CHAPTER 13

VLAN の設定

この章では、有線 LAN に設定された VLAN を使って動作するようにアクセス ポイントを設定する方法について説明します。次の項では、VLAN をサポートするようにアクセス ポイントを設定する方法について説明します。

VLAN の概要

VLAN は、物理的または地理的な基準ではなく、機能、プロジェクト チーム、あるいはアプリケーション別に論理的にセグメント化したスイッチド ネットワークです。たとえば、特定の作業グループ チームが使用するワークステーションおよびサーバを、ネットワークへの物理的接続や他のチームと混ざり合っている可能性などにかかわらず、すべて同じ VLAN に接続できます。VLAN によるネットワークの再設定は、デバイスやケーブルを物理的に取り外したり移動したりするのではなく、ソフトウェアを使って行います。

VLAN は、定義されたスイッチのセット内に存在するブロードキャスト ドメインと考えることができます。VLAN は、1 つのブリッジング ドメインによって接続された、ホストかネットワーク機器（ブリッジやルータなど）のいずれかに該当する複数のエンド システムで構成されます。ブリッジング ドメインは、さまざまなネットワーク機器でサポートされています。たとえば LAN スイッチは、VLAN ごとに異なるグループを使用して、スイッチ間のブリッジング プロトコルを処理します。

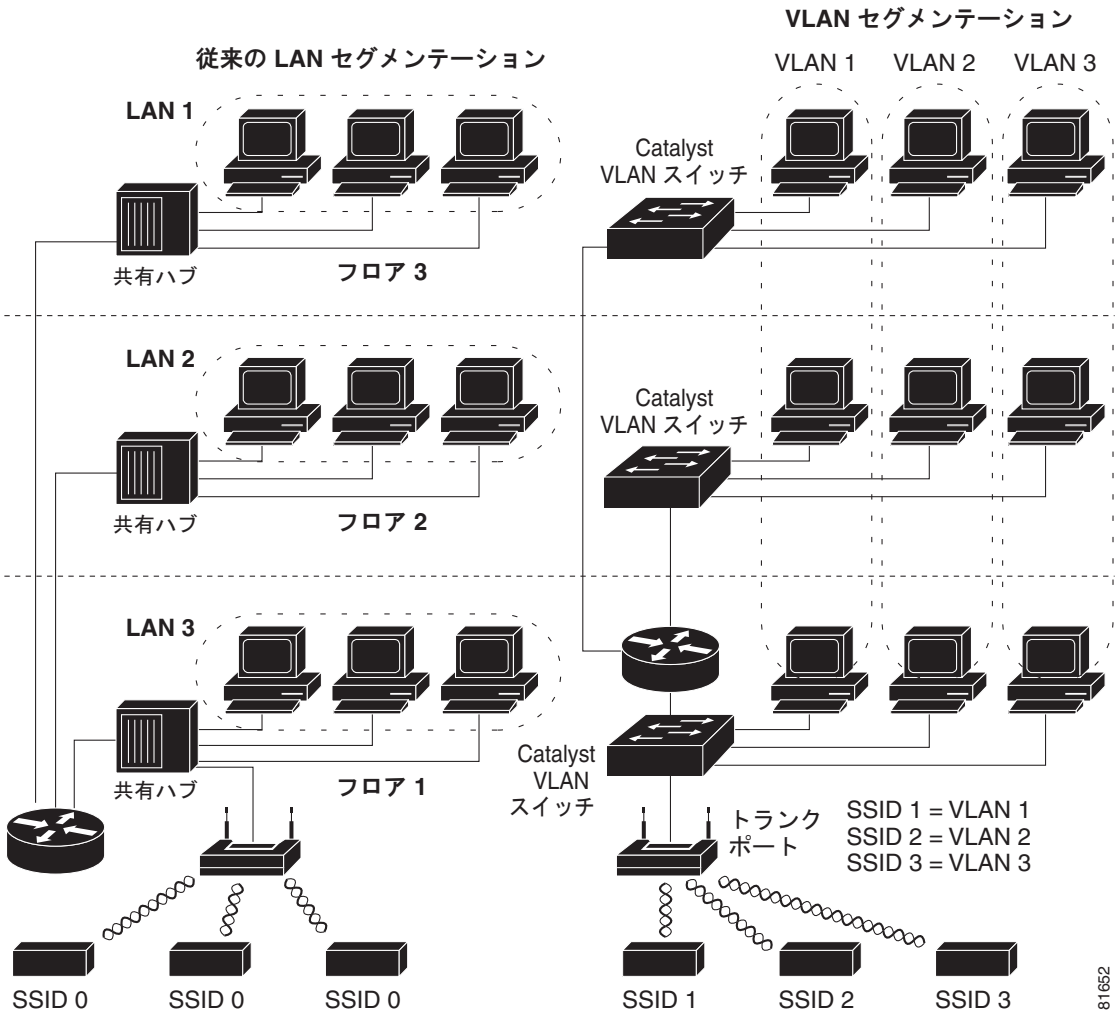
VLAN は、通常は LAN 設定のルータによって提供されるセグメンテーション サービスを提供します。VLAN はスケーラビリティ、セキュリティ、およびネットワーク管理に対応します。スイッチド LAN ネットワークを設計し構築する際は、いくつかの主要な問題を考慮する必要があります。

- LAN セグメンテーション
- セキュリティ
- ブロードキャスト制御
- パフォーマンス
- ネットワーク管理
- VLAN 間の通信

VLAN は、アクセス ポイントに IEEE 802.11Q タグ認識を追加することにより、無線 LAN に拡張することができます。異なる VLAN を宛先とするフレームは、Wired Equivalent Privacy（WEP）キーの異なる複数の Service Set Identifier（SSID; サービス セット ID）にアクセス ポイントによって無線送信されます。その VLAN と関連付けられたクライアントだけが、これらのパケットを受信できます。反対に、特定の VLAN と関連付けられたクライアントから送信されたパケットは、802.11Q タグが付加されてから、有線ネットワークに転送されます。

図 13-1 は、無線デバイスが接続された状態での、従来の物理的な LAN セグメンテーションと論理的な VLAN セグメンテーションとの違いを示しています。

図 13-1　無線デバイスを使用する LAN セグメンテーションと VLAN セグメンテーション



関連資料

VLAN の設計と設定に関する詳細は、次のマニュアルを参照してください。

- 『*Cisco IOS Switching Services Configuration Guide*』。次のリンクをクリックすると、この資料を参照できます。
  http://www.cisco.com/en/US/docs/ios/12_2/switch/configuration/guide/fswtch_c.html
- 『*Cisco Internetwork Design Guide*』。次のリンクをクリックすると、この資料を参照できます。
  http://www.cisco.com/en/US/docs/internetworking/design/guide/idg4.html
- 『*Cisco Internetworking Technology Handbook*』。次のリンクをクリックすると、この資料を参照できます。
  http://www.cisco.com/en/US/docs/internetworking/technology/handbook/ito_doc.html
- 『*Cisco Internetworking Troubleshooting Guide*』。次のリンクをクリックすると、この資料を参照できます。
  http://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1901.html

VLAN への無線デバイスの組み込み

VLAN の基本的な無線コンポーネントは、アクセス ポイントと、無線テクノロジーを使用してアクセス ポイントにアソシエートされるクライアントです。アクセス ポイントは、VLAN が設定されているネットワーク VLAN スイッチに、トランク ポートを介して物理的に接続されています。VLAN スイッチへの物理的な接続には、アクセス ポイントのイーサネット ポートが使用されます。

基本的に、特定の VLAN に接続するようにアクセス ポイントを設定する際に重要なのは、その VLAN を認識するように SSID を設定することです。VLAN は VLAN ID または名前によって識別されるため、アクセス ポイントの SSID が特定の VLAN ID または名前を認識するように設定された場合、VLAN との接続が確立されます。この接続が確立されると、同じ SSID を持つ、アソシエートされた無線クライアント デバイスは、このアクセス ポイントを介して VLAN にアクセスできます。VLAN は、有線ネットワークとのやり取りと同様に、クライアントとやり取りしてデータを処理します。アクセス ポイントには最大 16 の SSID を設定できるため、最大 16 の VLAN をサポートできます。1 つの VLAN には、1 つの SSID だけを割り当てることができます。

VLAN 機能を使用すると、より効率的かつ柔軟に無線デバイスを展開できます。たとえば、ネットワーク アクセスの方法や与えられている権限が多種多様にわたる複数のユーザの個別要件に、1 つのアクセス ポイントで対応できるようになります。VLAN 機能を使用しない場合は、許可されているアクセスの方法や与えられた権限に基づいて多様なユーザに対応するために、複数のアクセス ポイントを設置する必要があります。

無線 VLAN の配備には、2 つの一般的な戦略があります。

- ユーザ グループによるセグメンテーション：無線 LAN のユーザ コミュニティをセグメント化し、各ユーザ グループに異なるセキュリティ ポリシーを適用できます。たとえば、企業環境で、正社員用、パートタイム従業員用、およびゲスト アクセス用の 3 つの有線および無線 VLAN を構築することが可能です。
- デバイス タイプによるセグメンテーション：無線 LAN をセグメント化して、セキュリティ機能の異なる複数のデバイスがネットワークに接続できるようにします。たとえば、無線ユーザは静的 WEP だけをサポートするハンドヘルド デバイスを使用する場合や、動的 WEP を使用する高度なデバイスを使用している場合があります。これらのデバイスをグループ化して、個別の VLAN として切り離すことができます。

（注）　リピータ アクセス ポイントには複数の VLAN を設定できません。リピータ アクセス ポイントはネイティブ VLAN だけをサポートします。

VLAN の設定

次の項では、アクセス ポイントに VLAN を設定する方法について説明します。

- 「VLAN の設定」（P.13-5）
- 「VLAN への名前の割り当て」（P.13-6）
- 「Remote Authentication Dial-In User Service（RADIUS）サーバを使用した VLAN へのユーザの割り当て」（P.13-7）
- 「アクセス ポイントに設定された VLAN の表示」（P.13-8）

VLAN の設定

VLAN をサポートするようにアクセス ポイントを設定するプロセスは、次の 3 つの手順で行います。

1. 無線ポートとイーサネット ポートでの VLAN の有効化
2. SSID の VLAN への割り当て
3. 認証設定の SSID への割り当て

この項では、SSID を VLAN に割り当てる方法、およびアクセス ポイントの無線ポートとイーサネット ポートで VLAN を有効にする方法を説明します。SSID に認証タイプを割り当てる手順の詳細は、第 11 章「認証タイプの設定」を参照してください。その他の設定を SSID に割り当てる方法については、第 7 章「複数の SSID の設定」を参照してください。

アクセス ポイントには最大 16 の SSID を設定できるため、LAN に設定される VLAN は、最大 16 までサポートできます。

特権 EXEC モードから、次の手順に従って VLAN に SSID を割り当て、アクセス ポイントの無線ポートとイーサネット ポートで VLAN を有効にします。

	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 dot11radio 0** | **1**	無線インターフェイス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	**ssid** *ssid-string*	SSID を作成し、新しい SSID の SSID コンフィギュレーション モードを入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。 **（注）** 各 SSID に認証タイプを設定する場合は、**ssid** コマンドの認証オプションを使用します。認証タイプの設定方法については、第 11 章「認証タイプの設定」を参照してください。
ステップ 4	**vlan** *vlan-id*	（任意）ネットワーク上の VLAN に SSID を割り当てます。この SSID を使用してアソシエートするクライアント デバイスは、この VLAN にグループ化されます。VLAN ID を 1 ～ 4095 の範囲で入力します。1 つの VLAN には、1 つの SSID だけを割り当てることができます。 **ヒント** ネットワークで VLAN 名を使用している場合、アクセス ポイントの VLAN にも名前を割り当てることができます。手順については、「VLAN への名前の割り当て」（P.13-6）を参照してください。
ステップ 5	**exit**	無線インターフェイスのインターフェイス コンフィギュレーション モードに戻ります。
ステップ 6	**interface dot11radio 0.x** | **1.x**	無線 VLAN サブインターフェイス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 7	**encapsulation dot1q** *vlan-id* [**native**]	無線インターフェイスで VLAN を有効にします。 （任意）VLAN をネイティブ VLAN に指定します。多くのネットワークではネイティブ VLAN は VLAN 1 です。
ステップ 8	**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 9	**interface fastEthernet0.x**	イーサネット VLAN サブインターフェイス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。

	コマンド	目的
ステップ 10	**encapsulation dot1q** *vlan-id* [**native**]	イーサネット インターフェイスで VLAN を有効にします。 （任意）VLAN をネイティブ VLAN に指定します。多くのネットワークではネイティブ VLAN は VLAN 1 です。
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**	（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。

次の例は、次の方法を示します。

- SSID の名前の指定
- SSID の VLAN への割り当て
- 無線ポートとイーサネット ポートでのネイティブ VLAN として VLAN の有効化

```
ap1200# configure terminal
ap1200(config)# interface dot11radio0
ap1200(config-if)# ssid batman
ap1200(config-ssid)# vlan 1
ap1200(config-ssid)# exit
ap1200(config)# interface dot11radio0.1
ap1200(config-subif)# encapsulation dot1q 1 native
ap1200(config-subif)# exit
ap1200(config)# interface fastEthernet0.1
ap1200(config-subif)# encapsulation dot1q 1 native
ap1200(config-subif)# exit
ap1200(config)# end
```

VLAN への名前の割り当て

VLAN に ID 番号と名前を割り当てることができます。VLAN 名には、最大 32 文字の ASCII 文字を使用できます。アクセス ポイントでは、各 VLAN 名と ID のペアが表に格納されます。

VLAN 名を使用する際のガイドライン

VLAN 名を使用する際は、次のガイドラインに留意してください。

- VLAN 名の VLAN ID へのマッピングは各アクセス ポイントだけで使用されるため、同じ VLAN 名をネットワーク内の別の VLAN ID に割り当てることができます。

（注） 無線 LAN のクライアントがシームレスなローミングを必要とする場合には、すべてのアクセス ポイントで同じ VLAN ID に対して同じ VLAN 名を割り当てるか、または名前を使用せずに VLAN ID だけを使用することを推奨します。

- ID はアクセス ポイントに設定されているすべての VLAN に必要ですが、VLAN 名はオプションです。
- VLAN 名には、最大 32 文字の ASCII 文字を使用できます。ただし、VLAN 名を 1 ～ 4095 の数字にすることはできません。たとえば、*vlan4095* は VLAN 名として有効ですが、*4095* は無効です。アクセス ポイントでは、1 ～ 4095 の数字は VLAN ID 用に予約されています。

VLAN 名の作成

特権 EXEC モードから、次の手順に従って VLAN に名前を割り当てます。

	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	**dot11 vlan-name** *name* **vlan** *vlan-id*	VLAN 名を VLAN ID に割り当てます。名前には、最大 32 文字の ASCII 文字を使用できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**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。

VLAN から名前を削除する場合は、コマンドの **no** 形式を使用します。アクセス ポイントに設定されている VLAN 名と ID の組み合わせをすべて表示するには、特権 EXEC コマンド **show dot11 vlan-name** を使用します。

Remote Authentication Dial-In User Service（RADIUS）サーバを使用した VLAN へのユーザの割り当て

ユーザまたはユーザ グループがネットワークから認証を受けたときに、特定の VLAN に割り当てるように RADIUS 認証サーバを設定できます。

（注） WPA 情報エレメントでアドバタイズされる（さらに 802.11 でのアソシエーション中に決定される）ユニキャストとマルチキャストの暗号スイートは、明示的に割り当てられた VLAN でサポートされている暗号スイートと一致しない可能性があります。RADIUS サーバにより、以前決定された暗号スイートとは別の暗号スイートを使用する、新規の VLAN ID が割り当てられた場合、アクセス ポイントとクライアントは、この新たな暗号スイートに切り替えることができなくなります。現在、WPA プロトコルと Cisco Centralized Key Management（CCKM）プロトコルでは、最初の 802.11 暗号ネゴシエーション フェーズ以降での暗号スイートの変更は認められていません。このような場合、クライアント デバイスと無線 LAN とのアソシエーションが解除されてしまいます。

VLAN マッピングのプロセスは、次の手順で行われます。

1. クライアント デバイスはアクセス ポイントに設定された任意の SSID を使用して、アクセス ポイントにアソシエートします。
2. クライアントは、RADIUS 認証を開始します。
3. クライアントの認証に成功すると、RADIUS サーバはクライアントを特定の VLAN にマッピングします。この場合、クライアントがアクセス ポイントで使用している SSID に定義された VLAN マッピングは無視されます。サーバがクライアントの VLAN 属性を返さない場合、クライアントはアクセス ポイントでローカルにマッピングされた SSID の指定する VLAN に割り当てられます。

これらは VLAN ID の割り当てに使用される RADIUS ユーザ属性です。各属性はグループ化された関係を特定するため、1 ～ 31 の範囲の共通のタグ値を保有していなければなりません。

- IETF 64（トンネル タイプ）：属性を **VLAN** に設定
- IETF 65（トンネル メディア タイプ）：属性を **802** に設定
- IETF 81（トンネル プライベート グループ ID）：属性を *vlan-id* に設定

アクセス ポイントに設定された VLAN の表示

特権 EXEC モードで、**show vlan** コマンドを使用してアクセス ポイントがサポートする VLAN を表示します。次に、**show vlan** コマンドの出力例を示します。

```
Virtual LAN ID:  1 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  Dot11Radio0
FastEthernet0
Virtual-Dot11Radio0

 This is configured as native Vlan for the following interface(s) :
Dot11Radio0
FastEthernet0
Virtual-Dot11Radio0

   Protocols Configured:   Address:              Received:        Transmitted:
        Bridging        Bridge Group 1             201688                  0
        Bridging        Bridge Group 1             201688                  0
        Bridging        Bridge Group 1             201688                  0

Virtual LAN ID:  2 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  Dot11Radio0.2
FastEthernet0.2
Virtual-Dot11Radio0.2

   Protocols Configured:   Address:              Received:        Transmitted:
```

VLAN の設定例

次の例は、VLAN を使用して、大学の構内で無線デバイスを管理する方法を示しています。この例では、有線ネットワークに設定された VLAN を介した 3 つのアクセス レベルが用意されています。

- 管理アクセス：最高のアクセス レベル。ユーザはすべての内部ドライブとファイル、学部のデータベース、トップ レベルの財務情報、およびその他の機密情報にアクセスできます。管理ユーザは、Cisco LEAP を使用した認証が要求されます。
- 教職員アクセス：中級のアクセス レベル。ユーザは学内のイントラネットとインターネット、内部ファイル、および学生のデータベースにアクセスし、人事や給与、その他の教職員関連の資料といった内部情報を参照できます。教職員ユーザは、Cisco LEAP を使用した認証が要求されます。
- 学生アクセス：最も低いアクセス レベル。ユーザは学内のイントラネットおよびインターネットへのアクセス、授業日程の入手、成績の参照、面会の約束など学生に関係のある活動を実行できます。学生は静的 WEP を使用してネットワークに接続することが許可されます。

このシナリオでは、各アクセス レベルに 1 つずつ、少なくとも 3 つの VLAN 接続が必要です。アクセス ポイントは最大 16 の SSID を処理できるため、表 13-1 に示す基本設計を使用できます。

表 13-1　アクセス レベルの SSID と VLAN の割り当て

アクセス レベル	SSID	VLAN ID
管理	boss	01
教職員	teach	02
学生	learn	03

マネージャは SSID boss を使用するように無線クライアント アダプタを設定し、教職員メンバーは SSID teach を使用するようにクライアントを設定し、学生は無線クライアント アダプタを SSID learn を使用するように設定します。これらのクライアントをアクセス ポイントにアソシエートすると、自動的に適切な VLAN を選択します。

この例では、VLAN をサポートするために次の手順を実行します。

1. LAN スイッチのいずれかで、上記の VLAN を設定するか、VLAN 設定を確認します。
2. アクセス ポイントで、各 VLAN に SSID を割り当てます。
3. 各 SSID に認証タイプを割り当てます。
4. アクセス ポイント上の fastethernet および dot11radio インターフェイスの両方に対し、VLAN 1 となる管理 VLAN を設定します。この VLAN は、ネイティブ VLAN にする必要があります。
5. アクセス ポイントの fastethernet および dot11radio インターフェイスの両方に、VLAN 2 と VLAN 3 を設定します。
6. クライアント デバイスを設定します。

表 13-2 に、この例での 3 つの VLAN の設定に必要な各コマンドを示します。

表 13-2　VLAN のコンフィギュレーション コマンドの例

VLAN 1 の設定	VLAN 2 の設定	VLAN 3 の設定
ap1200# **configure terminal** ap1200(config)# **interface dot11radio 0** ap1200(config-if)# **ssid boss** ap1200(config-ssid)# **vlan 01** ap1200(config-ssid)# **end**	ap1200# **configure terminal** ap1200(config)# **interface dot11radio 0** ap1200(config-if)# **ssid teach** ap1200(config-ssid)# **vlan 02** ap1200(config-ssid)# **end**	ap1200# **configure terminal** ap1200(config)# **interface dot11radio 0** ap1200(config-if)# **ssid learn** ap1200(config-ssid)# **vlan 03** ap1200(config-ssid)# **end**
ap1200 **configure terminal** ap1200(config) **interface FastEthernet0.1** ap1200(config-subif) **encapsulation dot1Q 1 native** ap1200(config-subif) **exit**	ap1200(config) **interface FastEthernet0.2** ap1200(config-subif) **encapsulation dot1Q 2** ap1200(config-subif) **bridge-group 2** ap1200(config-subif) **exit**	ap1200(config) **interface FastEthernet0.3** ap1200(config-subif) **encapsulation dot1Q 3** ap1200(config-subif) **bridge-group 3** ap1200(config-subif) **exit**
ap1200(config)# **interface Dot11Radio 0.1** ap1200(config-subif)# **encapsulation dot1Q 1 native** ap1200(config-subif)# **exit** **（注）** ネイティブ VLAN として設定したサブインターフェイスには、ブリッジ グループを設定する必要はありません。このブリッジ グループは、ネイティブ サブインターフェイスに自動的に移動し、無線インターフェイスとイーサネット インターフェイスの両方を表す BVI 1 とのリンクを維持します。	ap1200(config) **interface Dot11Radio 0.2** ap1200(config-subif) **encapsulation dot1Q 2** ap1200(config-subif) **bridge-group 2** ap1200(config-subif) **exit**	ap1200(config) **interface Dot11Radio 0.3** ap1200(config-subif) **encapsulation dot1Q 3** ap1200(config-subif) **bridge-group 3** ap1200(config-subif) **exit**

表 13-3 は、表 13-2 のコンフィギュレーション コマンドの結果を示しています。アクセス ポイントで実行コンフィギュレーションを表示するには、**show running** コマンドを使用します。

表 13-3　コンフィギュレーション コマンド例の結果

VLAN 1 インターフェイス	VLAN 2 インターフェイス	VLAN 3 インターフェイス
interface Dot11Radio**0**.1 encapsulation dot1Q 1 native no ip route-cache no cdp enable bridge-group 1 bridge-group 1 subscriber-loop-control bridge-group 1 block-unknown-source no bridge-group 1 source-learning no bridge-group 1 unicast-flooding bridge-group 1 spanning-disabled	interface Dot11Radio**0**.2 encapsulation dot1Q 2 no ip route-cache no cdp enable bridge-group 2 bridge-group 2 subscriber-loop-control bridge-group 2 block-unknown-source no bridge-group 2 source-learning no bridge-group 2 unicast-flooding bridge-group 2 spanning-disabled	interface Dot11Radio**0**.3 encapsulation dot1Q 3 no ip route-cache bridge-group 3 bridge-group 3 subscriber-loop-control bridge-group 3 block-unknown-source no bridge-group 3 source-learning no bridge-group 3 unicast-flooding bridge-group 3 spanning-disabled
interface FastEthernet0.1 encapsulation dot1Q 1 native no ip route-cache bridge-group 1 no bridge-group 1 source-learning bridge-group 1 spanning-disabled	interface FastEthernet0.2 encapsulation dot1Q 2 no ip route-cache bridge-group 2 no bridge-group 2 source-learning bridge-group 2 spanning-disabled	interface FastEthernet0.3 encapsulation dot1Q 3 no ip route-cache bridge-group 3 no bridge-group 3 source-learning bridge-group 3 spanning-disabled

無線インターフェイスのブリッジ グループを設定する場合、次のコマンドが自動的に設定されることに注意してください。

```
bridge-group 2 subscriber-loop-control
bridge-group 2 block-unknown-source
no bridge-group 2 source-learning
no bridge-group 2 unicast-flooding
bridge-group 2 spanning-disabled
```

ファスト イーサネット インターフェイスのブリッジ グループを設定する場合、次のコマンドが自動的に設定されることに注意してください。

```
no bridge-group 2 source-learning
bridge-group 2 spanning-disabled
```