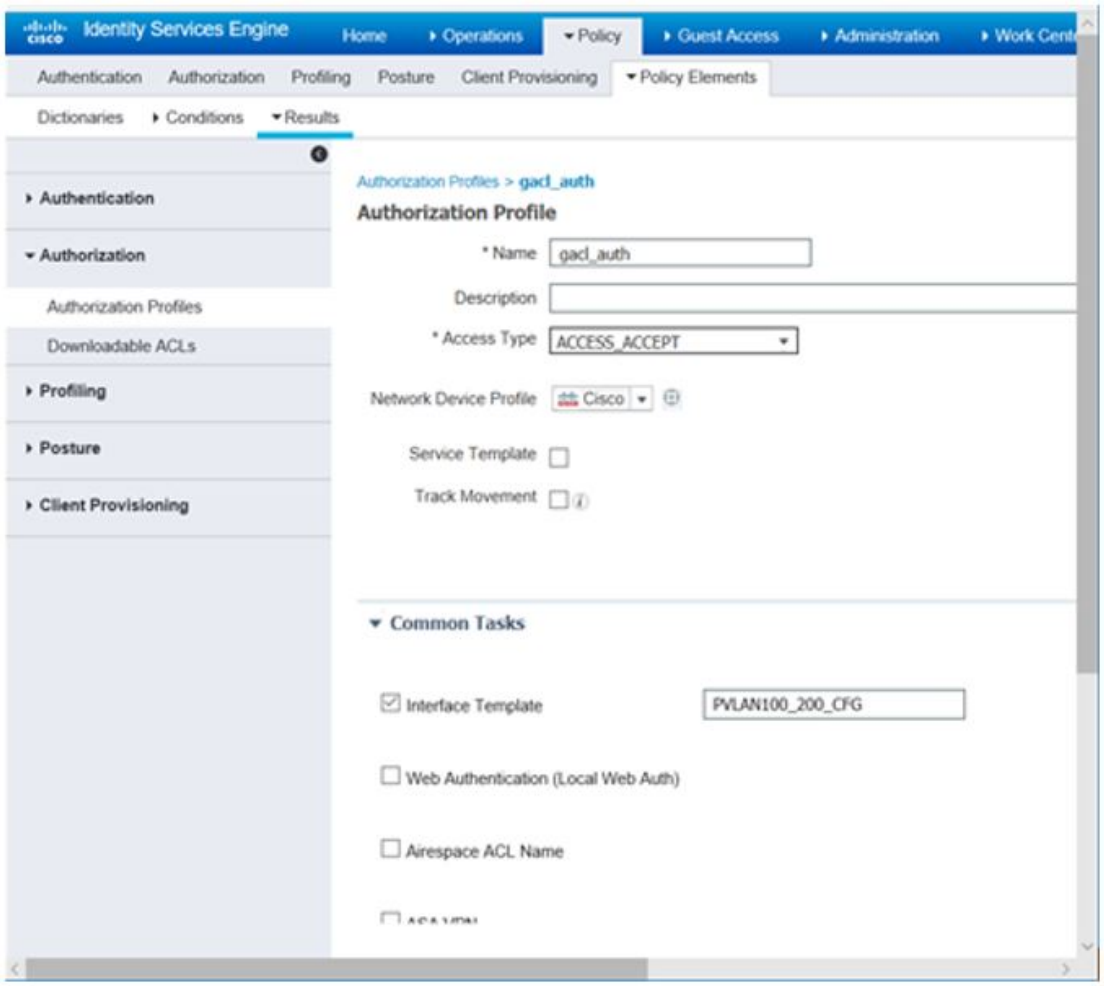
	コマンドまたはアクション	目的
		• *secondary_vlan_list* パラメータには複数のコミュニティ VLAN ID を含められますが、独立 VLAN ID は 1 つだけです。 • *secondary_vlan_list* を入力するか、または *secondary_vlan_list* で **add** キーワードを指定し、セカンダリ VLAN とプライマリ VLAN を関連付けます。 • セカンダリ VLAN とプライマリ VLAN 間の関連付けをクリアするには、*secondary_vlan_list* に **remove** キーワードを使用します。 • このコマンドは、VLAN コンフィギュレーション モードを終了するまで機能しません。
ステップ 9	**exit** 例： `Device(config-vlan)# 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 10	**template** *template-name* 例： `Device(config)# template PVLAN100_200_CFG`	ユーザーテンプレートを作成し、テンプレート 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	**switchport mode private-vlan host** 例： `Device(config-template)# switchport mode private-vlan host`	レイヤ 2 ポートを PVLAN ホストポートとしてテンプレートに設定します。
ステップ 12	**switchport private-vlan host-association** *primary_vlan_id secondary_vlan_id* 例： `Device(config-template)# switchport private-vlan host-association 100 200`	テンプレートの PVLAN とレイヤ 2 ポートの関連付けを設定します。

	コマンドまたはアクション	目的
ステップ 13	**exit** 例： `Device(config-template)# 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 14	**access-session interface-template sticky timer** *time* 例： `Device(config)# access-session interface-template sticky timer 60`	テンプレートの保持時間をグローバルに設定します。最後のクライアントが離れると、設定された保持時間の後にテンプレートがポートから削除されます。 （注） スティッキータイマーを60秒に設定することをお勧めします。
ステップ 15	**interface** *interface-id* 例： `Device(config)# interface GigabitEthernet1/0/1`	インターフェイス設定モードに入り、インターフェイスを指定します。
ステップ 16	**access-session interface-template sticky timer** *time* 例： `Device(config-if)# access-session interface-template sticky timer 60`	インターフェイス上のテンプレートの保持時間を設定します。最後のクライアントが離れると、設定された保持時間の後にテンプレートがポートから削除されます。 （注） スティッキータイマーを60秒に設定することをお勧めします。
ステップ 17	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

次のタスク

上記の手順の後、Identity Services Engine（ISE）またはその他の RADIUS サーバーを設定して、クライアントが正常に認証された後にクライアントのポートインターフェイスにテンプレートを割り当てます。

図 *1* : インターフェイステンプレートを割り当てるための *ISE* の設定



ISE を使用している場合、[Policy] > [Policy Elements] > [Authorization] > [Authorization Profile] ページの順にアクセスします。[Interface Template] チェックボックスをオンにして、クライアント インターフェイスに割り当てるテンプレートの名前を入力します。

別の RADIUS サーバーを使用している場合は、最初のクライアント認証が完了した後に、属性 **Cisco-AVpair="interface:template=name"** をスイッチにプッシュする必要があります。

有線ダイナミック PVLAN の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Bengaluru 17.5.1	有線ダイナミック PVLAN （ホワイトリスト P2P ブロッキング）	有線ダイナミック PVLAN 機能は、プライベート VLAN を使用してクライアントを分離し、ゼロトラストを提供します。これは、サブネット/VLAN 内のピアツーピア通信をブロックする方法です。クライアントは、ポートに接続された単一の有線クライアントを他のポートから分離する PVLAN に割り当てられます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/ に進みます。

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。