



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 \(P.14-1\)](#)
- [VLAN の設定 \(P.14-4\)](#)
- [VLAN の設定例 \(P.14-10\)](#)

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、ネットワークへの物理的な接続や他のチームとの混在の可能性にかかわらず、特定のワークグループ チームが使用するすべてのワークステーションとサーバを同じ VLAN に接続できます。VLAN によるネットワークの再設定は、デバイスやワイヤを物理的に取り外したり移動したりするのではなく、ソフトウェアを通じて行うことができます。

VLAN は、定義されたスイッチ セット内にあ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複数のエンド システム、つまりホストまたはネットワーク機器（ブリッジやルータなど）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。

- VLAN 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 802.1Q 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。

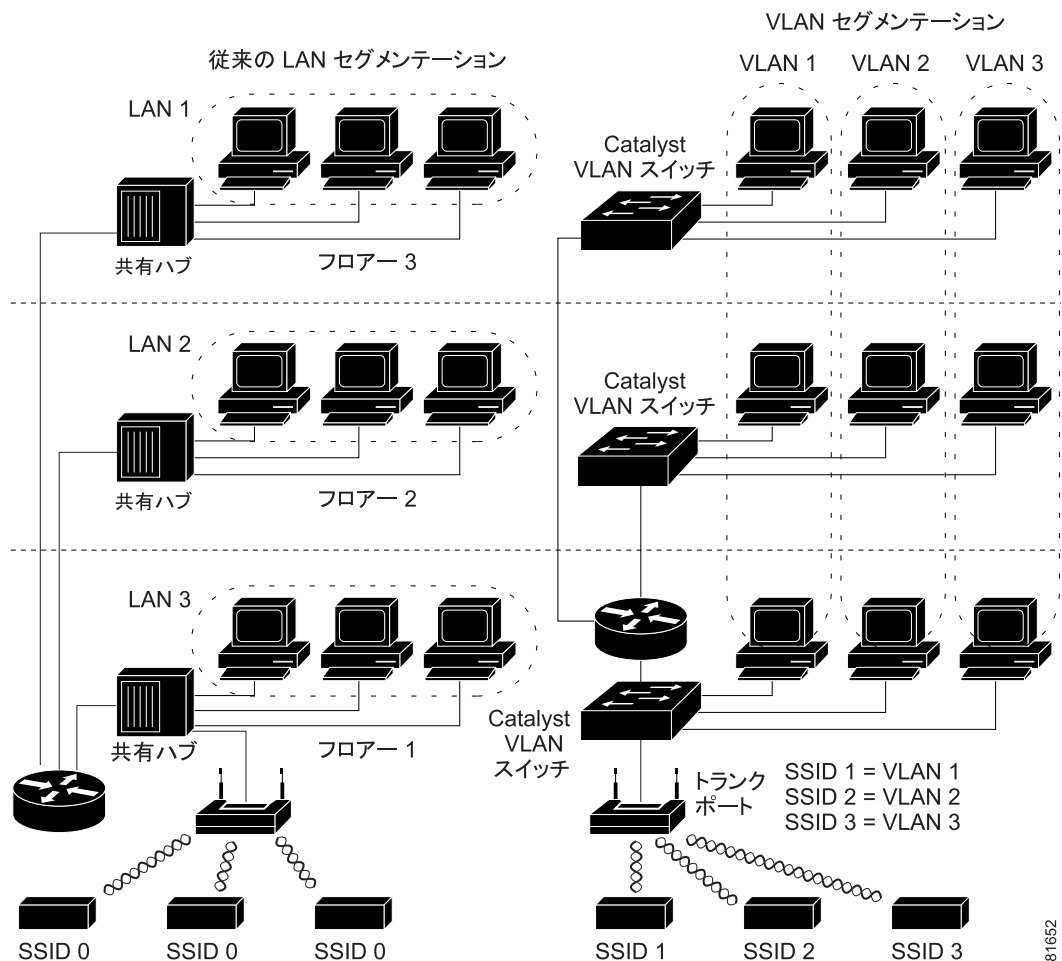
アクセスポイントのファーストイーサネットインターフェイスで 802.1q が設定されていると、アクセスポイントでは VLAN 1 が定義されていない場合でも、常に VLAN1 にキープアライブが送信されます。この結果、イーサネットスイッチはアクセスポイントに接続し、警告メッセージを生成します。アクセスポイントとスイッチのいずれにも機能の消失はありません。ただし、スイッチログには無意味なメッセージが記載され、これによって重要メッセージがラップされたり、表示されなくなることがあります。

特定のアクセスポイント上のすべての SSID がモビリティネットワークにアソシエートされている場合は、この動作によって問題が発生します。すべての SSID がモビリティネットワークにアソシエートされている場合は、アクセスポイントが接続されているイーサネットスイッチポートをアクセスポートとして設定できます。通常、アクセスポートはアクセスポイントのネイティブの VLAN に割り当てられ、これは VLAN1 である必要はありません。これによってイーサネットスイッチで 802.1q タグの付けられたトラフィックがアクセスポイントから送信されていることを示す警告メッセージが生成されます。

スイッチ上の過剰メッセージは、キープアライブ機能を無効にすることで解消できます。

図 14-1 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 14-1 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



81652

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、このマニュアルを参照できます。
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/switch_c/index.htm
- 『Cisco Internetwork Design Guide』。次のリンクをクリックすると、このマニュアルを参照できます。
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/index.htm>
- 『Cisco Internetworking Technology Handbook』。次のリンクをクリックすると、このマニュアルを参照できます。
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/index.htm
- 『Cisco Internetworking Troubleshooting Guide』。次のリンクをクリックすると、このマニュアルを参照できます。
http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/index.htm

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のポイントは、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ので、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 を設定できるので、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 台のアクセス 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 \(P.14-4\)](#)
- [VLAN への名前の割り当て \(P.14-6\)](#)
- [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 \(P.14-7\)](#)
- [アクセス ポイントに設定された VLAN の表示 \(P.14-9\)](#)

VLAN の設定



(注)

アクセス ポイント上で VLAN を設定する場合は、ネイティブ VLAN を VLAN1 にする必要があります。単一アーキテクチャでは、アクセス ポイントのイーサネット インターフェイス ネイティブ VLAN で確立された IP-Generic Routing Encapsulation (IP-GRE; IP 総称ルーティング カプセル化) トンネルによって、アクセス ポイントが受信するクライアント トラフィックがトンネリングされます。IP-GRE トンネルがあるために、別のスイッチ ポートを VLAN1 として設定できるユーザが発生します。この設定の誤りによってスイッチ ポートでエラーが発生します。

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。SSID にその他の設定を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	<code>configure terminal</code>	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	<code>interface dot11radio 0 1</code>	無線インターフェイスのインターフェイス設定モードを開始します。

	コマンド	目的
ステップ 3	ssid <i>ssid-string</i>	<p>SSID を作成し、新しい SSID の SSID 設定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。</p> <p>SSID には、最大 32 文字の英数字を使用でき、大文字と小文字が区別されます。</p> <p>先頭の文字に次の文字は使用できません。</p> <ul style="list-style-type: none"> • 感嘆符 (!) • ポンド記号 (#) • セミコロン (;) <p>次の文字は無効とされ、SSID に使用することはできません。</p> <ul style="list-style-type: none"> • プラス記号 (+) • 閉じ大カッコ (]) • スラッシュ (/) • 引用符 (") • タブ • 末尾のスペース <p> (注) 各 SSID に認証タイプを設定する場合は、コマンド <code>ssid</code> 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。</p>
ステップ 4	vlan <i>vlan-id</i>	<p>(オプション) 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。</p> <p> 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」の項 (P.14-6) を参照してください。</p>
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設定モードに戻ります。
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設定モードを開始します。
ステップ 7	encapsulation dot1q <i>vlan-id</i> [native]	無線インターフェイスで VLAN を有効にします。 (オプション) 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設定モードを開始します。
ステップ 10	encapsulation dot1q <i>vlan-id</i> [native]	イーサネット インターフェイスで VLAN を有効にします。 (オプション) 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。

	コマンド	目的
ステップ 11	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 12	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

次の例は、以下の方法を示します。

- 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 には数値による ID 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 名と VLAN ID の組み合わせは各アクセス ポイントでのみ使用されるため、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お勧めします。

- 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、1 ~ 4095 の数字を VLAN 名にすることはできません。たとえば、`vlan4095` は有効な VLAN 名ですが、`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	<code>configure terminal</code>	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	<code>dot11 vlan-name name vlan vlan-id</code>	VLAN ID に VLAN 名を割り当てます。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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

VLAN から名前を削除する場合は、コマンドの **no** フォームを使用します。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 (および 802.11 のアソシエーションの際に決定) 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ことがあります。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が正常に完了すると、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 マッピングにかかわらず、RADIUS サーバによってクライアントが特定の VLAN にマッピングされます。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** に設定します。
- IETF 65 (トンネル メディア タイプ) : 属性を **802** に設定します。
- IETF 81 (トンネル プライベート グループ ID) : 属性を *vlan-id* に設定します。

RADIUS サーバを使用したダイナミック モビリティ グループの割り当て

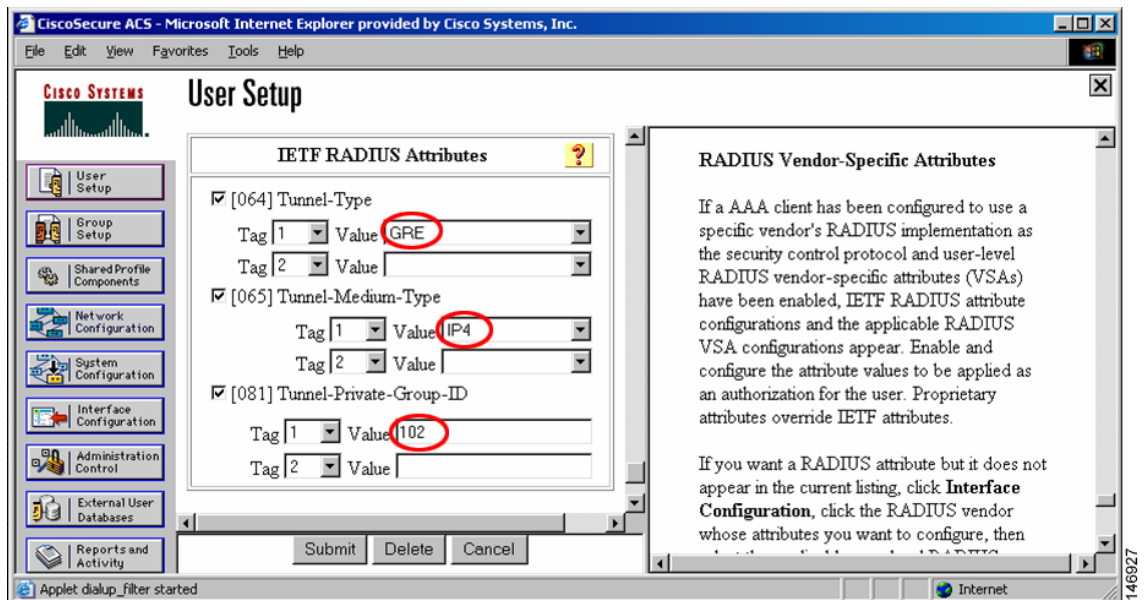
RADIUS サーバでは、モビリティ グループがユーザまたはユーザ グループに割り当てられるように設定できます。これによって、アクセス ポイントで複数の SSID を設定する必要が解消されます。代わりに、各アクセス ポイントに 1 つだけ SSID を設定すれば済みます。

ユーザが SSID にアソシエートされると、アクセス ポイントはそのログイン情報を WLSM に転送し、WLSM はさらにこの情報を RADIUS サーバに転送します。ログイン情報に基づいて、RADIUS サーバはユーザを適切なモビリティ グループに割り当て、そのクレデンシャルで応答を送信します。

ダイナミック モビリティ グループの割り当てを有効にするには、RADIUS サーバで次の属性を設定する必要があります。

- Tunnel-Type (64)
- Tunnel-Medium-Type(65)
- Tunnel-Private-Group-ID (81)

図 14-2 ダイナミック モビリティ グループの割り当て



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、シスコ Light Extensible Authentication Protocol (LEAP; 拡張認証プロトコル) を使用した認証が要求されます。
- **教授アクセス**：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、その他の教授関連の資料といった内部情報にアクセスできます。教員ユーザは、シスコ 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、授業日程と成績の入手、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 ポイントは最大で 16 個の SSID を処理できるため、表 14-1 に示す基本設計を使用できます。

表 14-1 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
教授	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、教授メンバーは 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 ポイント上のファースト イーサネット インターフェイスと dot11radio インターフェイスの両方で、管理 VLAN となる VLAN 1 を設定します。この VLAN は、ネイティブ VLAN にします。
5. アクセス ポイントのファースト イーサネット インターフェイスと dot11radio インターフェイスの両方で、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 14-2 は、この例の 3 つの VLAN の設定に必要な各コマンドを示しています。

表 14-2 VLAN の設定コマンドの例


VLAN 1 の設定	VLAN 2 の設定	VLAN 3 の設定
<pre>ap1200# configure terminal ap1200(config)# interface dot11radio 0 ap1200(config-if)# ssid boss ap1200(config-ssid)# vlan 01 ap1200(config-ssid)# end</pre>	<pre>ap1200# configure terminal ap1200(config)# interface dot11radio 0 ap1200(config-if)# ssid teach ap1200(config-ssid)# vlan 02 ap1200(config-ssid)# end</pre>	<pre>ap1200# configure terminal ap1200(config)# interface dot11radio 0 ap1200(config-if)# ssid learn ap1200(config-ssid)# vlan 03 ap1200(config-ssid)# end</pre>
<pre>ap1200 configure terminal ap1200(config) interface FastEthernet0.1 ap1200(config-subif) encapsulation dot1Q 1 native ap1200(config-subif) exit</pre>	<pre>ap1200(config) interface FastEthernet0.2 ap1200(config-subif) encapsulation dot1Q 2 ap1200(config-subif) bridge-group 2 ap1200(config-subif) exit</pre>	<pre>ap1200(config) interface FastEthernet0.3 ap1200(config-subif) encapsulation dot1Q 3 ap1200(config-subif) bridge-group 3 ap1200(config-subif) exit</pre>
<pre>ap1200(config)# interface Dot11Radio 0.1 ap1200(config-subif)# encapsulation dot1Q 1 native ap1200(config-subif)# exit</pre>	<pre>ap1200(config) interface Dot11Radio 0.2 ap1200(config-subif) encapsulation dot1Q 2 ap1200(config-subif) bridge-group 2 ap1200(config-subif) exit</pre>	<pre>ap1200(config) interface Dot11Radio 0.3 ap1200(config-subif) encapsulation dot1Q 3 ap1200(config-subif) bridge-group 3 ap1200(config-subif) exit</pre>
 <p>(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。</p>		

表 14-3 は、表 14-2 の設定コマンドの結果を示しています。アクセス ポイントで実行中の設定を表示するには、**show running** コマンドを使用します。

表 14-3 設定コマンド例の結果

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
<pre>interface Dot11Radio0.1 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</pre>	<pre>interface Dot11Radio0.2 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</pre>	<pre>interface Dot11Radio0.3 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</pre>
<pre>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</pre>	<pre>interface FastEthernet0.2 encapsulation dot1Q 2 no ip route-cache bridge-group 2 no bridge-group 2 source-learning bridge-group 2 spanning-disabled</pre>	<pre>interface FastEthernet0.3 encapsulation dot1Q 3 no ip route-cache bridge-group 3 no bridge-group 3 source-learning bridge-group 3 spanning-disabled</pre>

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
```