

Cisco Aironet ワイヤレス装置との VLAN の併用

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[表記法](#)

[VLAN](#)

[ネイティブ VLAN の意味](#)

[アクセス ポイント上の VLAN](#)

[アクセス ポイントの概念](#)

[アクセス ポイントの設定](#)

[ブリッジ上の VLAN](#)

[ブリッジの概念](#)

[ブリッジの設定](#)

[RADIUS サーバを使用した VLAN へのユーザの割り当て](#)

[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](#)

[アクセス ポイントとブリッジでのブリッジ グループの設定](#)

[Integrated Routing and Bridging \(IRB \)](#)

[関連スイッチとの相互対話](#)

[スイッチの設定 : Catalyst OS](#)

[スイッチの設定 : IOSベースのCatalystスイッチ](#)

[スイッチの設定 : Catalyst 2900XL/3500XL](#)

[確認](#)

[ワイヤレス装置の確認](#)

[スイッチの確認](#)

[トラブルシュート](#)

[関連情報](#)

概要

このドキュメントは、Cisco Aironet ワイヤレス装置で Virtual VLAN (VLAN; 仮想 LAN) を使用するための設定例を紹介しています。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- Cisco Aironet ワイヤレス装置に精通していること
- VLAN と VLAN トランキングの LAN 切り替えコンセプトについて精通していること

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Aironet アクセス ポイントとワイヤレス ブリッジ
- Cisco Catalyst スイッチ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

関連製品

この設定のスイッチ側は、次のハードウェアまたはソフトウェアで使用できます。

- CatOS または IOS が稼働している Catalyst 6x00/5x00/4x00
- IOS が稼働している Catalyst 35x0/37x0/29xx
- IOS が稼働している Catalyst 2900XL/3500XL

表記法

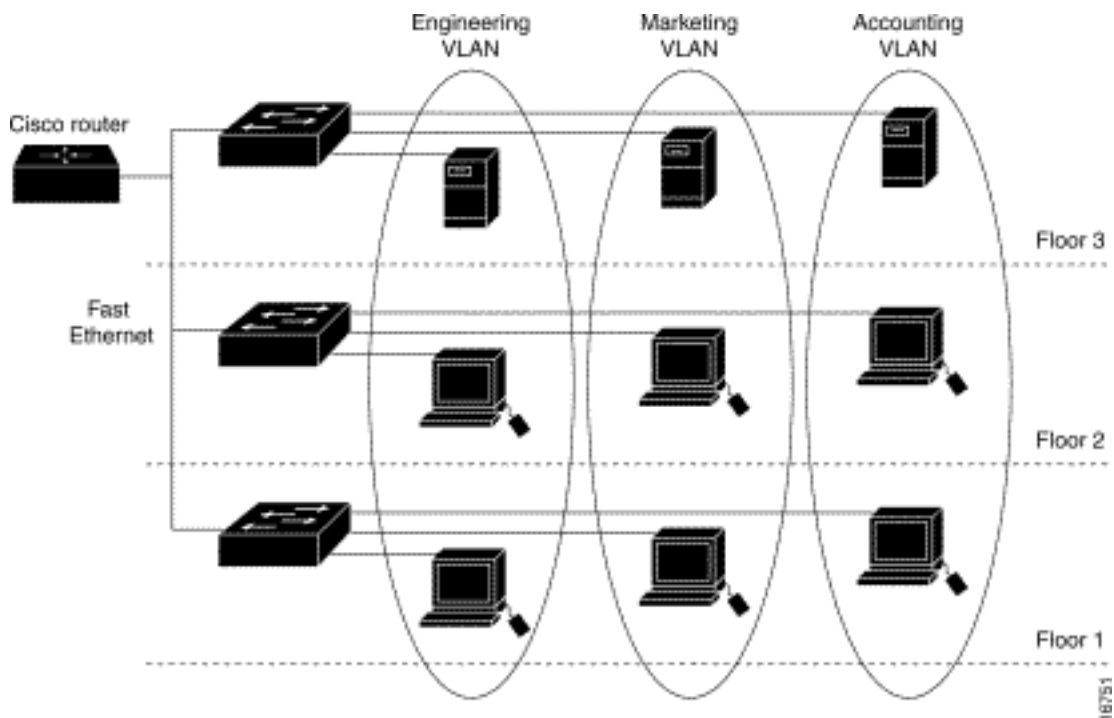
ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

VLAN

VLAN とは、物理的または地理的な基盤ではなく、機能、プロジェクト チーム、またはアプリケーションに基づいて論理的にセグメント化されたスイッチド ネットワークです。たとえば、特定のワークグループ チームで使用されているすべてのワークステーションとサーバを、現在のネットワークへの物理的接続や他のチームとの混合の可能性にかかわらず、同じ VLAN に接続できます。VLAN を使用することにより、デバイスや回線を物理的に取り外したり移動したりするのではなく、ソフトウェアでネットワークを再設定します。

VLAN は、一連の定義済みスイッチ内に存在するブロードキャスト ドメインであると考えられます。VLAN は、単一のブリッジング ドメインによって接続された数多くのエンドシステム、つまりホストまたはネットワーク機器（ブリッジ、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 スイッチでは、VLAN ごとに異なるグループを使用してスイッチ間でブリッジング プロトコルが稼働します。

デバイスを Cisco Catalyst スイッチに接続すると、デバイスが接続されているポートは VLAN 1 のメンバになります。デバイスの MAC アドレスは VLAN 1 の一部です。単一のスイッチで複数の VLAN を定義でき、ほとんどの Catalyst モデルでスイッチポートを設定できます。



ネットワーク内のポート数がスイッチのポート容量を超える場合は、複数のスイッチシャーシを相互接続してトランクを定義する必要があります。トランクとは VLAN のメンバではなく、1つまたは複数の VLAN にトラフィックを受け渡す導管です。

基本的に、特定の VLAN に接続するアクセスポイントの設定では、SSID を設定して、その VLAN を認識することが重要です。VLAN は VLAN ID または名前で識別されるため、特定の VLAN ID または名前が認識されるようにアクセスポイントの SSID が設定されると、その VLAN への接続が確立されます。この接続が確立されると、同じ SSID を持つ関連するワイヤレスクライアントデバイスは、アクセスポイント経由で VLAN にアクセスできます。VLAN は、クライアントとの間でやり取りされるデータを、有線接続でやり取りされるデータと同じように処理します。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 に割り当てることができる SSID は 1つだけです。

VLAN をワイヤレス LAN に拡張するには、IEEE 802.11Q タグ認識をアクセスポイントに追加します。宛先の VLAN が異なるフレームは、アクセスポイントによって、それぞれ異なる WEP キーを使用して、異なる SSID でワイヤレスに送信されます。その VLAN に関連付けられたクライアントだけがそれらのパケットを受信します。反対に、特定の VLAN に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、有線ネットワークに転送される前に、802.11Q のタグ付けがされます。

たとえば、社員と訪問客が同時に企業のワイヤレスネットワークにアクセスした場合、そのアクセスを個別に管理することが可能です。VLAN は SSID へのマッピングを実行し、ワイヤレスクライアントは適切な SSID のアタッチを行います。ワイヤレスブリッジを使用したネットワークでは、ワイヤレスリンクに複数の VLAN を通すことにより、別々の場所から VLAN に接続できます。

アクセスポイントのファストイーサネット インターフェイスで 802.1q が設定されていると、そのアクセスポイントは、VLAN 1 が定義されていない場合でも、常に VLAN 1 でキープアライブを送信します。その結果、イーサネットスイッチがアクセスポイントに接続して、警告メッセージを生成します。このことがアクセスポイントやスイッチの機能に悪影響を及ぼすことはありませんが、スイッチ ログに意味のないメッセージが記録されることによって、重要なメッセージが折り返されたり、表示されなくなったりする場合があります。

この動作により、アクセスポイントですべての SSID がモビリティ ネットワークに関連付けられ

ると問題が発生します。すべての SSID がモビリティ ネットワークに関連付けられている場合、アクセス ポイントの接続先のイーサネット 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 VLAN に割り当てられます。これは必ずしも VLAN 1 とは限りません。これにより、イーサネット スイッチ は 802.1q タグのトラフィックがアクセスポイントから送信されたことを示す警告メッセージを生成します。

キーブアライブ機能を無効にすると、スイッチでの過剰なメッセージを解消できます。

Cisco Aironet ワイヤレス装置で VLAN を展開する際、たとえ小さなポイントでも、これらの概念を無視すると、予期しないパフォーマンス上の問題が発生する場合があります。その例を次に示します。

- ワイヤレス デバイスで定義された VLAN に対し、トランク上で許可されている VLAN の制限障害スイッチ上では VLAN 1、10、20、30 および 40 が定義されているのに、ワイヤレス装置上では VLAN 1、10、30 しか定義されていない場合、トランク スイッチポートからその他の VLAN を削除する必要があります。
- インフラストラクチャ SSID の指定の誤使用アクセス ポイントを設置する際に、次の装置で SSID を使用する場合だけインフラストラクチャ SSID を割り当てます。ワークグループブリッジ デバイスリピータ アクセス ポイント非ルートブリッジクライアントがワイヤレスラップトップコンピュータだけの場合、SSID にインフラストラクチャ SSID を指定するのは誤設定であり、予期しない結果が発生します。ブリッジの設置では、1 つのインフラストラクチャ SSID だけを設定できます。このインフラストラクチャ SSID は、ネイティブ VLAN に関連する SSID である必要があります。
- ゲスト モード SSID 指定の誤使用または誤設計Cisco Aironet ワイヤレス装置上で複数の SSID/VLAN を定義すると、802.11 無線ビーコンにおいて SSID ブロードキャストできるゲスト モード SSID として、SSID を 1 つ割り当てることが可能です。その他の SSID はブロードキャストされません。クライアント デバイスは、接続先の SSID を指定する必要があります。
- 複数の VLAN と SSID が複数の OSI モデル レイヤ 3 サブネットを示していることが認識不能Cisco Aironet ソフトウェアの廃止バージョンは、1 つの VLAN に複数の SSID をバインドすることを許容します。現在のバージョンにはこの機能はありません。
- OSI モデル レイヤ 3 のルーティング障害または誤設計各 SSID とその SSID にリンクされている VLAN には、ルーティング デバイスと、クライアントにアドレスを割り当てるためのソース (たとえば、DHCP サーバまたは DHCP サーバのスコープ) が必要です。
- ネイティブ VLAN の誤認識または誤設定ネットワークの物理的インフラストラクチャを構成しているルータおよびスイッチは、その物理インフラストラクチャにアタッチされているクライアント PC とは異なる方式が管理されています。これらのルータやスイッチのインターフェイスがそのメンバとして所属している VLAN は、ネイティブ VLAN (デフォルトでは VLAN 1) と呼ばれます。クライアント PC は、IP 電話が別の VLAN のメンバであるのと同じように、別の VLAN のメンバです。アクセス ポイントまたはブリッジの管理インターフェイス (インターフェイス BVI1) は、VLAN や SSID が対象のワイヤレス デバイスに何を受け渡すかにかかわらず、ネイティブ VLAN の一部と見なされ、番号が付けられます。

ネイティブ VLAN の意味

IEEE 802.1Q トランク ポートを使用する場合、すべてのフレームにタグが付けられます。ただし、ポートの「ネイティブ VLAN」として設定された VLAN 上のフレームを除きます。ネイティブ VLAN 上のフレームは常にタグなしで送信され、通常はタグなしで受信されます。したがって、AP をスイッチポートに接続する場合、その AP に設定されているネイティブ VLAN は、スイッ

チポートに設定されているネイティブ VLAN と一致している必要があります。

注： ネイティブ VLAN が一致しない場合、フレームは廃棄されます。

このシナリオについて、例を示して詳しく説明します。スイッチポート上のネイティブ VLAN が VLAN 12 として設定され、AP 上でネイティブ VLAN が VLAN 1 として設定されているとします。この場合、AP がそのネイティブ VLAN でフレームをスイッチに送信すると、AP のネイティブ VLAN からのフレームにはタグが付いていないため、スイッチはそのフレームを VLAN 12 に属しているものと見なします。これにより、ネットワークで混乱が生じ、接続の問題が発生します。スイッチポートがそのネイティブ VLAN から AP にフレームを転送する際も、同じことが起きます。

ワイヤレス ネットワークでリピータ AP を設定している場合は、ネイティブ VLAN の設定がさらに重要になります。リピータ AP には複数の VLAN を設定できません。リピータ AP でサポートされるのはネイティブ VLAN だけです。したがって、ルート AP、AP の接続先スイッチポート、およびリピータ AP でネイティブ VLAN 設定が同じである必要があります。異なる場合は、スイッチ経由のトラフィックがリピータ AP を通過しなくなります。

リピータ AP のネイティブ VLAN 設定の不一致により問題が発生する可能性があるシナリオの例として、ルート AP の接続先スイッチの背後で DHCP サーバが使用されている場合があります。この場合、リピータ AP のネイティブ VLAN (ルート AP やスイッチと同じではない) からのフレーム (この例では DHCP 要求) が廃棄されるため、リピータ AP に関連付けられているクライアントは DHCP サーバから IP アドレスを受信しません。

また、スイッチポートを設定する際、AP に設定されているすべての VLAN が、スイッチポートで許可されていることを確認します。たとえば、AP (ワイヤレス ネットワーク) に VLAN 6、7、および 8 が存在する場合、スイッチポートでこれらの VLAN が許可されている必要があります。スイッチで次の設定コマンドを使用して、これを実行できます。

```
switchport trunk allowed vlan add 6,7,8
```

デフォルトでは、トランクとして設定されているスイッチポートは、すべての VLAN でトランクポートを通過することを許可します。スイッチポートの設定方法の詳細は、『[関連スイッチとの相互対話](#)』を参照してください。

注： 特に大規模なネットワークの場合は、AP 上のすべての VLAN を許可することも問題になる場合があります。これにより、AP の CPU 使用率が高くなる可能性があります。CPU 使用率の上昇を回避するには、AP が対象とする VLAN トラフィックだけが AP を通過するように、スイッチで VLAN をプルーニングします。

[アクセス ポイント上の VLAN](#)

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注： このドキュメントで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#)(登録ユーザ専用)を使用してください。

アクセス ポイントの概念

このセクションは、アクセス ポイントで VLAN を展開する方法についての概念を説明し、次のネットワーク ダイアグラムを参照しています。

このサンプル ネットワークでは、VLAN 1 がネイティブ VLAN です。また、VLAN 10、20、30、および 40 が存在し、別のスイッチ シャーシにトランクされています。VLAN 10 と 30 だけがワイヤレス ドメインに拡張されています。ネイティブ VLAN は、管理機能とクライアント認証を提供する必要があります。

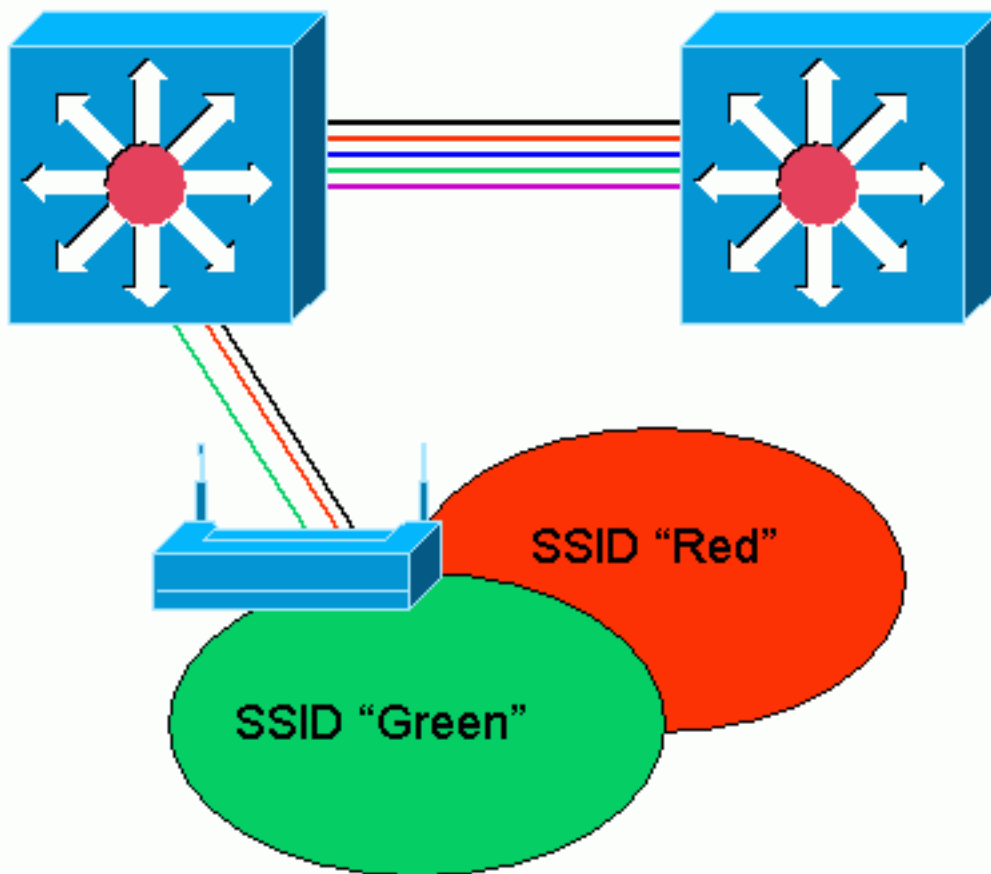
VLAN 1 (Native)

VLAN 10

VLAN 20

VLAN 30

VLAN 40



アクセス ポイントの設定

VLAN 用にアクセス ポイントを設定するには、次の手順を実行します。

1. APのGUIから、[Services] > [VLAN]をクリックして[Services]に移動します。VLAN] ページから [Routing] を選択します。最初のステップではネイティブ VLAN を設定します。Current VLAN List から New を選択します。VLAN ID ボックスに、ネイティブ VLAN の VLAN 番号を入力します。VLAN 番号は、スイッチで設定されているネイティブ VLAN と一致している必要があります。ネイティブ VLAN のサブインターフェイスにインターフェイス BVI 1 が関連付けられているため、インターフェイス BVI 1 に割り当てられている IP アドレスは、ネットワーク上の他のインフラストラクチャ デバイス (つまり、CatOS が稼働している Catalyst スイッチ上のインターフェイス SC0) と同じ IP サブネットにある必要があります

。ネイティブ VLAN のチェックボックスをオンにします。この VLAN を適用する無線インターフェイス (複数可) のチェックボックスをオンにします。[Apply] をクリックします。

The screenshot shows the Cisco 1200 Access Point configuration interface. The main content area is titled "Services: VLAN" and contains the following sections:

- Global VLAN Properties:** Shows "Current Native VLAN: VLAN 1".
- Assigned VLANs:** Contains a "Current VLAN List" with a dropdown menu showing "VLAN 1", "VLAN 10", and "VLAN 30". To the right is a "Create VLAN" form with a "VLAN ID" field set to "1" (range 1-4095), a checked "Native VLAN" box, and two radio buttons for "Radio 0-802.11B" (checked) and "Radio 1-802.11A". SSID fields are set to "<NONE>".
- VLAN Information:** Shows "View information for: VLAN 1" and a table of statistics.

	FastEthernet Packets	Radio0-802.11B Packets	Radio1-802.11A Packets
Received	27712	27711	
Transmitted	0	0	

At the bottom of the interface, there is a "Refresh" button and a footer with the text "Copyright (c) 1992-2002, 2003 by Cisco Systems, Inc."

または、CLI で次のコマンドを実行します。

```
AP# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AP(config)# interface Dot11Radio0.1
AP(config-subif)# encapsulation dot1Q 1 native
AP(config-subif)# interface FastEthernet0.1
AP(config-subif)# encapsulation dot1Q 1 native
AP(config-subif)# end
AP# write memory
```

2. 他の VLAN を設定するには、次の手順を実行します。Current VLAN List から **New** を選択します。VLAN ID ボックスに、目的の VLAN の VLAN 番号を入力します。VLAN 番号は、スイッチで設定されている VLAN と一致している必要があります。この VLAN を適用する無線インターフェイス (複数可) のチェックボックスをオンにします。[Apply] をクリックします。

The screenshot shows the Cisco 1200 Access Point configuration page for 'Services: VLAN'. The 'Global VLAN Properties' section shows 'Current Native VLAN: VLAN1'. The 'Assigned VLANs' section has a 'Current VLAN List' containing '< NEW >', 'VLAN1', 'VLAN2', and 'VLAN3'. The 'Create VLAN' section shows 'VLAN ID: 10 (-4095)' with checkboxes for 'Native VLAN', 'Enable Public Secure Packet Forwarding', and 'Radio0-802.11B' (checked). SSID fields are set to 'Red' and '< NONE >'. The 'VLAN Information' table shows statistics for 'VLAN1'.

	FastEthernet Packets	Radio0-802.11B Packets	Radio1-802.11A Packets
Received	77712	77711	
Transmitted	0	0	

または、CLI で次のコマンドを実行します。

```
AP# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AP(config)# interface Dot11Radio0.10
AP(config-subif)# encapsulation dot1q 10
AP(config-subif)# interface FastEthernet0.10
AP(config-subif)# encapsulation dot1q 10
AP(config-subif)# end
AP# write memory
```

目的の各 VLAN に対して手順 2a ~ 2d を繰り返します。または、CLI でサブインターフェイスと VLAN 番号を適宜変更して次のコマンドを入力します。

```
AP# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AP(config)# interface Dot11Radio0.30
AP(config-subif)# encapsulation dot1q 30
AP(config-subif)# interface FastEthernet0.30
AP(config-subif)# encapsulation dot1q 30
AP(config-subif)# end
AP# write memory
```

3. 次に、設定した VLAN を SSID に割り当てます。これを行うには、[Security] > [SSID Manager]をクリックします。注：アクセスポイントで定義されているすべてのVLANを

SSIDに関連付ける必要はありません。たとえば、セキュリティ上の理由により、ほとんどのアクセスポイントのインストールでは、ネイティブ VLAN に SSID の関連付けを行いません。新しい SSID を作成するには、**New** を選択します。SSID ボックスに、目的の SSID を入力します（大文字と小文字が区別されます）。ドロップダウンリストから、この SSID に関連付ける VLAN 番号を選択します。注：このドキュメントを目的の範囲内に収めるために、SSIDのセキュリティは取り上げていません。**[Apply-RadioX]** をクリックして、選択した無線インターフェイスに SSID を作成するか、**[Apply-all]** をクリックして、すべての無線インターフェイスに SSID を作成します。

The screenshot displays the Cisco 1200 Access Point web interface. The main title is "Cisco 1200 Access Point". The interface is divided into several sections:

- Navigation Menu (Left):** Includes HOME, EXPRESS SETUP, NETWORK WAP, ASSOCIATION, NETWORK INTERFACES, SECURITY (highlighted), Admin Access, SSID Manager (highlighted), Encryption Manager, Server Manager, Local RADIUS Server, Advanced Security, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG.
- Radio Selection:** Two tabs are visible: "RADIO0-802.11B" (selected) and "RADIO1-802.11A".
- Hostname:** "ap" with "ap uptime is 1 hour, 59 minutes".
- Security: SSID Manager - Radio0 802.11B**
 - SSID Properties:**
 - Current SSID List:** A list with options: "<NEW>", "Green", and "Red" (selected).
 - SSID:** "Red" (input field).
 - VLAN:** "10" (dropdown menu).
 - Buttons:** "Delete-Radio0" and "Delete-All".
 - Authentication Methods Accepted:**
 - Open Authentication: "< NO ADDITION >"
 - Shared Authentication: "< NO ADDITION >"
 - Network EAP: "< NO ADDITION >"
 - Authenticated Key Management:**
 - None
 - LCKM: "Mandatory"
 - WPA: "Optional"
 - WPA Pre-shared Key:** (input field) with radio buttons for "ASCII" (selected) and "Hexadecimal".
 - EAP Client (optional):** Username and Password input fields.
 - Association Limit (optional):** (input field) with "1-255".
 - Enable Proxy Mobile IP
 - Enable Accounting
 - Buttons:** "Apply-Radio0", "Apply-All", "Cancel".
- Global Radio0-802.11B SSID Properties:**
 - Set Guest Mode SSID:** "<NONE >"
 - Set Infrastructure SSID:** "<NONE >" with checkbox "Force Infrastructure Devices to associate only to this SSID".
 - Buttons:** "Apply", "Cancel".

または、CLI で次のコマンドを発行します。

```
AP# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.  
AP(config)# interface Dot11Radio0  
AP(config-if)# ssid Red  
AP(config-if-ssid)# vlan 10  
AP(config-if-ssid)# end  
AP# write memory
```

4. 目的の各 SSID に対して手順 3a ~ 3d を繰り返します。または、CLI で SSID を適宜変更して次のコマンドを入力します。

```
AP# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
AP(config)# interface Dot11Radio0  
AP(config-if)# ssid Green  
AP(config-if-ssid)# vlan 30  
AP(config-if-ssid)# end  
AP# write memory
```

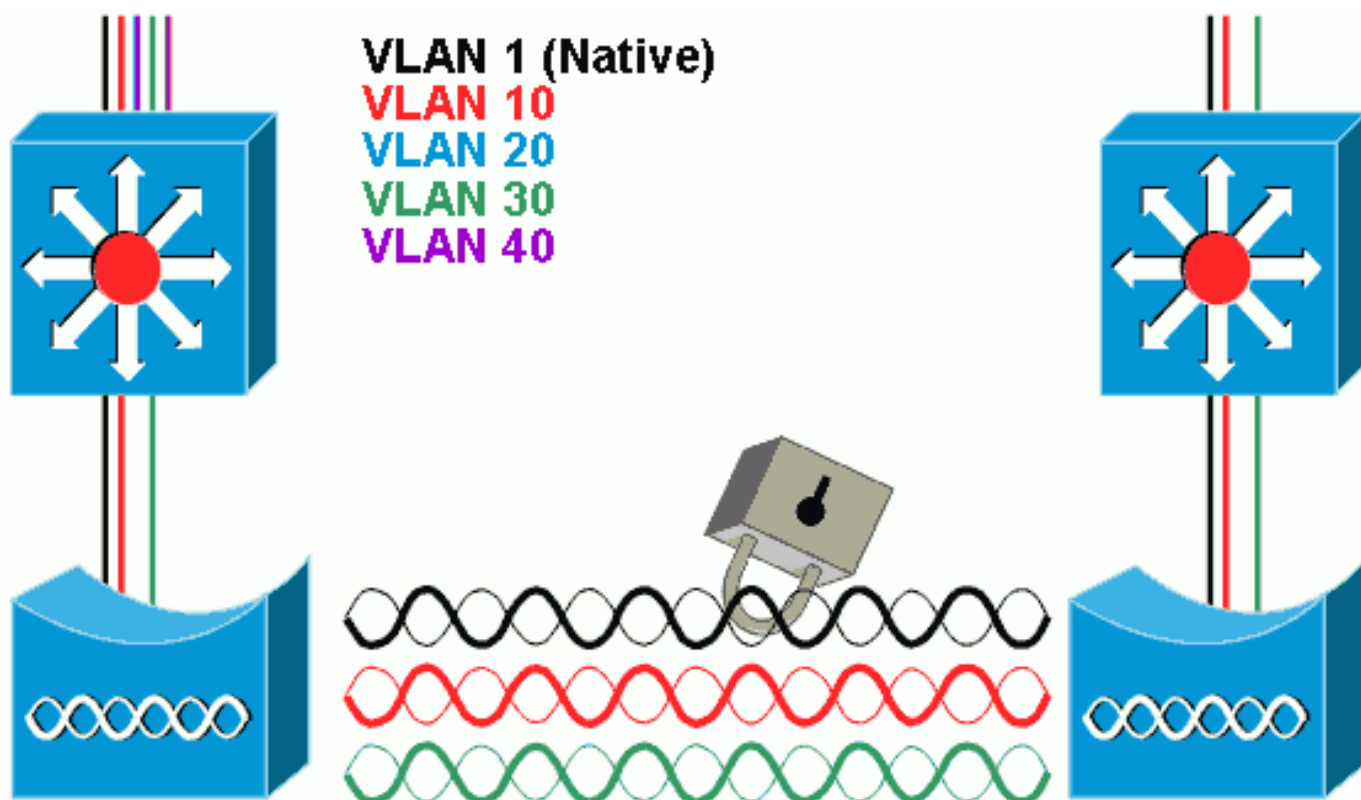
注：これらの例には認証は含まれていません。クライアントで何らかの認証形式 (Open、Network-EAP など) を関連付ける必要があります。

ブリッジ上の VLAN

ブリッジの概念

このセクションは、ブリッジで VLAN を展開する方法に関連する概念を説明し、次のネットワークダイアグラムを参照しています。

このサンプル ネットワークでは、VLAN 1 がネイティブ VLAN です。また、VLAN 10、20、30、および 40 が存在します。VLAN 10 と 30 だけがリンクの相手側まで拡張されています。ワイヤレスリンクは暗号化されています。



無線リンクを通過するデータを暗号化するには、ネイティブ VLAN の SSID だけに暗号化を適用します。その暗号化が、他のすべての VLAN に適用されます。ブリッジング時に、各 VLAN に個別の SSID を関連付ける必要はありません。VLAN 設定は、ルートブリッジと非ルートブリッジの両方で同じです。

ブリッジの設定

サンプルネットワークダイアグラムに示すように VLAN にブリッジを設定するには、次の手順を実行します。

1. APのGUIで、[Services] > [VLAN]をクリックし、サービスに移動します。[VLAN] ページから [Routing] を選択します。最初のステップではネイティブ VLAN を設定します。これを行うには、Current VLAN Listから[<New>]を選択します。VLAN ID ボックスに、ネイティブ VLAN の VLAN 番号を入力します。これは、スイッチ上で設定されているネイティブ VLAN と一致する必要があります。ネイティブ VLAN のサブインターフェイスにインターフェイス BVI 1 が関連付けられているため、インターフェイス BVI 1 に割り当てられている IP アドレスは、ネットワーク上の他のインフラストラクチャ デバイス (つまり、CatOS が稼働している Catalyst スイッチ上のインターフェイス SC0) と同じ IP サブネットにある必要があります。ネイティブ VLAN のチェックボックスをオンにします。[Apply] をクリックします。

The screenshot shows the Cisco 1200 Access Point GUI. The main content area is titled "Services: VLAN".

Global VLAN Properties

Current Native VLAN: VLAN 1

Assigned VLANs

Current VLAN List: <NEW>, VLAN 1, VLAN 10, VLAN 30. A "Delete" button is next to the list.

Create VLAN

VLAN ID: 1 (-4095)

Native VLAN

Enable Public Secure Packet Forwarding

Radius 0-802.11B

SSID: <NONE> Define SSID

Radius 1-802.11A

SSID: <NONE> Define SSID

Buttons: Apply, Cancel

VLAN Information

View information for: VLAN 1

	Ethernet Packets	Radius 0-802.11B Packets	Radius 1-802.11A Packets
Received	27712	77711	
Transmitted	0		

Buttons: Refresh

Footer: Copyright © 1992-2002, 2003 by Cisco Systems, Inc.

または、CLI で次のコマンドを実行します。

```
bridge# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
bridge(config)# interface Dot11Radio0.1  
bridge(config-subif)# encapsulation dot1Q 1 native  
bridge(config-subif)# interface FastEthernet0.1  
bridge(config-subif)# encapsulation dot1Q 1 native  
bridge(config-subif)# end  
bridge# write memory
```

2. 他の VLAN を設定するには、次の手順を実行します。Current VLAN List から **New** を選択します。VLAN ID ボックスに、目的の VLAN の VLAN 番号を入力します。VLAN 番号は、スイッチで設定されている VLAN と一致している必要があります。[Apply] をクリックします

The screenshot shows the Cisco 1200 Access Point configuration interface. The main content area is titled "Services: VLAN" and "Global VLAN Properties". It displays "Current Native VLAN: VLAN1" and "Assigned VLANs". Under "Assigned VLANs", there is a "Current VLAN List" dropdown menu with options: <NEW>, VLAN1, VLAN10 (selected), and VLAN30. To the right of this list is a "Delete" button. Below the list is the "Create V_LAN" section, which includes a "VLAN ID:" field set to "10 (-4095)". There are four checkboxes: "Native VLAN" (unchecked), "Enable Public Secure Packet Forwarding" (unchecked), "Radio0-802.11B" (checked), and "Radio1-802.11A" (unchecked). Below these are two "SSID:" dropdown menus. The first is for "Radio0-802.11B" and is set to "Red". The second is for "Radio1-802.11A" and is set to "<NONE>". There are "Define SSID" links next to each dropdown. At the bottom right of the configuration area are "Apply" and "Cancel" buttons. Below the configuration area is a "VLAN Information" section with a "View information for:" dropdown set to "VLAN1". Below this is a table with three columns: "FastEthernet Packets", "Radio0-802.11B Packets", and "Radio1-802.11A Packets". The table has two rows: "Received" and "Transmitted".

	FastEthernet Packets	Radio0-802.11B Packets	Radio1-802.11A Packets
Received	77712	77711	
Transmitted	0	0	

または、CLI で次のコマンドを実行します。

```
bridge# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
bridge(config)# interface Dot11Radio0.10  
bridge(config-subif)# encapsulation dot1Q 10  
bridge(config-subif)# interface FastEthernet0.10  
bridge(config-subif)# encapsulation dot1Q 10  
bridge(config-subif)# end
```

```
bridge# write memory
```

目的の各 VLAN に対して手順 2a ~ 2c を繰り返します。または、CLI でサブインターフェイスと VLAN 番号を適宜変更して次のコマンドを入力します。

```
AP# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bridge(config)# interface Dot11Radio0.30
bridge(config-subif)# encapsulation dot1Q 30
bridge(config-subif)# interface FastEthernet0.30
bridge(config-subif)# encapsulation dot1Q 30
bridge(config-subif)# end
bridge# write memory
```

3. SSID Manager([Security] > [SSID Manager]メニュー項目の下)で、ネイティブVLANをSSIDに関連付けます。注：ブリッジを作成する場合、VLANに関連付ける必要があるSSIDは、ネイティブVLANに関連付けられているSSIDだけです。このSSIDをインフラストラクチャSSIDとして指定する必要があります。Current SSID ListからNewを選択します。SSIDボックスに、目的のSSIDを入力します(大文字と小文字が区別されます)。ネイティブVLANに関連するVLAN番号をドロップダウンリストから選択します。注：このドキュメントを目的の範囲内に収めるために、SSIDのセキュリティは取り上げていません。Applyをクリックして、無線インターフェイスにSSIDを作成し、ネイティブVLANに関連付けます。

The screenshot displays the configuration interface for a Cisco Aironet 1300 Series Wireless Bridge. The page title is "Cisco Aironet 1300 Series Wireless Bridge". The hostname is "labbr1310ip93" and the uptime is "3 days, 18 hours, 45 minutes". The navigation menu on the left includes "HOME", "EXPRESS SET-UP", "EXPRESS SECURITY", "NETWORK MAP", "ASSOCIATION", "NETWORK INTERFACES", "SECURITY", "Admin Access", "Encryption Manager", "SSID Manager", "Server Manager", "Advanced Security", "SERVICES", "WIRELESS SERVICES", "SYSTEM SOFTWARE", and "EVENT LOG". The main content area is titled "Security: SSID Manager". Under "SSID Properties", the "Current SSID List" shows a single entry "< NEW >". To the right, the "SSID" is set to "Black", the "VLAN" is set to "1", and the "Network ID" is "(0-4096)". There is a "Delete" button below the list. The "Authentication Settings" section is visible below, showing "Authentication Methods Accepted" with "Open Authentication" checked and "Shared Authentication" and "Network EAP" unchecked. The "Server Priorities" section is partially visible at the bottom.

ページの一番下までスクロールし、Global Radio0-802.11G SSID Properties で Set Infrastructure SSID ドロップダウン リストから SSID を選択します。[Apply] をクリックします。

Username: Password:

Apply Cancel

Global Radio0-802.11G SSID Properties

Set Guest Mode SSID:

Set Infrastructure SSID: Force Infrastructure Devices to associate only to this SSID

Apply Cancel

Close Window Copyright (c) 1992-2004 by Cisco Systems, Inc.

または、CLI で次のコマンドを発行します。

```
AP# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AP(config)# interface Dot11Radio0
AP(config-if)# ssid Black
AP(config-if-ssid)# vlan 1
AP(config-if-ssid)# infrastructure-ssid
AP(config-if-ssid)# end
AP# write memory
```

注：VLANが使用されている場合、SSIDは論理サブインターフェイスではなく、物理 Dot11Radio インターフェイスで設定されます。注：この例には認証は含まれていません。ルートブリッジと非ルートブリッジでは、関連付けに何らかの認証形式（Open、Network-EAP など）が必要です。

[RADIUS サーバを使用した VLAN へのユーザの割り当て](#)

ユーザが認証を行う際に、そのユーザまたはユーザグループを特定の VLAN に割り当てられるように、RADIUS サーバを設定することができます。この機能の詳細については、『Cisco Aironet アクセスポイント用 Cisco IOS ソフトウェア設定ガイド、12.4(3g)JA および 12.3(8)JEB』ドキュメントの「[RADIUS サーバを使用してユーザを VLAN に割り当てる](#)」セクションで、

[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 サーバを設定して、モビリティ グループをユーザまたはユーザグループに動的に割り当てることもできます。これにより、アクセスポイントで複数の SSID を設定する必要がなくなります。代わりに、アクセスポイントごとに SSID を 1 つだけ設定する必要があります。この機能の詳細については、『Cisco Aironet アクセスポイント用 Cisco IOS ソフトウェア設定ガイド、12.4(3g)JA および 12.3(8)JEB』ドキュメントの「[ダイナミックモビリティグループの割り当てに RADIUS サーバを使用する](#)」セクションを参照してください。

[アクセスポイントとブリッジでのブリッジグループの設定](#)

一般的に、ブリッジグループは、セグメント化されたスイッチドメインを作成します。トラフィックは、ブリッジグループ間ではなく、各ブリッジグループ内のホストに制限されます。スイッチは、ブリッジグループを構成するホスト間だけにトラフィックを転送します。これは、ブロードキャストおよびマルチキャストトラフィック（フラッディング）をそれらのホストだけに制限

します。ブリッジグループはネットワーク輻輳を緩和し、さらにトラフィックを特定のネットワークエリアにセグメント化する場合は、ネットワークセキュリティを強化します。

詳細は、「[ブリッジングの概要](#)」を参照してください。

ワイヤレス ネットワークでは、ブリッジグループがワイヤレス アクセス ポイントとブリッジで設定されて、VLAN のデータトラフィックがワイヤレス メディアから有線側に、またはその逆に転送されます。

AP の CLI で次のステップを実行して、アクセス ポイントまたはブリッジでブリッジグループをグローバルに有効にします。

この例では、ブリッジグループ番号 1 を使用しています。

Ap(configure)#bridge 1

注：ブリッジグループには、1 ~ 255の番号を付けることができます。

ワイヤレス デバイスの無線インターフェイスとファスト イーサネット インターフェイスを設定して、同じブリッジグループに所属するようにします。これにより、これらの 2 つの異なるインターフェイス間にパスが作成され、これらのインターフェイスはタギングのために同じ VLAN に割り当てられています。その結果、無線インターフェイス経由でワイヤレス側から送信されたデータは、有線ネットワークの接続先イーサネット インターフェイスに送信されます（その逆も同様）。つまり、同じブリッジグループに属している無線インターフェイスとイーサネット インターフェイスは、実際にはそれらのインターフェイス間でデータをブリッジングしていることとなります。

アクセス ポイントやブリッジでは、トラフィックが有線からワイヤレス、またはその逆に通過できるように、VLAN ごとに 1 つのブリッジグループが必要です。したがって、ワイヤレスにトラフィックを渡す必要がある VLAN が多いほど、必要なブリッジグループの数が増加します。

たとえば、トラフィックをネットワークのワイヤレス側から有線側に渡す VLAN が 1 つしか存在しない場合は、AP またはブリッジの CLI からブリッジグループを 1 つだけ設定します。トラフィックをワイヤレス側から有線側に、および有線側からワイヤレス側に渡す VLAN が複数存在する場合は、無線サブインターフェイスとファスト イーサネット サブインターフェイスで VLAN ごとにブリッジグループを設定します。

1. bridge group dot11radio インターフェイスコマンドを使用して、ワイヤレスインターフェイスでブリッジグループを設定します。次に例を示します。

```
AP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)# interface Dot11Radio0.1
Ap(config-subif)# encapsulation dot1q 1 native
Ap(config-subif)# bridge group 1 !--- Here "1" represents the bridge group number.
ap(config-subif)# exit
```

2. ファスト イーサネット インターフェイスに同じブリッジグループ番号（この例では「1」）のブリッジグループを設定して、VLAN 1 のトラフィックがワイヤレス インターフェイス経由でこの有線側に渡される（その逆も同様）ようにします。

```
Ap(config)# interface fastEthernet0.1
Ap(config-subif)# encapsulation dot1q 1 native
Ap(config-subif)# bridge group 1 !--- Here "1" represents the bridge group number.
Ap(config-subif)# exit
```

注：無線インターフェイスでブリッジグループを設定すると、これらのコマンドは自動的に設定されます。bridge-group 1 subscriber-loop-controlbridge-group 1 block-unknown-sourceno bridge-group 1 source-learningno bridge-group 1 unicast-floodingbridge-group 1 spanning-disabled注：ファーストイーサネットインターフェイスでブリッジグループを設定すると、これらのコマンドは自動的に設定されます。no bridge-group 1 source-learningbridge-group 1 spanning-disabled

Integrated Routing and Bridging (IRB)

Integrated Routing and Bridging を使用すると、ルーテッド インターフェイスとブリッジ グループ間、またはブリッジ グループ間でそれぞれ特定のプロトコルをルーティングできます。ローカルトラフィックまたはルーティング不可能なトラフィックを、同じブリッジ グループ内のブリッジド インターフェイス間でブリッジングできます。一方、ルーティング可能なトラフィックは、他のルーテッド インターフェイスまたはブリッジ グループにルーティングできます。

Integrated Routing and Bridging では、次の処理が可能です。

- パケットをブリッジド インターフェイスからルーテッド インターフェイスにスイッチングする
- パケットをルーテッド インターフェイスからブリッジド インターフェイスにスイッチングする
- パケットを同じブリッジ グループ内でスイッチングする

ワイヤレス アクセス ポイントとブリッジで IRB を有効にして、ブリッジ グループ間またはルーテッド インターフェイスとブリッジ グループ間でトラフィックをルーティングします。ブリッジ グループ間またはブリッジ グループとルーテッド インターフェイス間でトラフィックをルーティングするには、外部ルータまたはレイヤ 3 スイッチが必要です。

次のコマンドを発行して、AP またはブリッジで IRB を有効にします。

```
AP(configure)#bridge irb
```

Integrated Routing and Bridging は Bridge-Group Virtual Interface (BVI; ブリッジ グループ仮想インターフェイス) の概念を使用して、ルーテッド インターフェイスとブリッジ グループ間またはブリッジ グループ間でトラフィックをルーティングします。

BVI は、通常のルーテッド インターフェイスのように動作するレイヤ 3 スイッチ ルータ内の仮想インターフェイスです。BVI はブリッジングをサポートしませんが、実際にはレイヤ 3 スイッチ ルータ内のルーテッド インターフェイスに対応するブリッジ グループとなっています。BVI には、対応するブリッジ グループに適用されるすべてのネットワーク レイヤ アトリビュート (ネットワーク レイヤ アドレスやフィルタなど) があります。この仮想インターフェイスに割り当てられているインターフェイス番号は、この仮想インターフェイスが表すブリッジ グループに対応しています。この番号が仮想インターフェイスとブリッジ グループ間のリンクになります。

次の手順を実行して、アクセス ポイントとブリッジで BVI を設定します。

1. BVI を設定し、さらに BVI にブリッジ グループの対応する番号を割り当てます。次の例では、ブリッジ グループ番号 1 を BVI に割り当てています。

```
Ap(configure)#interface BVI 1
AP(config-if)#ip address 10.1.1.1 255.255.0.0 !--- Assign an IP address to the BVI.
Ap(config-if)#no shut
```

2. BVI を有効にして、対応するブリッジ グループから受信したルーティング可能なパケットを受け入れ、ルーティングします。

```
Ap(config)# bridge 1 route ip!---
```

!--- This example enables the BVI to accept and route the IP packet.

BVI が必要になるのは、AP が配置されている管理 VLAN またはネイティブ VLAN (この例では VLAN 1) だけであるということを理解することが重要です。AP またはブリッジに設定されている VLAN やブリッジ グループの数に関係なく、その他のサブインターフェイスには BVI は必要ありません。これは、その他のすべての VLAN (ネイティブ VLAN を除く) ではトラフィックにタグを付け、トランキングしたインターフェイス dot1q を経由してスイッチの有線側にそのトラフィックを送出するからです。たとえば、ネットワークに 2 つの VLAN がある場合は 2 つのブリッジ グループが必要ですが、ワイヤレス ネットワークには、管理 VLAN に対応する BVI は 1 つだけで十分です。ブリッジ グループ仮想インターフェイスで特定のプロトコルのルーティングを有効にすると、ルーテッド インターフェイスから送信された、ブリッジ ドメイン内のホスト宛てのパケットは、ブリッジ グループの仮想インターフェイスにルーティングされ、対応するブリッジ インターフェイスに転送されます。ブリッジ グループ仮想インターフェイスにルーティングされたすべてのトラフィックは、対応するブリッジ グループにブリッジドトラフィックとして転送されます。ブリッジド インターフェイスで受信されたすべてのルーティング可能なトラフィックは、ブリッジ グループ仮想インターフェイスから直接送信されたかのように、他のルーテッド インターフェイスにルーティングされます。ブリッジングと IRB についての詳細は、『[ブリッジングの設定](#)』を参照してください。

[関連スイッチとの相互対話](#)

このセクションでは、Cisco Aironet ワイヤレス装置に接続する Cisco スイッチを設定したり、その設定を確認するために必要な情報を提供しています。

注：このドキュメントで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#)(登録ユーザ専用)を使用してください。

[スイッチの設定 : Catalyst OS](#)

Catalyst OSが稼働するスイッチをアクセスポイントにVLANをトランクするように設定するには、コマンド構文は `set trunk <module #/port #> on dot1q` と `set trunk <module #/port #> <vlan list>` です。

サンプル ネットワーク ダイアグラムの例では、次のようになります。

```
set trunk 2/1 on dot1q
set trunk 2/1 1,10,30
```

[スイッチの設定 : IOSベースのCatalystスイッチ](#)

次の場合は、インターフェイス コンフィギュレーション モードで下記のコマンドを入力します。

- スイッチポートを設定して、VLAN をアクセス ポートにトランクする
- IOS が稼働している Catalyst スイッチで設定する

- CatIOS には次のバージョンが含まれるが、これらに限定されない6x004x0035x0295x

```
switchport mode trunk
switchport trunk encapsulation dot1q
switchport nonegotiate
switchport trunk native vlan 1
switchport trunk allowed vlan add 1,10,30
```

注：IOSベースのCisco Aironetワイヤレス機器はDynamic Trunking Protocol(DTP)をサポートしていないため、スイッチはDTPのネゴシエートを試行しないでください。

スイッチの設定：Catalyst 2900XL/3500XL

IOS が稼働している Catalyst 2900XL または 3500XL スイッチでスイッチポートを設定して、VLAN をアクセス ポイントにトランクさせる場合は、インターフェイス コンフィギュレーション モードで次のコマンドを入力します。

```
switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk native vlan 1
switchport trunk allowed vlan 1,10,30
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

ワイヤレス装置の確認

- **show vlan** : アクセスポイントで現在設定されているすべてのVLANとそのステータスを表示します

```
ap#show vlan
```

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

```
vLAN Trunk Interfaces: FastEthernet0.1
Dot11Radio0.1
Virtual-Dot11Radio0.1
```

This is configured as native Vlan for the following interface(s) :

```
FastEthernet0
Dot11Radio0
Virtual-Dot11Radio0
```

Protocols Configured:	Address:	Received:	Transmitted:
Bridging	Bridge Group 1	36954	0
Bridging	Bridge Group 1	36954	0

```
Virtual LAN ID: 10 (IEEE 802.1Q Encapsulation)
```

```
vLAN Trunk Interfaces: FastEthernet0.10
Dot11Radio0.10
Virtual-Dot11Radio0.10
```

Protocols Configured:	Address:	Received:	Transmitted:
Bridging	Bridge Group 10	5297	0
Bridging	Bridge Group 10	5297	0
Bridging	Bridge Group 10	5297	0

Virtual LAN ID: 30 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interfaces: FastEthernet0.30
 Dot11Radio0.30
 Virtual-Dot11Radio0.30

Protocols Configured:	Address:	Received:	Transmitted:
Bridging	Bridge Group 30	5290	0
Bridging	Bridge Group 30	5290	0
Bridging	Bridge Group 30	5290	0

ap#

- **show dot11 associations**:SSID/VLANごとに、関連付けられたクライアントに関する情報を表示します

ap#**show dot11 associations**

802.11 Client Stations on Dot11Radio0:

SSID [Green] :

SSID [Red] :

Others: (not related to any ssid)

ap#

スイッチの確認

- Catalyst OSベースのスイッチで**show trunk <module #/port #>** : 特定のポートのトランクのステータスを表示します

Console> (enable) show trunk 2/1

* - indicates vtp domain mismatch

Port	Mode	Encapsulation	Status	Native vlan
2/1	on	dot1q	trunking	1

Port Vlans allowed on trunk

2/1	1,10,30
-----	---------

Port Vlans allowed and active in management domain

2/1	1,10,30
-----	---------

Port Vlans in spanning tree forwarding state and not pruned

2/1	1,10,30
-----	---------

Console> (enable)

- IOSベースのスイッチで**show interface fastethernet <module #/port #> trunk** : 特定のインターフェイス上のトランクのステータスを表示します

2950g#show interface fastEthernet 0/22 trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/22	on	802.1q	trunking	1

```
Port          Vlans allowed on trunk
Fa0/22      1,10,30
```

```
Port          Vlans allowed and active in management domain
Fa0/22       1,10,30
```

```
Port          Vlans in spanning tree forwarding state and not pruned
Fa0/22       1,10,30
2950gA#
```

- Catalyst 2900XL/3500XLスイッチでは、**show interface fastethernet <module #/port #> switchport** : 特定のインターフェイス上のトランクのステータスを表示します

```
cat3524xl#show interface fastEthernet 0/22 switchport
```

```
Name: Fa0/22
```

```
Switchport: Enabled
```

```
Administrative mode: trunk
```

```
Operational Mode: trunk
```

```
Administrative Trunking Encapsulation: dot1q
```

```
Operational Trunking Encapsulation: dot1q
```

```
Negotiation of Trunking: Disabled
```

```
Access Mode VLAN: 0 ((Inactive))
```

```
Trunking Native Mode VLAN: 1 (default)
```

```
Trunking VLANs Enabled: 1,10,30,1002-1005
```

```
Trunking VLANs Active: 1,10,30
```

```
Pruning VLANs Enabled: 2-1001
```

```
Priority for untagged frames: 0
```

```
Override vlan tag priority: FALSE
```

```
Voice VLAN: none
```

```
Appliance trust: none
```

```
Self Loopback: No
```

```
wlan-cat3524xl-a#
```

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [VLAN の設定 \(アクセス ポイント コンフィギュレーション ガイド\)](#)
- [VLAN の設定 \(ブリッジ コンフィギュレーション ガイド\)](#)
- [トランキングに関するテクニカル サポート](#)
- [関連スイッチとの相互対話](#)
- [トランキングを実装するためのシステム要件](#)
- [ブリッジングの概要](#)
- [固定 ISR のワイヤレス認証種別の設定例](#)
- [SDM による固定 ISR のワイヤレス認証種別の設定例](#)
- [ISR と WEP 暗号化および LEAP 認証を使用するワイヤレス LAN 接続の設定例](#)
- [基本的な無線 LAN 接続の設定例](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)