CHAPTER 19

リピータ/スタンバイ アクセス ポイントおよびワークグループ ブリッジ モードの設定

この章では、アクセス ポイントをリピータ、ホット スタンバイ ユニット、またはワークグループ ブリッジとして設定する方法について説明します。

リピータ アクセス ポイントの概要

リピータ アクセス ポイントは有線 LAN には接続されません。インフラストラクチャの範囲を拡大したり、無線通信を妨げる障害物を回避したりするために、有線 LAN に接続されているアクセス ポイントの無線範囲内に配置されます。2.4 GHz 無線または 5 GHz 無線をリピータとして設定できます。2 つの無線を装備したアクセス ポイントでは、1 つの無線しかリピータにすることができません。もう 1 つの無線はシャットダウンするか、ルート、スキャナ、またはスペクトラム無線として設定する必要があります。

リピータは、別のリピータや、有線 LAN に接続されているアクセス ポイントにパケットを送信することによって、無線ユーザと有線 LAN との間でトラフィックを転送します。データは、クライアントに最高のパフォーマンスを提供するルートを経由して送信されます。アクセス ポイントをリピータとして設定した場合、アクセス ポイントのイーサネット ポートはトラフィックを転送しません。

複数のリピータ アクセス ポイントをチェーンとして設定することもできますが、リピータ チェーンの末端のクライアント デバイスのスループットは大幅に低下します。これは、それぞれのリピータが各パケットの受信と再送に同じチャネルを使用する必要があるため、チェーンに追加された各リピータのスループットが半分に減少することによります。

リピータのアクセス ポイントは、最適な接続を確立しているアクセス ポイントにアソシエートします。ただし、リピータがアソシエートするアクセス ポイントを指定することはできます。リピータとルート アクセス ポイント間に静的な特定のアソシエーションを設定すると、リピータのパフォーマンスが向上します。

リピータを設定するには、親（ルート）アクセス ポイントとリピータ アクセス ポイントの両方で Aironet 拡張機能を有効にする必要があります。Aironet 拡張機能はデフォルトで有効になっており、これらを使用すると、アクセス ポイントで、アソシエートされている Cisco Aironet クライアント デバイスの能力がより正確に認識されるようになります。Aironet 拡張機能を無効にすると、アクセス ポイントとシスコ以外のクライアント デバイス間の相互運用性が改善される場合があります。シスコ以外のクライアント デバイスでは、リピータ アクセス ポイントおよびリピータがアソシエートしているルート アクセス ポイントとの通信に問題が生じる場合があります。

SSID をアクセス ポイントとリピータとの間で使用するには、SSID で [Infrastructure SSID] オプションを有効にして、リピータ通信で AP を許可する必要があります。

インフラストラクチャ Service Set Identifier（SSID; サービス セット ID）はネイティブ VLAN に割り当てる必要があります。アクセス ポイントまたはワイヤレス ブリッジに複数の VLAN が作成されている場合、インフラストラクチャ SSID は非ネイティブ VLAN に割り当てできません。インフラストラクチャ SSID を非ネイティブ VLAN に設定すると、次のメッセージが表示されます。

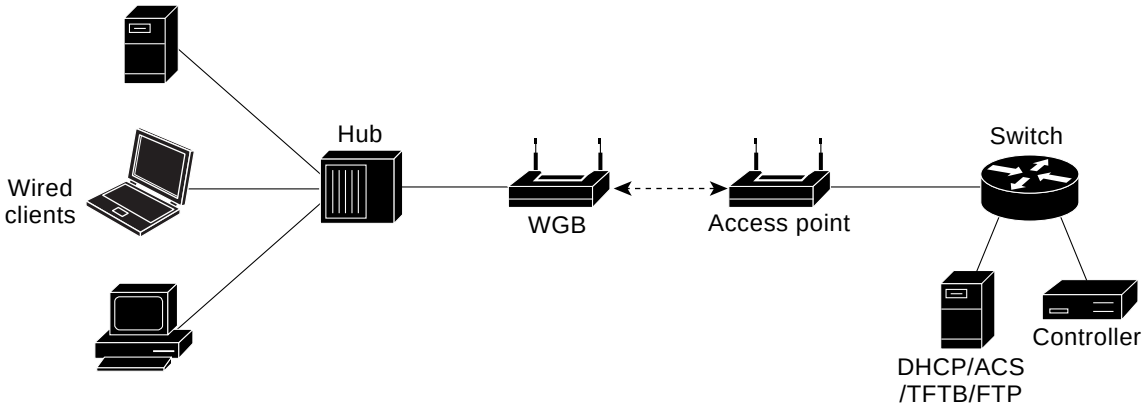
```
SSID [xxx] must be configured as native-vlan before enabling infrastructure-ssid
```

（注） アクセス ポイントは、各無線インターフェイスに対して仮想インターフェイスを生成するため、リピータ アクセス ポイントはルート アクセス ポイントに 2 回（実際のインターフェイスに 1 回、仮想インターフェイスに 1 回）アソシエートします。

（注） 無線は、リピータとして機能すると同時に他の SSID をサポートするよう設定することはできません。リピータ無線はネイティブ VLAN だけをリピートすることができます。無線をリピータとして設定した後、ネイティブ VLAN 以外の VLAN にマッピングされた SSID をその無線にマッピングすることはできません。ただし、もう 1 つの無線は複数の SSID と複数の VLAN をサポートするよう設定することができます。

図 19-1 は、リピータとして機能するアクセス ポイントを示しています。

図 19-1　リピータとしてのアクセス ポイント



リピータ アクセス ポイントの設定

この項では、アクセス ポイントをリピータとして設定する手順について、次の項目で説明します。

- デフォルト コンフィギュレーション（19-3 ページ）
- リピータのガイドライン（19-3 ページ）
- リピータの設定（19-4 ページ）
- リピータ操作の確認（19-6 ページ）
- アンテナの位置合わせ（19-6 ページ）
- リピータの EAP-FAST クライアントとしての設定（19-7 ページ）
- リピータの WPA2 クライアントとしての設定（19-6 ページ）

デフォルト コンフィギュレーション

アクセス ポイントは、デフォルトではルート ユニットとして設定されています。表 19-1 は、無線 LAN におけるアクセス ポイントの役割を制御する設定のデフォルト値を示しています。

表 19-1　無線 LAN での役割のデフォルト値

機能	デフォルト設定
ステーションの役割	ルート
親	none
拡張機能	Aironet

リピータのガイドライン

リピータ アクセス ポイントを設定する場合は、次のガイドラインに従います。

- 高いスループットを要求しないクライアント デバイスを構成する場合は、リピータを使用します。リピータは無線 LAN のカバレッジ領域を拡大しますが、スループットを大きく減少させます。
- リピータは、それにアソシエートするクライアント デバイスのすべて、または大半が Cisco Aironet クライアントの場合に使用します。他社のクライアントが予想される場合、それらのクライアントが Aironet IE 拡張をサポートすることを確認します。このオプションは、AP とリピータとの間の通信を許可するために SSID で必要です。
- リピータ アクセス ポイントに設定されたデータレートが、親アクセス ポイントのデータ レートと一致しているかどうか確認してください。データ レートの設定については、「無線データ レートの設定」セクション（6-12 ページ）を参照してください。
- リピータ無線で設定された SSID は、ネイティブ VLAN にマッピングする必要があります。

（注） Cisco IOS ソフトウェアを実行するリピータ アクセス ポイントは、Cisco IOS を実行しない親アクセス ポイントにアソシエートできません。

（注） リピータ アクセス ポイントは Wireless Domain Service（WDS; 無線ドメイン サービス）をサポートしません。リピータ アクセス ポイントを WDS 候補として設定しないでください。また、WDS アクセス ポイントを、イーサネット障害時にリピータ モードに戻るように設定しないでください。リピータは、必要なときにはいつでも WDS のインフラストラクチャに参加して WDS のクライアントとして機能できます。

（注） リピータの親として指定されているルート アクセス ポイント上で複数の Basic Service Set Identifier（BSSID）が設定されている場合、親アクセス ポイントで BSSID が追加または削除されると、親 MAC アドレスが変更される可能性があります。無線 LAN 上で複数の BSSID を使用し、無線 LAN 上のリピータが特定の親にアソシエートするように設定されている場合、親アクセス ポイント上で BSSID を追加または削除するときは、リピータのアソシエーションの状態を確認します。必要に応じて、アソシエートされていないデバイスを再設定して、BSSID の新しい MAC アドレスを使用するようにします。

リピータの設定

特権 EXEC モードから、次の手順に従ってアクセス ポイントをリピータとして設定します。

	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。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。
ステップ 3	**ssid** *ssid-string*	リピータがルート アクセス ポイントにアソシエートするときに使用する SSID をコールします。次の手順で、この SSID をインフラストラクチャ SSID に指定します。ルート アクセス ポイントにインフラストラクチャ SSID を作成している場合、リピータにも同じ SSID を作成します。 SSID をインフラストラクチャ SSID に指定します。リピータは、この SSID を使用してルート アクセス ポイントにアソシエートします。**optional** キーワードを入力している場合を除き、インフラストラクチャ デバイスはこの SSID を使用して、リピータ アクセス ポイントにアソシエートする必要があります。 インフラストラクチャ Service Set Identifier（SSID; サービス セット ID）はネイティブ VLAN に割り当てる必要があります。アクセス ポイントまたはワイヤレス ブリッジに複数の VLAN が作成されている場合、インフラストラクチャ SSID は非ネイティブ VLAN に割り当てできません。インフラストラクチャ SSID を非ネイティブ VLAN に設定すると、次のメッセージが表示されます。 `SSID [xxx] must be configured as native-vlan before enabling infrastructure-ssid`
ステップ 4	**station-role repeater**	アクセス ポイントの無線 LAN での役割をリピータに設定します。
ステップ 5	**dot11 extension aironet**	Aironet 拡張機能が無効になっている場合、Aironet 拡張機能を有効にします。

	コマンド	目的
ステップ 6	**parent** {*1-4*} *mac-address* [*timeout*]	(任意)リピータがアソシエートするアクセス ポイントの MAC アドレスを入力します。 • 最大 4 つの親アクセス ポイントの MAC アドレスを入力できます。このポイントには、1 ～ 4 の番号が指定されます。リピータは、必ずその親アクセス ポイントのリストからベストなアクセス ポイントにアソシエートしようとします。リピータは、「タイムアウト」オプションを設定しない限り、親リストにない MAC アドレスにはアソシエートしません。 (注)　複数の BSSID が親アクセス ポイント上で設定されている場合、親アクセス ポイントで BSSID が追加または削除されると、親 MAC アドレスが変更される可能性があります。 • (任意)タイムアウト値は秒単位で入力できますが、これはどれだけの時間、リピータがその親リストにあるアクセス ポイントとアソシエートしようとするかを決めています。このタイムアウト期間内にアソシエートできない場合、リピータは親リストにないアクセス ポイントにアソシエートしようとします。 0 ～ 65535 秒の範囲のタイムアウト値を入力できます。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**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。

3 つの潜在的な親アクセス ポイントをもつリピータ アクセス ポイントの設定例を次に示します。このアクセス ポイントには、1 ～ 3 の番号が指定されます。

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid chicago
AP(config-if)# station-role repeater
AP(config-if)# dot11 extension aironet
AP(config-if)# parent 1 0987.1234.h345
AP(config-if)# parent 2 7809.b123.c345
AP(config-if)# parent 3 6543.a456.7421
AP(config-if)# end
```

次の例は、1 つの親を親リストから除く方法を示しています。この例では、親 2 を除いています。

```
AP(config-if)# no parent 2
```

次に、親リストに 60 秒のタイムアウトを設定する例を示します。

```
AP(config-if)# parent timeout 60
```

次に、親リストでタイムアウト値をディセーブルにする方法の例を示します。

```
AP(config-if)# no parent timeout
```

アンテナの位置合わせ

アクセス ポイントをリピータとして設定するとき、**dot11 antenna-alignment** CLI コマンドを使用して、アクセス ポイントのアンテナを別のリモート アンテナと位置合わせできます。

コマンドによって位置合わせテストが開始します。無線は親からのアソシエーションが解除され、隣接する無線デバイスをプローブし、受け取る応答の MAC アドレスおよび信号強度を記録します。タイムアウトの後、無線は親と再アソシエートされます。

アンテナ位置合わせテストを実行する手順は、次のとおりです。

	コマンド	目的
ステップ 1	イネーブル化	特権 EXEC モードを開始します。
ステップ 2	**dot11 dot11radio** { **0** | **1** } **antenna-alignment timeout** *timeout-in-seconds*	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。 • 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 • 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。 • *timeout-in-seconds*: アンテナ位置合わせテストがタイムアウトする前に実行される時間を秒単位で入力します。デフォルト値は 5 秒です。

show dot11 antenna-alignment コマンドを使用すると、プローブに最後に応答した 10 台のデバイスの MAC アドレスおよび信号レベルをリストします。

リピータ操作の確認

リピータを設定した後、リピータが正しく動作している場合、ルート アクセス ポイントのアソシエーション テーブルで、リピータ アクセス ポイントはルート アクセス ポイントにアソシエートされて表示されます。

リピータの WPA2 クライアントとしての設定

WPA キー管理では暗号化方式を組み合わせて用い、クライアント デバイスとアクセス ポイントとの通信を保護します。リピータ アクセス ポイントを、他の WPA2 対応のクライアント デバイスと同様に、ネットワークで認証されるよう設定できます。

特権 EXEC モードから、次の手順に従ってリピータを WPA2 クライアントとして設定します。

	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	**ssid** *ssid-string*	SSID を無線インターフェイスにアソシエートします。
ステップ 3	**authentication open**	SSID 用の open 認証を有効にします。
ステップ 4	**authentication key-management wpa**	SSID 用の WPA 認証済みキー管理を有効にします。

	コマンド	目的
ステップ 5	**infrastructure ssid**	SSID を、リピータが他のアクセス ポイントにアソシエートするために使用する SSID として指定します。
ステップ 6	**wpa-psk** { **hex** | **ascii** } [**0** | **7**] *encryption-key*	リピータ用に事前共有キーを入力します。 16 進数または ASCII 文字を使用して、キーを入力します。16 進数を使用する場合は、256 ビット キーを完成するために 64 桁の 16 進数を入力する必要があります。ASCII を使用する場合は、8 ～ 63 個の ASCII 文字を入力する必要があります。アクセス ポイントがキーを展開します。
ステップ 7	**exit**	SSID 設定サブモードを終了します。
ステップ 8	**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。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。
ステップ 9	**encryption mode ciphers aes-ccm**	無線インターフェイスで AES CCMP 暗号化を有効にします。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**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。

リピータの EAP-FAST クライアントとしての設定

リピータ アクセス ポイントを、他の無線クライアント デバイスと同様に、ネットワークで認証されるよう設定できます。リピータ アクセス ポイントのネットワーク ユーザ名とパスワードを提供すると、ユーザのクレデンシャルを使用して、ルート AP によってネットワークで認証されるようにできます。

リピータを EAP-FAST またはその他の 802.1x/EAP 認証メソッド クライアントとして設定するには、3 つの主要な手順が必要です。

1. 認証サーバでリピータの認証ユーザ名とパスワードを作成します。
2. リピータがアソシエートするルート アクセス ポイントでサポートされるように認証メソッドを設定します。リピータがアソシエートするアクセス ポイントは、親アクセス ポイントと呼ばれます。認証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。

(注) リピータ アクセス ポイントでは、親アクセス ポイントで有効にしたものと同じ暗号スイートまたは WEP 暗号化方式と WEP 機能を有効にする必要があります。

3. 選択したメソッドでリピータが 802.1x/EAP クライアントとして機能するように設定します。次に、EAP-FAST コンフィギュレーションの例を示します。

	コマンド	目的
ステップ 1	**eap profile** *profile-name*	使用する認証方式を指定するためにリピータが使用するプロファイルの名前を入力します。
ステップ 2	**method fast**	使用するメソッドとして EAP-FAST を設定します。

	コマンド	目的
ステップ 3	**dot1x credentials** *name*	ワイヤレス インフラストラクチャでの認証にリピータが使用するユーザ クレデンシャルを設定します。
ステップ 4	**username** *user-name*	dot1x クレデンシャル内のユーザ名を設定します。
ステップ 5	**password 0** *password*	リピータがインフラストラクチャで認証されるときに使用するパスワードを設定します。
ステップ 6	**exit**	特権 EXEC モードに戻ります。
ステップ 7	**dot11 ssid** *ssid-name*	新しい SSID を作成します。
ステップ 8	**authentication open eap eap_methods**	Open+ EAP 認証を許可します（EAP-FAST またはその他）。
ステップ 9	**authentication network-eap eap_methods**	LEAP 認証を許可します。この例では、LEAP は最善の選択肢ではありませんが、LEAP はデフォルトのメソッドです。802.1x/EAP プロセスをトリガーするには、LEP をイネーブルにする必要があります。EAP プロファイルは、どの方式が実際に使用されるかを決定します。
ステップ 10	**authentication key-management wpa version 2**	キー管理を WPA バージョン 2 に設定します。
ステップ 11	**dot1x credentials** *name*	リピータがワイヤレス インフラストラクチャで認証されるときに作成される dot1x クレデンシャルを使用します。dot1x クレデンシャル プロファイルで定義されたクレデンシャルが使用されます。
ステップ 12	**dot1x eap profile EAP-only**	リピータがワイヤレス インフラストラクチャで認証されるときに上記で作成された EAP 専用プロファイルを使用します。eap プロファイルで定義されたメソッド（この例では EAP-FAST）が使用されます。
ステップ 13	**infrastructure ssid** [**optional**]	（任意）SSID を、他のアクセス ポイントおよびワークグループ ブリッジがこのアクセス ポイントにアソシエートするために使用する SSID として指定します。SSID をインフラストラクチャ SSID として指定しない場合、インフラストラクチャ デバイスはどの SSID を使用してもアクセス ポイントにアソシエートできます。SSID をインフラストラクチャ SSID として指定する場合、**optional** キーワードも入力する場合を除き、インフラストラクチャ デバイスはその SSID を使用してアクセス ポイントにアソシエートする必要があります。
ステップ 14	**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。 2.4 GHz 無線および 2.4 GHz 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 1 です。
ステップ 15	**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が、空白を使用できません。SSID では、大文字と小文字が区別されます。
ステップ 16	**end**	特権 EXEC モードに戻ります。
ステップ 17	**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。

ホット スタンバイの概要

ホットスタンバイ モードでは、アクセス ポイントが他のアクセス ポイントのバックアップとして指定されます。スタンバイ アクセス ポイントは、モニタするアクセス ポイントの近くに配置され、そのアクセス ポイントとまったく同じように設定する必要があります。スタンバイ アクセス ポイントは、モニタするアクセス ポイントにクライアントとしてアソシエートし、イーサネット ポートと無線ポートの両方からそのアクセス ポイントに対して IAPP クエリを送信します。モニタするアクセス ポイントから応答がない場合、スタンバイ アクセス ポイントはオンラインに切り替わり、そのアクセス ポイントの役割をネットワーク上で引き継ぎます。

スタンバイ アクセス ポイントの設定は、IP アドレスを除き、モニタするアクセス ポイントの設定と一致している必要があります。モニタするアクセス ポイントがオフラインになり、スタンバイ アクセス ポイントがネットワークでその役割を引き継ぐ場合、設定のマッチングによりクライアント デバイスは簡単にスタンバイ アクセス ポイントに切り替わります。

スタンバイ アクセス ポイントは、インターフェイスとインターフェイスの関係ではなく、デバイスとデバイスの関係として、別のアクセス ポイントをモニタします。たとえば、スタンバイ アクセス ポイントの 5 GHz 無線はアクセス ポイント alpha 内の 5 GHz 無線をモニタするように設定し、スタンバイの 2.4 GHz 無線はアクセス ポイント bravo 内の 2.4 GHz 無線をモニタするように設定するということはできません。また、デュアル無線のアクセス ポイント内の 1 つの無線をスタンバイ無線として設定し、もう 1 つの無線をクライアント デバイスに対応するように設定することもできません。

ホット スタンバイ モードはデフォルトでは、無効に設定されています。

(注) モニタするアクセス ポイントに障害が発生し、スタンバイ アクセス ポイントがその役割を引き継いだ場合は、モニタするアクセス ポイントを修復または交換する際に、スタンバイ アクセス ポイントのホットスタンバイを再度設定してください。スタンバイ アクセス ポイントは、自動的にはスタンバイ モードに戻りません。

(注) モニタするユニット上の BSSID が追加または削除されると、モニタするアクセス ポイントの MAC アドレスが変更される可能性があります。無線 LAN 上で複数の BSSID を使用する場合は、モニタするアクセス ポイント上で BSSID を追加または削除するときに、スタンバイ ユニットの状態を確認します。必要に応じて、スタンバイ ユニットを再設定して、BSSID の新しい MAC アドレスを使用するようにします。

(注) ホット スタンバイは、AP モードに設定されている BR1410 ではサポートされていません。

ホット スタンバイ アクセス ポイントの設定

スタンバイ アクセス ポイントを設定する場合、スタンバイ ユニットがモニタするアクセス ポイントの無線 MAC アドレスを入力する必要があります。2 つの無線でアクセス ポイントをモニタするには、両方の無線の MAC アドレスが必要です。スタンバイ アクセス ポイントを設定する前に、モニタするアクセス ポイントの MAC アドレスを記録してください。

スタンバイ アクセス ポイントでは、モニタするアクセス ポイントのいくつかの主要な設定を複製する必要があります。複製するのは次の設定です。

- プライマリ SSID（およびモニタするアクセス ポイントに設定された追加 SSID）
- デフォルト IP サブネット マスク
- デフォルト ゲートウェイ
- データ レート
- セキュリティ設定
- 認証タイプと認証サーバ
- 無線の設定と状態

スタンバイ アクセス ポイントを設定する前に、モニタするアクセス ポイントを確認し、設定を記録してください。

(注)　スタンバイ アクセス ポイントにアソシエートされている無線クライアント デバイスは、ホット スタンバイを設定している間、接続が切断されます。

ヒント　スタンバイ アクセス ポイント上でモニタするアクセス ポイントの設定をすばやく複製するには、モニタするアクセス ポイントの設定を保存して、それをスタンバイ アクセス ポイント上にロードします。コンフィギュレーション ファイルのアップロードとダウンロードの方法については、第 20 章「コンフィギュレーション ファイルの操作」を参照してください。

特権 EXEC モードから、次の手順に従ってアクセス ポイントでホット スタンバイ モードを有効にします。

	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	**iapp standby** *mac-address*	アクセス ポイントをスタンバイ モードに移行し、モニタするアクセス ポイントの無線の MAC アドレスを指定します。 (注)　2 つの無線を装備したアクセス ポイントで 2 つの無線を装備したアクセス ポイントをモニタするように設定する場合、モニタする 2.4 GHz 無線と 5 GHz 無線の両方の MAC アドレスを入力する必要があります。2.4 GHz 無線 MAC アドレスを最初に入力し、次に 5 GHz MAC アドレスが続きます。 (注)　モニタするユニット上の BSSID が追加または削除されると、モニタするアクセス ポイントの MAC アドレスが変更される可能性があります。無線 LAN 上で複数の BSSID を使用する場合は、モニタするアクセス ポイント上で BSSID を追加または削除するときに、スタンバイ ユニットの状態を確認します。必要に応じて、スタンバイ ユニットを再設定して、BSSID の新しい MAC アドレスを使用するようにします。 (注)　ホット スタンバイは、AP モードに設定されている BR1410 ではサポートされていません。

	コマンド	目的
ステップ 3	**iapp standby poll-frequency** *seconds*	スタンバイ アクセス ポイントが、モニタするアクセス ポイントの無線ポートとイーサネット ポートに送信するクエリの間隔を秒数で設定します。デフォルトのポーリング周期は 2 秒です。
ステップ 4	**iapp standby timeout** *seconds*	スタンバイ アクセス ポイントが、モニタするアクセス ポイントからの応答を待ち、動作不良だと判断するまでの時間を秒数で設定します。デフォルトのタイムアウト値は 20 秒です。 (注)　スタンバイ アクセス ポイントとモニタするアクセス ポイントの間のブリッジ パスが 20 秒よりも長い間失われる可能性がある場合（スパニングツリーの再計算中など）、スタンバイ タイムアウトの設定を延長する必要があります。 (注)　モニタするアクセス ポイントが、最も混雑の少ないチャネルを選択するように設定されている場合、スタンバイ タイムアウトの設定の延長が必要になる場合があります。モニタするユニットが最も混雑の少ないチャネルを選択するまで、最大で 40 秒かかる場合があります。
ステップ 5	**iapp standby primary-shutdown**	（任意）スタンバイ アクセス ポイントが、モニタするアクセス ポイントに Dumb Device Protocol（DDP）メッセージを送信し、スタンバイ ユニットが有効になったときに、モニタするアクセス ポイントの無線を無効にします。この機能によって、モニタするアクセス ポイントにアソシエートされているクライアント デバイスが、障害の発生したユニットにアソシエートしたままになることが回避できます。
ステップ 6	**show iapp standby-parms**	入力内容を確認します。アクセス ポイントがスタンバイ モードの場合、このコマンドにより、モニタするアクセス ポイントの MAC アドレス、ポーリング周期、タイムアウトの値などのスタンバイ パラメータが表示されます。アクセス ポイントがスタンバイ モード以外の場合、*no iapp standby mac-address* が表示されます。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**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。

スタンバイ モードを有効にした後、モニタするアクセス ポイントから記録した設定をスタンバイ アクセス ポイントの設定と一致するように変更します。

スタンバイ操作の確認

スタンバイ アクセス ポイントの状態を確認する場合は、次のコマンドを使用します。

show iapp standby-status

このコマンドは、スタンバイ アクセス ポイントのステータスを表示します。表 19-2 は、表示されるスタンバイ ステータス メッセージを示しています。

表 19-2　スタンバイ ステータス メッセージ

メッセージ	説明
IAPP Standby is Disabled	アクセス ポイントがスタンバイ モードに設定されていません。
IAPP—AP is in standby mode	アクセス ポイントがスタンバイ モードになっています。
IAPP—AP is operating in active mode	スタンバイ アクセス ポイントが、モニタするアクセス ポイントを引き継いでおり、ルート アクセス ポイントとして機能しています。
IAPP—AP is operating in repeater mode	スタンバイ アクセス ポイントが、モニタするアクセス ポイントを引き継いでおり、リピータ アクセス ポイントとして機能しています。
Standby status: Initializing	スタンバイ アクセス ポイントが、モニタするアクセス ポイントとのリンク テストを初期化しています。
Standby status: Takeover	スタンバイ アクセス ポイントがアクティブ モードに移行しています。
Standby status: Stopped	スタンバイ モードがコンフィギュレーション コマンドによって停止されました。
Standby status: Ethernet Linktest Failed	スタンバイ アクセス ポイントからモニタするアクセス ポイントへのイーサネット リンク テストが失敗しました。
Standby status: Radio Linktest Failed	スタンバイ アクセス ポイントからモニタするアクセス ポイントへの無線リンク テストが失敗しました。
Standby status: Standby Error	未定義のエラーが発生しました。
Standby State: Init	スタンバイ アクセス ポイントが、モニタするアクセス ポイントとのリンク テストを初期化しています。
Standby State: Running	スタンバイ アクセス ポイントがスタンバイ モードで動作しており、モニタするアクセス ポイントへのリンク テストを実行しています。
Standby State: Stopped	スタンバイ モードがコンフィギュレーション コマンドによって停止されました。
Standby State: Not Running	アクセス ポイントはスタンバイ モードではありません。

スタンバイ設定を確認する場合は、次のコマンドを使用します。

show iapp standby-parms

このコマンドは、スタンバイ アクセス ポイントの MAC アドレス、スタンバイ タイムアウト、ポーリング周期の値を表示します。スタンバイ アクセス ポイントが設定されていない場合、次のメッセージが表示されます。

```
no iapp standby mac-address
```

スタンバイ アクセス ポイントが、モニタするアクセス ポイントを引き継ぐ場合、スタンバイ アクセス ポイントが引き継いだ原因を特定するために **show iapp statistics** コマンドを使用できます。

ワークグループ ブリッジ モードの概要

アクセス ポイントをワークグループ ブリッジ(WGB)として設定できます。ワークグループ ブリッジ(WGB)モードのアクセス ポイントは、別のアクセス ポイントにクライアントとしてアソシエートして、イーサネット ポートに接続されたデバイスをネットワークに接続します。たとえば、ネットワーク プリンタのグループを無線で接続する必要がある場合は、プリンタをハブまたはスイッチに接続し、ハブまたはスイッチをアクセス ポイントのイーサネット ポートに接続し、そのアクセス ポイントをワークグループ ブリッジとして設定します。ワークグループ ブリッジはネットワーク上のアクセス ポイントにアソシエートします。

アクセス ポイントに 2 つの無線がある場合、ワークグループ ブリッジ モードで、2.4 GHz 無線または 5 GHz 無線のいずれかが機能します。一方の無線インターフェイスをワークグループ ブリッジとして設定すると、他方の無線はアップ状態のままになります。ただし、両方の無線が同時にワークグループ ブリッジとして機能するようには設定できません。他方の無線はディセーブル(シャットダウン)にするか、ルート(アクセス ポイントまたはブリッジ)、スキャナ、またはスペクトル モードにできます。

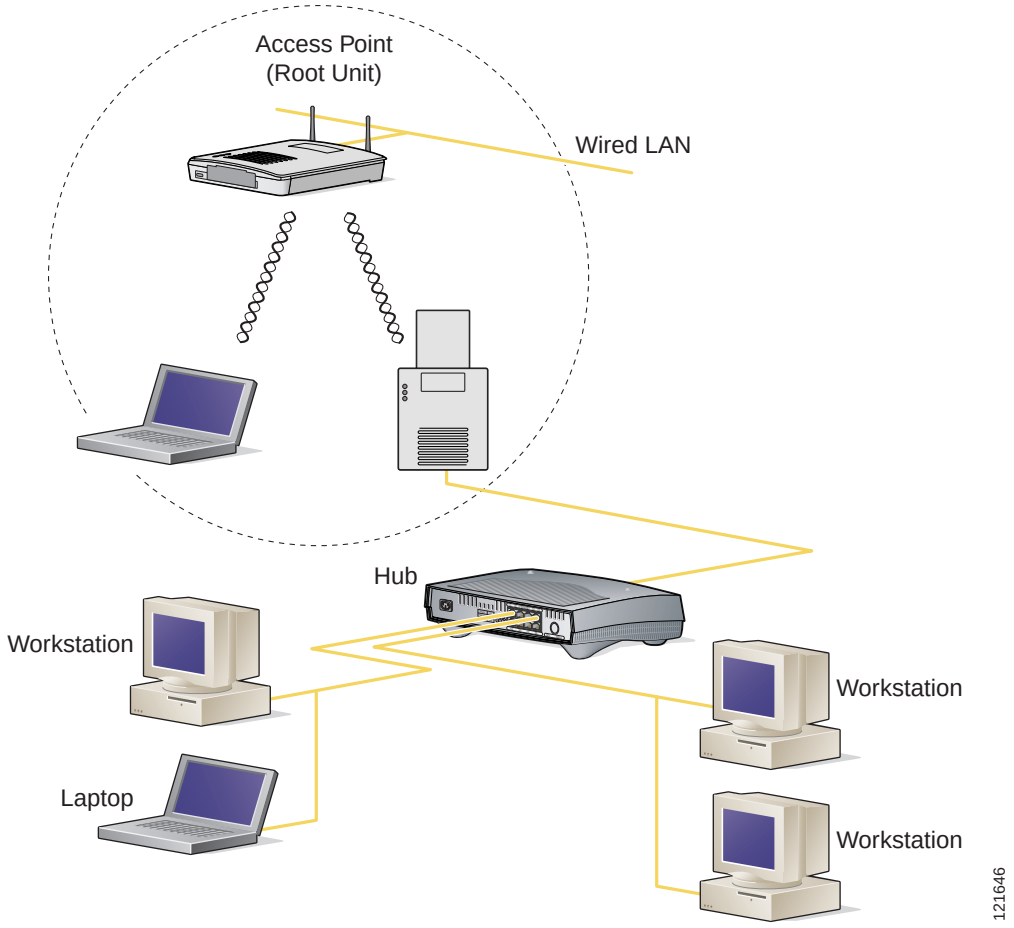
注意　ワークグループ ブリッジ モードのアクセス ポイントでイーサネットポートを有線 LAN に接続すると、ブリッジ ループが発生することがあります。ネットワークのブリッジ ループを防止するには、ワークグループ ブリッジとして設定する前または設定後すぐにワークグループ ブリッジを有線 LAN から切断します。

(注)　ワークグループ ブリッジの親として指定されているルート アクセス ポイント上で複数の BSSID が設定されている場合、親アクセス ポイントで BSSID が追加または削除されると、親 MAC アドレスが変更される可能性があります。無線 LAN 上で複数の BSSID を使用し、無線 LAN 上のワークグループ ブリッジが特定の親にアソシエートするように設定されている場合、親アクセス ポイント上で BSSID を追加または削除するときは、ワークグループ ブリッジのアソシエーションの状態を確認します。必要に応じて、ワークグループ ブリッジを再設定して、BSSID の新しい MAC アドレスを使用するようにします。

(注)　ワークグループ ブリッジ モードでのアクセス ポイントは、ブリッジとして機能はしますが、無線範囲が限定されています。ワークグループ ブリッジは、数キロにわたって通信するようにワイヤレス ブリッジを設定できる、**distance** 設定をサポートしていません。

図 19-2 は、ワークグループ ブリッジ モードのアクセス ポイントを示しています。

図 19-2　ワークグループ ブリッジ モードのアクセス ポイント



インフラストラクチャ デバイスまたはクライアント デバイスとしてのワークグループ ブリッジの扱い

ワークグループ ブリッジがアソシエートするアクセス ポイントは、そのワークグループ ブリッジをインフラストラクチャ デバイスまたは単にクライアント デバイスとして扱うことができます。デフォルトでは、アクセス ポイントやブリッジはワークグループ ブリッジをクライアント デバイスとして扱います。

信頼性を向上させるために、ワークグループ ブリッジをクライアント デバイスとしてではなく、アクセス ポイントやブリッジと同じインフラストラクチャ デバイスとして扱うように、アクセス ポイントとブリッジを設定できます。ワークグループ ブリッジがインフラストラクチャ デバイスとして扱われる場合、アクセス ポイントはアドレス解決プロトコル（ARP）パケットなどのマルチキャスト パケットを、確実にワークグループ ブリッジに配信します。ワークグループ ブリッジをインフラストラクチャ デバイスとして扱うようにアクセス ポイントとブリッジを設定するには、設定インターフェイス コマンド **infrastructure-client** を使用します。

ワークグループ ブリッジをクライアント デバイスとして扱うようにアクセス ポイントとブリッジを設定すると、より多くのワークグループ ブリッジが同じアクセス ポイントにアソシエートできます。つまり、より多くのワークグループ ブリッジが、インフラストラクチャ SSID ではない SSID を使用してアソシエートできます。信頼性の高いマルチキャスト配信のパフォーマンス コストのため(マルチキャスト パケットが各ワークグループ ブリッジに二重に送信されるので)、アクセス ポイントまたはブリッジにアソシエートできるワークグループ ブリッジなどのインフラストラクチャ デバイスの数は制限されます。アクセス ポイントにアソシエートできるワークグループ ブリッジの数を 21 以上にするには、アクセス ポイントがマルチキャスト パケットをワークグループ ブリッジに配信するときの信頼性を低くする必要があります。信頼性が低くなると、アクセス ポイントはマルチキャスト パケットが目的のワークグループ ブリッジに到達したかどうか確認できず、アクセス ポイントのカバレッジ領域の端にあるワークグループ ブリッジの有線クライアントは、すべてのマルチキャスト フレームを受信しない可能性があります。ワークグループ ブリッジをクライアント デバイスとして扱うと、パフォーマンスは向上しますが、信頼性は低くなります。ワークグループ ブリッジを単なるクライアント デバイスとして扱うようにアクセス ポイントとブリッジを設定するには、設定インターフェイス コマンド **no infrastructure client** を使用します。これがデフォルト設定です。

ワークグループ ブリッジに接続されたデバイスが、アクセス ポイントまたはブリッジと同等のネットワークに対する信頼性を必要とする場合には、ワークグループ ブリッジをインフラストラクチャ デバイスとして使用する必要があります。次の条件を満たす場合には、ワークグループ ブリッジをクライアント デバイスとして使用します。

- 同じアクセス ポイントまたはブリッジに 20 台を超えるワークグループ ブリッジがアソシエートする。
- ワークグループ ブリッジがインフラストラクチャ SSID ではない SSID を使用してアソシエートする。
- ワークグループ ブリッジがモバイルである。

ワークグループ ブリッジがアソシエートされているアクセス ポイントに **(no) infrastructure client** コマンドが入力されることに注意してください。このコマンドは、アクセス ポイントが各マルチキャスト フレームのユニキャスト コピーを追加するために、セル内の各ワークグループ ブリッジへ信頼性のある方式(確認応答のあるユニキャスト)で送信するかどうかを判断します。

インフラストラクチャ クライアントがアクセス ポイントで設定されている場合、各ワークグループ ブリッジはマルチキャスト初期フレームとユニキャスト コピーの両方を受信する可能性があります。両方のフレーム(同じ上位層内容がある)を処理すると、ワークグループ ブリッジでの処理が非効率になります。マルチキャスト フレームを考慮してユニキャスト コピーを破棄するか(デフォルト)、ユニキャスト フレームを考慮してマルチキャスト ソースのフレームを廃棄するようにワークグループ ブリッジを設定できます。ワークグループ ブリッジ無線でこの動作を設定するには、コマンド **station-role workgroup-bridge multicast mode {client | infrastructure}** を使用します。クライアント オプションでは、マルチキャスト フレームを考慮して、ユニキャスト コピーを破棄します。インフラストラクチャ オプションでは、メイン アクセス ポイントのインフラストラクチャ クライアント設定を反映し、マルチキャスト フレームのユニキャスト コピーを考慮してマルチキャスト フレームを処理しないようにワークグループ ブリッジを設定します。

ローミング用ワークグループ ブリッジの設定

デフォルトでは、ワークグループ ブリッジは静的です。そのため、アクセス ポイント SSID にアソシエートされると、他のアクセス ポイントをスキャンしません。

ワークグループ ブリッジがモバイルの場合、親アクセス ポイントやブリッジへのより良好な無線接続をスキャンするように設定できます。ワークグループ ブリッジをモバイル ステーションとして設定するには、次のコマンドを使用します。

ap(config)# **mobile station**

この設定を有効にすると、Received Signal Strength Indicator（RSSI; 受信信号強度表示）の数値が低い、電波干渉が多い、またはフレーム損失率が高いことが検出された場合に、ワークグループ ブリッジは新しい親アソシエーションをスキャンします。これらの基準を使用して、モバイル ステーションとして設定されたワークグループ ブリッジは新しい親アソシエーションを検索し、現在のアソシエーションが失われる前に新しい親にローミングします。モバイル ステーションの設定が無効の場合（デフォルトの設定）、ワークグループ ブリッジは現在のアソシエーションを失った後で新しいアソシエーションを検索します。

ap(config-if)**#mobile station minimum-rate <data rate>**

これは、WGB が新しいローミング イベントをいつ開始するかを制御するための設定可能なパラメータです。この CLI が設定され、現在のデータ レートが設定値より小さい場合、新しいローミング プロセスが開始されます。これにより不要なローミングが減り、所要のレート値が得られます。

また、スキャンの周期を設定することもできます。接続状態が低下した場合、ワークグループ ブリッジは、接続するより良いアクセス ポイントをスキャンします。ワークグループ ブリッジがスキャンによってより良い接続ポイントを見つけられない場合、**mobile station period** *number-of-seconds* コマンドを使って次のスキャン サイクルまでの周期を特定します。

限定チャネル スキャン用のワークグループ ブリッジの設定

鉄道などのモバイル環境では、ワークグループ ブリッジはすべてのチャネルをスキャンする代わりに、限定チャネルのセットのみのスキャンに制限されます。こうすることで、ワークグループ ブリッジのローミングが 1 つのアクセス ポイントから別のアクセス ポイントに切り替わるとき、ハンドオフによる遅延が減少します。ワークグループ ブリッジがスキャンするチャネル数を必要な数に限定することによって、モバイル ワークグループ ブリッジで高速かつスムーズなローミングが可能な継続的な無線 LAN 接続が実現されて維持されます。

限定チャネル セットの設定

この限定チャネル セットは、**mobile station scan <set of channels>** CLI コマンドを使用して設定し、すべてのチャネルまたは指定されたチャネルのスキャンを開始します。設定できるチャネルの最大数に制限はありません。設定できるチャネルの最大数は、無線がサポートできるチャネル数だけに制限されます。スキャンを実行すると、ワークグループ ブリッジは、この限定チャネル セットだけをスキャンします。この限定チャネル機能は、ワークグループ ブリッジが現在アソシエートされているアクセス ポイントから受け取る既知のチャネル リストにも影響します。チャネルが既知のチャネル リストに追加されるのは、チャネルが限定チャネル セットに含まれる場合に限られます。

次の例は、コマンドを使用する方法を示しています。この例では、チャネル 1、6、および 11 がスキャンに指定されています。

```
ap#
ap#confure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#int d0
ap(config-if)#ssid limited_scan
ap(config-if)#station-role workgroup-bridge
ap(config-if)#mobile station
ap(config-if)#mobile station scan 1 6 11
ap(config-if)#end
ap#
```

no mobile station scan コマンドを使用すると、すべてのチャネルのスキャンが復元されます。

CCX ネイバー リストの無視

さらにワークグループ ブリッジは、AP Adjacent レポートや Enhanced Neighbor List レポートなどの CCX レポートを使用して、既知のチャネル リストを更新します。ただし、ワークグループ ブリッジが限定チャネル スキャンに設定されている場合、CCX レポートを処理して既知のチャネル リストを更新する必要がありません。**mobile station ignore neighbor-list** コマンドを使用して、CCX 近接リスト レポートの処理を無効にします。このコマンドは、ワークグループ ブリッジが限定チャネル スキャンに設定されている場合だけ有効です。次の例は、このコマンドを使用する方法を示しています。

```
ap#
ap#confure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#int d0
ap(config-if)#mobile station ignore neighbor-list
ap(config-if)#end
```

クライアント VLAN の設定

ワークグループ ブリッジのイーサネット ポートに接続されたデバイスをすべて特定の VLAN に割り当てる必要がある場合、接続されたデバイスに対して VLAN を設定できます。ワークグループ ブリッジで、次のコマンドを入力します。

```
ap(config)# workgroup-bridge client-vlan vlan-id
```

ワークグループ ブリッジのイーサネット ポートに接続されたデバイスが、すべてこの VLAN に割り当てられます。

ワークグループ ブリッジの VLAN タギング

ワークグループ ブリッジ（WGB）の VLAN タギング機能を使用すると、Unified WGB ソリューションに対する VLAN 数に基づいた VLAN トラフィックの分離がイネーブルになります。

この機能がイネーブルの場合、VLAN クライアントから無線 LAN コントローラ（WLC）へのパケットの送信中に、WGB が 802.1q ヘッダーを削除します。WGB は、802.1q ヘッダーなしで VLAN クライアントに向かうパケットを取得します。WGB の背後にあるスイッチにフレームを転送する場合は、802.1q ヘッダーを追加するように、WGB コードを変更する必要があります。

WGB は、Internet Access Point Protocol（IAPP）アソシエーション メッセージの有線クライアント VLAN 情報で WLC を更新します。WLC は WGB クライアントを VLAN クライアントとして扱い、送信元 MAC アドレスに基づき正しい VLAN インターフェイスにパケットを転送します。

アップストリーム方向では、WGB はパケットから 802.1q ヘッダーを削除すると同時にパケットを WLC に送信します。ダウンストリーム方向では、WLC は有線クライアントを接続するスイッチにパケットを転送しながら、802.1q タグなしで、そのパケットを WGB に送信します。WGB は、宛先 MAC アドレスに基づき、4 バイトの 802.1q ヘッダーを追加します。（VLAN の詳細については、第 14 章「VLAN の設定」を参照してください）。

次のコマンドを入力して、WGB の VLAN タギングを有効にします。

```
WGB(config)#workgroup-bridge unified-vlan-client ?
       -replicate  Enable WGB broadcast to all vlans
       <cr>
```

ワークグループ ブリッジ モードの設定

特権 EXEC モードから、次の手順に従ってアクセス ポイントをワークグループ ブリッジとして設定します。

	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	**station-role workgroup-bridge** [**universal** *mac-address*]	ワークグループ ブリッジに無線の役割を設定します。 (任意) ワークグループ ブリッジとして設定された場合、アクセス ポイントは特定のメッセージをプライマリ アクセス ポイントに送信し、ワークグループ ブリッジ無線経由でリレーされた有線クライアントの MAC アドレスについて通知します。プライマリ アクセス ポイントがシスコのアクセス ポイントでない場合、これらのメッセージは認識されません。 ワークグループ ブリッジがシスコ以外のアクセス ポイントと正常にアソシエートおよび通信できるようにするには、**universal** オプション引数を使用します。このモードでは、1 つの有線クライアントだけがサポートされるという制限があります。 このモードを設定する場合、ワークグループ ブリッジ経由でトラフィックがリレーされる有線クライアントの MAC アドレスを設定する必要があります。プライマリ AP に有線クライアント リストを送信する代わりに、ワークグループ ブリッジは有線クライアントの MAC アドレスを使用してアクセス ポイントに直接アソシエートします。有線クライアントの MAC アドレスがワークグループ ブリッジの MAC アドレス テーブルにない場合、ワークグループ ブリッジは独自の MAC アドレスを使用してアソシエートします。その後、有線クライアントが接続され、MAC アドレスがワークグループ ブリッジ MAC アドレス テーブルに表示されると、WGB は有線クライアントの MAC アドレスを使用してアソシエーションを解除し、再アソシエートします。このプロセスは、無線クライアントと MAC アドレスとの間で固有のマッピングが必要なシスコ以外のアクセス ポイントをサポートします。

	コマンド	目的
ステップ 4	**station-role workgroup-bridge multicast mode {client | infrastructure}**	(任意)プライマリ アクセス ポイントが **infrastructure client** コマンドで設定された場合、マルチキャスト フレームもユニキャスト経由でワークグループ ブリッジに送信されます。このような場合、ユニキャスト経由でリレーされるマルチキャスト フレームには、ヘッダーに次の 4 つの MAC アドレスがあります。ワークグループ ブリッジ ユニキャスト宛先 MAC アドレス、送信アクセス ポイント MAC アドレス、マルチキャスト宛先 MAC アドレス、元の送信者の送信元 MAC アドレス。 元のマルチキャスト フレーム ヘッダーには、マルチキャスト宛先 MAC アドレス、送信アクセス ポイント MAC アドレス、元の送信者の送信元 MAC アドレスの 3 つの MAC アドレスだけが含まれます。 プライマリ アクセス ポイントで **infrastructure client** コマンドを使う場合、ステーション ロール ワークグループ ブリッジ マルチキャスト モード インフラストラクチャを使って、マルチキャスト フレームを無視し、マルチキャスト フレームのリレーされたユニキャスト コピーだけを処理するようワークグループ ブリッジに指示します。ステーション ロール ワークグループ ブリッジ マルチキャスト モード クライアントを使って、標準フレームのみを考慮し、ヘッダーに 4 つの MAC アドレスが表示されるリレーされたフレームは無視するようワークグループ ブリッジに指示します。 • クライアント クライアント モードは、3 MAC アドレス ヘッダー マルチキャスト パケットだけを受け入れます • インフラストラクチャ インフラストラクチャ モードは、4 MAC アドレス ヘッダー マルチキャスト パケットだけを受け入れます
ステップ 5	**ssid** *ssid-string*	親アクセス ポイントまたはブリッジにアソシエートするためにワークグループ ブリッジが使用する SSID を指定します。
ステップ 6	**infrastructure-ssid**	SSID をインフラストラクチャ SSID に指定します。 (注)　ワークグループ ブリッジは、ルート アクセス ポイントまたはブリッジにアソシエートするために、インフラストラクチャ SSID を使用する必要があります。
ステップ 7	**authentication client username** *username* **password** *password*	(任意)親アクセス ポイントが LEAP 認証を必要とするように設定されている場合、ワークグループ ブリッジが LEAP 認証を実行するときに使用するユーザ名とパスワードを設定します。このユーザ名とパスワードは、認証サーバでワークグループ ブリッジに設定したユーザ名とパスワードに一致する必要があります。
ステップ 8	**exit**	SSID コンフィギュレーション モードを終了し、無線インターフェイス コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 9	**parent** {*1-4*} *mac-address* [*timeout*]	(任意) ワークグループ ブリッジがアソシエートするアクセス ポイントの MAC アドレスを入力します。 • 最大 4 つの親アクセス ポイントの MAC アドレスを入力できます。このポイントには、1 ～ 4 の番号が指定されます。ワークグループ ブリッジは、必ずその親アクセス ポイントのリストからベストなアクセス ポイントにアソシエートしようとします。ワークグループ ブリッジは、「タイムアウト」オプションを設定しない限り、親リストにない MAC アドレスにはアソシエートしません。 (注)　複数の BSSID が親アクセス ポイント上で設定されている場合、親アクセス ポイントで BSSID が追加または削除されると、親 MAC アドレスが変更される可能性があります。 • (任意) タイムアウト値は秒単位で入力できますが、これはどれだけの時間、ワークグループ ブリッジがその親リストにあるアクセス ポイントとアソシエートしようとするかを決めています。このタイムアウト期間内にアソシエートできない場合、ワークグループ ブリッジは親リストにないアクセス ポイントにアソシエートしようとします。0 ～ 65535 秒の範囲のタイムアウト値を入力できます。
ステップ 10	**mobile station**	(任意) ワークグループ ブリッジをモバイル ステーションとして設定します。 この設定を有効にすると、Received Signal Strength Indicator (RSSI; 受信信号強度表示) の数値が低い、電波干渉が多い、またはフレーム損失率が高いことが検出された場合に、ワークグループ ブリッジは新しい親アソシエーションをスキャンします。この設定が無効の場合 (デフォルトの設定)、ワークグループ ブリッジは現在のアソシエーションを失った後で新しいアソシエーションを検索します。
ステップ 11	**mobile station period** *number-of-seconds*	(任意) ワークグループ ブリッジがアソシエートされているアクセス ポイントへの信号が低下した場合、ワークグループ ブリッジは代替アクセス ポイントをスキャンします。このスキャンに失敗した場合 (より良い信号のアクセス ポイントが見つからなかった場合)、ここで入力した秒数は次のスキャンの試行までの間隔となります。
ステップ 12	**mobile station minimum-rate** *rate*	(任意) ワークグループ ブリッジが代替アクセス ポイントをスキャンする場合、このコマンドは、ワークグループ ブリッジが代替アクセス ポイントを接続ポイントの候補として考慮するために、新しいアクセス ポイントで達成する必要がある最小データ レートを指定します。
ステップ 13	**mobile station scan**	(任意) ワークグループ ブリッジが代替アクセス ポイントを探すためにスキャンするチャネル リストを制限します。
ステップ 14	**mobile station ignore neighbor-list**	(任意) スキャンされたチャネルのリストを制限するようワークグループ ブリッジが設定されている場合、このコマンドは、候補となるネイバー アクセス ポイントおよびチャネルを示す CCX ネイバー リストのメッセージを無視するようワークグループ ブリッジに指示します。

	コマンド	目的
ステップ 15	**exit**	無線コンフィギュレーション モードを終了し、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 16	**workgroup-bridge client-vlan** *vlan-id*	(任意)ワークグループ ブリッジのイーサネット ポートに接続されたデバイスを割り当てる VLAN を指定します。
ステップ 17	**end**	特権 EXEC モードに戻ります。
ステップ 18	**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、アクセス ポイントをワークグループ ブリッジとして設定する方法を示しています。この例では、ワークグループ ブリッジは設定されたユーザ名とパスワードを使用して LEAP 認証を実行し、イーサネット ポートに接続されたデバイスが VLAN 22 に割り当てられます。

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# station-role workgroup-bridge
AP(config-if)# ssid infra
AP(config-ssid)# infrastructure-ssid
AP(config-ssid)# authentication client username wgb1 password cisco123
AP(config-ssid)# exit
AP(config-if)# exit
AP(config)# workgroup-bridge client-vlan 22
AP(config)# end
```

次の例は、1 および 2 の番号が指定された親アクセス ポイントを持つワークグループ ブリッジの設定方法を示しています。

```
AP(config-if)# parent 1 0040.9631.81cf
AP(config-if)# parent 2 0040.9631.81da
```

次の例は、1 つの親を親リストから除く方法を示しています。この例では、親 2 を除いています。

```
AP(config-if)# no parent 2
```

次に、親リストに 60 秒のタイムアウトを設定する例を示します。

```
AP(config-if)# parent timeout 60
```

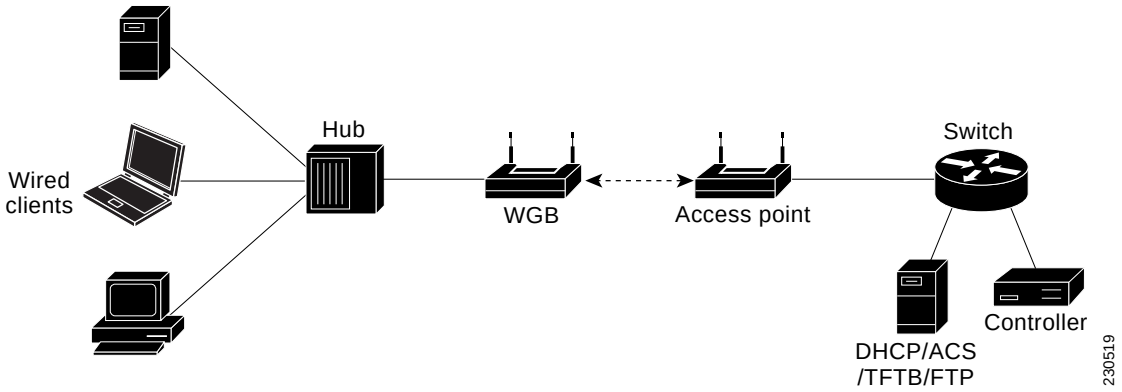
次に、親リストでタイムアウト値をディセーブルにする方法の例を示します。

```
AP(config-if)# no parent timeout
```

Lightweight 環境でのワークグループ ブリッジの使用

アクセス ポイントをワークグループ ブリッジとして動作するように設定することで、アクセス ポイントはワークグループ ブリッジ アクセス ポイントにイーサネットで接続されているクライアントの代理として Lightweight アクセス ポイントへの無線接続を提供できます。ワークグループ ブリッジは、イーサネット インターフェイス側にある有線クライアントの MAC アドレスを学習し、Internet Access Point Protocol(IAPP; インターネット アクセス ポイント プロトコル)メッセージングを使用して、MAC アドレスを Lightweight アクセス ポイントに報告します。この方法によって、単一の無線セグメントを介して有線ネットワークに接続します。ワークグループ ブリッジは、Lightweight アクセス ポイントへの単一の接続を確立することで、有線クライアントへの無線アクセス接続を提供します。Lightweight アクセス ポイントはワークグループ ブリッジを無線クライアントとして扱います。

図 19-3　Lightweight 環境でのワークグループ ブリッジ



(注)　Lightweight アクセス ポイントに障害が発生した場合、ワークグループ ブリッジは別のアクセス ポイントへのアソシエートを試行します。

ワークグループ ブリッジを Lightweight 環境で使用する際のガイドライン

ワークグループ ブリッジを Lightweight ネットワークで使用する場合は、次のガイドラインに従います。

- ワークグループ ブリッジは、ワークグループ ブリッジ モードをサポートし、Cisco IOS Release JA 以降（32 MB アクセス ポイント）または Cisco IOS Release 12.3(8)JEB 以降（16MB アクセス ポイント）を実行する任意の自律アクセス ポイントを使用できます。これらのアクセス ポイントには、AP1040、AP1140、および AP1260 が含まれます。12.4(3g)JA および 12.3(8)JEB よりも前の Cisco IOS リリースはサポートされません。

(注)　アクセス ポイントに 2 つの無線がある場合、1 つだけをワークグループ ブリッジ モードに設定できます。この無線は Lightweight アクセス ポイントへの接続に使用されます。2 番目の無線を無効にすることをお勧めします。

ワークグループ ブリッジでワークグループ ブリッジ モードを有効にするには、次のいずれかを実行します。

- ワークグループ ブリッジ アクセス ポイント GUI にある [Network] > [Network Interfaces] > [Radio0-802.11N 2.4 GHz / Radio1-802.11N 5 GHz] > [Settings] ページで、無線ネットワークのロールとして [Workgroup Bridge] を選択します。
  または、WGB アクセス ポイント CLI 無線コンフィギュレーション サブモードで、次のコマンドを入力します：**station-role workgroup-bridge**
- ワークグループ ブリッジはクライアント モード（デフォルト値）だけがサポートされます。Lightweight アクセス ポイントは、アソシエートされたワークグループ ブリッジにユニキャスト方式でマルチキャスト フレームをリレーしません。ワークグループ ブリッジのクライアント モードを有効にするには、次のいずれかを実行します。

  - 無線コンフィギュレーション ページで、ワークグループ ブリッジへの信頼性のあるマルチキャスト パラメータで [Disabled] を選択します。
  - 無線コンフィギュレーション サブモードから、次のコマンドを入力します：**no infrastructure client**.
- ワークグループ ブリッジでは次の Lightweight 機能の使用がサポートされています。
  - ゲスト N+1 冗長性
  - ローカル EAP
- ワークグループ ブリッジでは次の Lightweight 機能の使用はサポートされません。
  - Cisco Centralized Key Management（CCKM）
  - ハイブリッド REAP
  - アイドル タイムアウト
  - Web 認証

(注)　ワークグループ ブリッジが Web 認証 WLAN にアソシエートする場合、ワークグループ ブリッジは除外リストに追加され、ワークグループ ブリッジの有線クライアントのすべてが削除されます。

- メッシュ ネットワークでは、ワークグループ ブリッジはその役割がルート アクセス ポイントかメッシュ アクセス ポイントかに関係なく、すべてのメッシュ アクセス ポイントにアソシエートできます。
- ワークグループ ブリッジに接続する有線クライアントは、セキュリティが認証されません。その代わり、ワークグループ ブリッジがアソシエートするアクセス ポイントに対してワークグループ ブリッジが認証されます。したがって、ワークグループ ブリッジの有線側は物理的に保護することを推奨します。
- レイヤ 3 ローミングで、ワークグループ ブリッジのローミングが別のコントローラ（外部コントローラなど）に切り替わった後にワークグループ ブリッジ ネットワークに有線クライアントを接続する場合、有線クライアントの IP アドレスはアンカー コントローラだけに表示され、外部コントローラには表示されません。
- ワークグループ ブリッジの記録をコントローラから削除すると、ワークグループ ブリッジの有線クライアントの記録もすべて削除されます。
- ワークグループ ブリッジに接続されている有線クライアントは、ワークグループ ブリッジの QoS および AAA オーバーライド属性を継承します。
- ワークグループ ブリッジに接続されている有線クライアントでは、次の機能がサポートされません。
  - MAC フィルタリング
  - リンク テスト
  - アイドル タイムアウト
- コントローラに何も設定しなくても、ワークグループ ブリッジと Lightweight アクセス ポイントとの通信を有効にできます。ただし、適切な通信を確保するには、ワークグループ ブリッジに設定された SSID およびセキュリティ方式と一致する WLAN をコントローラに作成する必要があります。

サンプル ワークグループ ブリッジ アソシエーションの確認

ワークグループ ブリッジがアクセス ポイントにアソシエートしていることを確認するには、ワークグループ ブリッジで次のコマンドを入力します。

show dot11 association

有線クライアントがトラフィックを長期間送信しない場合、トラフィックがその有線クライアントに連続して送信されている場合でも、ワークグループ ブリッジはそのクライアントをブリッジ テーブルから削除します。その結果、有線クライアントへのトラフィック フローに障害が発生します。トラフィックの損失を避けるには、有線クライアントがブリッジ テーブルから削除されないようにします。これを行うには、ワークグループ ブリッジで次の IOS コマンドを使用して、ワークグループ ブリッジのエージアウト タイマーを大きな値に設定します。

```
configure terminal
bridge bridge-group-number aging-time seconds
exit
end
```

bridge-group-number は 1 ～ 255 の値、seconds は 10 ～ 1,000,000 秒の値です。seconds パラメータを有線クライアントのアイドル時間の値よりも大きく設定することをお勧めします。

ワークグループ ブリッジでの VideoStream サポートの有効化

VideoStream は、無線経由でユニキャスト フレームにマルチキャスト フレームを変換することによって、IP マルチキャスト ストリームの信頼性を向上させます。Cisco IOS Release 15.2(2)JA 以降では、ワークグループ ブリッジに接続された有線デバイス向けに VideoStream サポートを提供しています。リリース 15.2(2)JA 以降を実行しているアクセス ポイントに関しては、ワークグループ ブリッジが無線 LAN コントローラ(WLC)のマルチキャスト テーブルに追加され、そのワークグループ ブリッジは VideoStream ユニキャスト フレームをイーサネット マルチキャスト フレームに変換して、それを有線クライアントに送信します。

ワークグループ ブリッジの VideoStream を有効にするには、WLC で次のコマンドを入力します。

config media-stream wired-client enable

高速ローミングのためのワークグループ ブリッジの設定

高速鉄道の車両など、ワークグループ ブリッジ AP の高速ローミングが関係するワイヤレス ネットワークの導入について考えてみます。車両が移動すると、車両のワークグループ ブリッジ AP は 1 つの親 AP(ルート AP)から線路に沿ってマウントされている次の 親 AP に移動します。このようなシナリオでは、約 100 km/h で走行する列車が関係する場合もあり、親 AP は線路で 200～300 m の間隔で配置されています。

このようなシナリオでは、次のように設定されていることを確認します。

(注)　高速ローミングのシナリオに対応するワークグループ ブリッジの設定がサポートされているのは、Cisco Aironet 3600 および 3700 シリーズ アクセス ポイントと、IW3700 シリーズ アクセス ポイントのみです。

ワイヤレス コントローラでの 802.11v BSS 遷移

高速ローミングが機能するには、ワイヤレス コントローラで、802.11v BSS 遷移をイネーブルにする必要があります。これにより、ワークグループ ブリッジ AP はアソシエートされた AP（現在の親 AP）からネイバー リストを要求して受信できるようになります。ワークグループ ブリッジ AP はこのリストを使って、次の親 AP を見つけるためにスキャンする必要がある一部のチャネルを識別します。

WGB での設定

範囲から遠ざかる際に、現在の親 AP が最適でないことを WGB がどれだけ素早く検出するか、また次の親 AP を検出するためにローミングを開始する必要があることを設定するには、次のコマンドを使用します。
drssi roaming threshold *value* **period** *value* **packet** *value* **neighlist-update-interval** *value*

このコマンドは次のような特徴を持ちます。

- DRSSI ローミングしきい値は RSSI しきい値です。このしきい値を超える RSSI 値を持つ AP はアソシエーション対象として考慮されません。

  DRSSI ローミングしきい値は、線路上の 2 つの AP の中間点における平均 RSSI レベルよりも約 2 ～ 3 dBm 低くすることが推奨されています。設定済みのしきい値 x は -x dBm に対応します。
- period は、現在の親へのリンクの品質を WGB が評価する頻度を制御します。たとえば、列車が高速で移動している場合、WGB がより頻繁にリンクの品質を評価するように設定します。ただし、速度が遅い場合、WGB はリンクの品質評価の頻繁な計算を回避します。
- packet は、AP とのリンク品質を追跡するために WGB が使用する現在のルート AP のサンプル データ パケットのしきい値です。WGB AP は、ルート AP から最後に受信したデータ パケットの RSSI の継続的な平均を保持します。この継続的な平均がしきい値を下回る場合、WGB はローミングを開始します。たとえば、列車が高速で移動している場合、少数のサンプルを使ってスイッチするタイミングを判断できます。
- neighlist-update-interval は、ローミングの WGB ネイバー リストを更新する時間間隔です。これは、アソシエートされた AP に対する定期的な dot11v クエリをその AP のネイバー リストでトリガーするため使用されます。1 ~ 10000（秒単位）の値を入力できます。デフォルトは 10 秒です。

次の例のように、100 km/h までであれば、DRSSI のローミングしきい値 67、period 値 1、packet 値 20 の設定で問題なく機能します。

```
ap#confure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)#int d0
ap(config-if)#drssi roaming threshold 67 period 1 packet 20
ap(config-if)#end
```

また、次のコマンドを使用して、最後にアソシエートされた AP から受信したネイバー リストのみをスキャンするようワークグループ ブリッジを設定することもできます。
drssi scan-only current-neighbor-list

上記のコマンドをディセーブルにして、ワークグループ ブリッジがネイバー リストを徐々にエージ アウトするようにすることもできます。エージ アウト要因はローミングごとに 1 つずつ削減されます。デフォルトのエージは 2 です。ディセーブルにするには、コマンド **no drssi scan-only current-neighbor-list** を使用します。

（注）　**mobile station** コマンドまたは **drssi** コマンドを使用してローミングを設定できます。両方のコマンドを同時に設定しないでください。

debug コマンドおよび show コマンド

WGB で、現在のネイバー リストのテーブルを表示するには、次のコマンドを使用します:
show dot11 bss-trans neighbor-list

WGB で、802.11v BSS 遷移のデバッグをイネーブルにするには、次のコマンドを使用します:
debug dot11 dot11v {detail | errors | all}

PROFINET トラフィックの透過転送の設定

PROFINET は PROFIBUS International（PI）のオープンな工業イーサネット標準であり、オートメーション コントロール用に TCP/IP および IT 標準を使用しています。PROFINET は工業オートメーション システムとプロセス制御ネットワークで特に有用です。PROFINET はデータ交換を重視しており、速度要件に合った通信パスを定義しています。

PROFINET 通信は、次の 3 つの点でスケーラブルです。

- 標準の非リアルタイム通信では TCP/IP を使用し、約 100 ms のバス サイクル タイムが実現されます。ダウンロード、診断、および管理に使用されます。
- リアルタイム（RT）：リアルタイム通信では、約 10 ms のサイクル タイムが実現されます。トラフィック、タイム クリティカルなアラーム メッセージの制御に使用されます。リアルタイム データは、TCP（UDP）/IP データよりも高い優先度で処理されます。標準の既存プロトコル コンポーネントを使用して（特殊フレーム etherType = 0x8892 を含むイーサネットと VLAN タグに含まれる優先順位値を使用）確定的および巡回型のデータ転送を実現します。
- 等時間隔のリアルタイム（IRT）：等時間隔のリアルタイム通信では、約 1 ms のサイクル タイムが実現されます。IRT の主な目的は、正確に制御された通信を必要とする通信の「タイミング」です。これは、特別なハードウェアおよび IEEE 1588 PTP プロトコルを使用して実現されます。IRT はこのマニュアルの範囲外です。

PROFINET I/O は、分散型オートメーション アプリケーション用のモジュラ通信フレームワークです。PROFINET I/O は巡回型のデータ転送を使用して、プログラマブル コントローラ、入力/出力（I/O）装置、およびその他のオートメーション コントローラ（モーション コントローラなど）とデータ、アラーム、診断情報を交換します。

この機能により、IW3700 シリーズではワイヤレス経由で透過的な PROFINET RT トラフィックを転送できます。この機能により、PROFINET サービス クラス（CoS）値を含む PROFINET RT トラフィックを Wi-Fi ネットワーク経由で透過的にリレーできます。

（注）　FlexConnect モードと Autonomous モードの両方がこの機能でサポートされます。

図 19-4 は、自律 AP および WGB 設定のトポロジを示しています。

自律 AP には 2 つの vlan が設定されています。ネイティブ vlan（vlan 0）は、自律 AP の接続に使用されます。IE スイッチと自律 AP 間の PROFINET パケットは vlan x で転送されます。ワイヤレス PROFINET トラフィックは、CoS 値に基づいて、対応するアクセス カテゴリ（AC）キュー内に置かれます。WGB は IO デバイスに直接接続します。ダウンストリームはタグなしで、アップストリーム は vlan 0 を使用して CoS の優先順位を表します。

図 19-4　自律 AP（ルート AP および WGB）

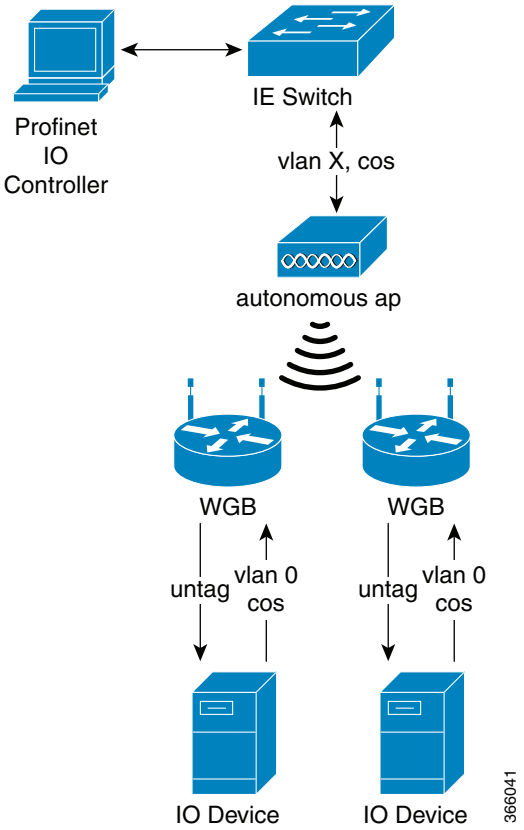
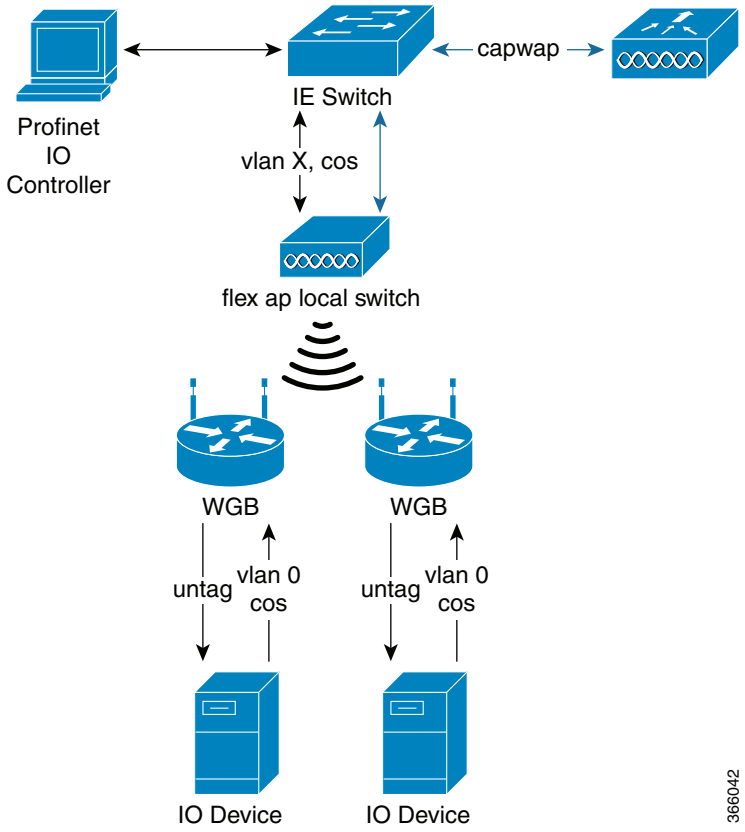


図 19-5 は、ユニファイド AP ローカル スイッチング設定のトポロジを示しています。WLC は capwap パケットによって AP と通信して制御メッセージを交換します。緑色の線と矢印は、Profinet データ フローです。黒い線と矢印は、capwap 制御パケット フローです。

図 19-5　ユニファイドAP ローカル スイッチング



設定例

このセクションでは、自律 AP と WGB の設定例を示します。次の例では、ネイティブ vlan 201 が制御メッセージに使用されます。vlan 203 は Profinet に使用されます。

自律 AP の設定

自律 AP を設定するには、次の手順を実行します。

ステップ 1　vlan 203 で ssid #Profinet を作成します。

```
ap(config)#dot11 ssid #Profinet
ap(config-ssid)#vlan 203
ap(config-ssid)#authentication open
ap(config-ssid)#authentication key-management wpa version 2
ap(config-ssid)#wpa-psk ascii 0 12345678
ap(config-ssid)#exit
```

ステップ 2　ssid #Profinet を dot11 5 G に合わせます。

```
ap(config)#interface d1
ap(config-if)#encryption vlan 203 mode ciphers aes-ccm
ap(config-if)#ssid #Profinet
ap(config-if)#station-role root
```

ステップ 3　vlan ブリッジを作成します。

```
ap(config)#interface Dot11Radio1.201
ap(config-subif)#encapsulation dot1Q 201 native
ap(config-subif)#exit

ap(config)#interface Dot11Radio1.203
ap(config-subif)#encapsulation dot1Q 203
ap(config-subif)#bridge-group 203
ap(config-subif)#exit

ap(config)#interface GigabitEthernet0.201
ap(config-subif)#encapsulation dot1Q 201 native
ap(config-subif)#exit

ap(config)#interface GigabitEthernet0.203
ap(config-subif)#encapsulation dot1Q 203
ap(config-subif)#bridge-group 203
ap(config-subif)#exit
```

WGB の設定

次の手順に従い、WGB を設定します。

ステップ 1　ネイティブ vlan で ssid #Profinet を作成します。

```
wgb(config)#dot11 ssid #Profinet
wgb(config-ssid)#authentication open
wgb(config-ssid)#authentication key-management wpa version 2
wgb(config-ssid)#wpa-psk ascii 0 12345678
wgb(config-ssid)#exit
```

ステップ 2　ssid #Profinet を dot11 に合わせます。

```
wgb(config)#interface d1
wgb(config-if)#encryption mode ciphers aes-ccm
wgb(config-if)#ssid #Profinet
```

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。