

Cisco Aironet ワイヤレス装置との VLAN の併用

目次

[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](#)

[トラブルシューティング](#)

[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くものです。

- 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たものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分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場合、デバイスが接続されるポートは VLAN 1 のメンバです。そのデバイスの MAC アドレスは、VLAN 1 の一部です。単一のスイッチに複数の VLAN を定義することが可能で、ほとんどの Catalyst モデルのスイッチ ポートを、複数の VLAN のメンバとして設定できます。

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 である必要はありません。これにより、イーサネットスイッチは、802.1q タグが付加さ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を生成するようになります。

キープ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: AP ですべての VLAN を許可すると、特に大規模なネットワークでは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](#)

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

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。

[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 GUI から、> サービスにナビゲートする VLAN 『Services』 をクリックして下さい: 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。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。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。これをするために、Security > SSID Manager の順にクリックして下さい。注: VLAN SSID 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: SSID [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。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: 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

ツ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 GUI から、> サービスにナビゲートする VLAN 『Services』 をクリックして下さい: 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。これをするために、現在の VLAN リストから 『<new>』 を選択して下さい。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。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。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 マネージャから (セキュリティ > SSID マネージャ メニュー項目の下で、) SSID とネイティブ VLAN を関連付けて下さい。注: VLAN SSID VLAN SSID 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: SSID 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。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。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 SSID Dot11Radio
注: 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。この機能の情報に関しては、Cisco Aironet アクセスポイントに資料 *Cisco IOS* ソフトウェア コンフィギュレーション ガイドの [VLAN にユーザを割り当てるために RADIUS サーバを使用して](#) セクションを 12.4(3g)JA 及び 12.3(8)JEB 参照して下さい。

[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。この機能の情報に関しては、Cisco Aironet アクセスポイントのための資料 *Cisco IOS* ソフトウェア コンフィギュレーション ガイドの [ダイナミック モビリティ グループ 割り当てのための RADIUS サーバを使用して](#) セクションを、12.4(3g)JA 及び 12.3(8)JEB 参照して下さい。

[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にだけ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 インターフェイスにブリッジ 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:
`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`注:
`no bridge-group 1 source-learning`
`bridge-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、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](#)

スイッチを設定するためにアクセスポイントにランキングするために Catalyst OS を VLAN 実行するコマンド構文は dot1q および set trunk <module #/port #> <vlan リストの set trunk <module #/port #> > 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 ワイヤレス装置は Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル) をサポートしていません。そのため、スイッチでは DTP のネゴシエーション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、設定が正常に動作していることを確認します。

ワイヤレス装置の確認

- show vlan - アクセス ポイント上で現在設定されているすべての VLAN とその状態を表示します。 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 #> —ある特定のポートのトランクのステータスを表示する 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 ファーストイーサネット <module #/port #> は trunk** — 所定のインターフェイスのトランクのステータスを表示する
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、**show interface ファーストイーサネット <module #/port #> は switchport** — 所定のインターフェイスのトランクのステータスを表示する
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

現在のところ、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 認証を使用する無線 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](#)