



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。2.4GHz 無線または 5GHz 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せん。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
```



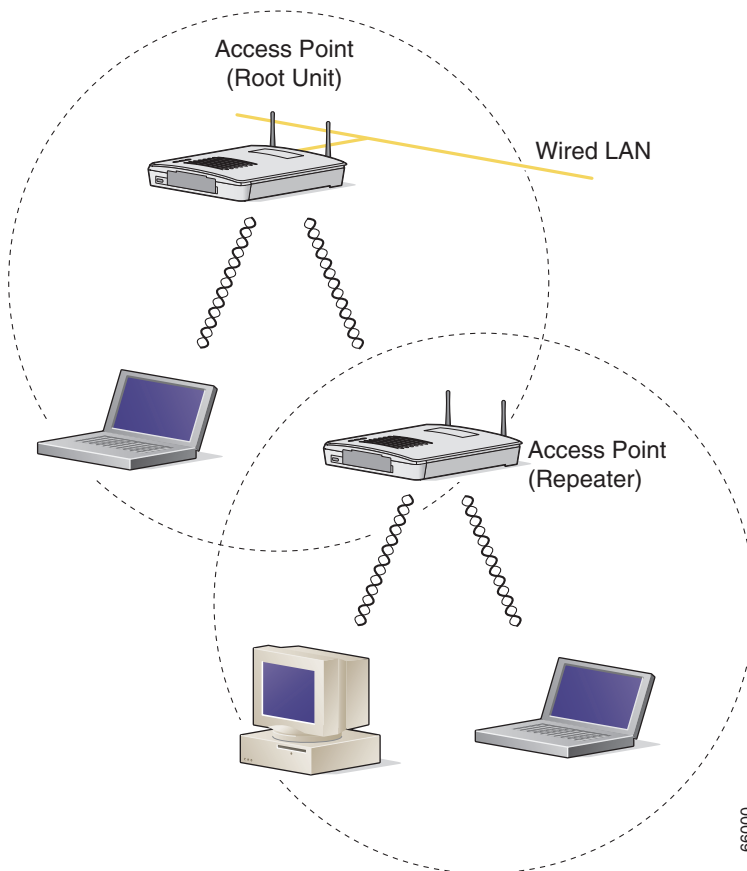
(注) アクセス ポイントは、各無線インターフェイスに対して仮想インターフェイスを生成するため、リピータ アクセス ポイントはルート アクセス ポイントに 2 回 (実際のインターフェイスに 1 回、仮想インターフェイスに 1 回) アソシエートします。



(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 だけをリピータ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



66000

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(6-8 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、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	<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 コンフィギュレーション モードを開始します。 2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 3	<code>ssid ssid-string</code>	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

	コマンド	目的
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。
ステップ 6	parent {1-4} mac-address [timeout]	<p>(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。</p> <ul style="list-style-type: none"> 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。 <p>(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。</p> <ul style="list-style-type: none"> (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。 <ul style="list-style-type: none"> 2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5 GHz 無線および 5GHz 802.11n 無線は 1 です。 <i>timeout-in-seconds</i>: 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る用い、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。 2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 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なります。

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。

■ アンテナの位置合わせ

	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 クレデンシアルを設定します。
ステップ 4	username user-name	dot1x クレデンシア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時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時に作成される dot1x クレデンシアルを使用します。dot1x クレデンシアル プロファイルで定義されたクレデンシアルが使用されます。
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時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 デバイスはこの 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。 2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 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 5GHz 無線はアクセスポイント alpha 内の 5GHz 無線をモニタするように設定し、スタンバイの 2.4GHz 無線はアクセスポイント bravo 内の 2.4GHz 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。

■ ホットスタンバイ アクセス ポイントの設定

- 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	<p>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。</p> <p>(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 2.4GHz 無線と 5GHz 無線の両方の MAC アドレスを入力する必要があります。2.4GHz 無線 MAC アドレスを最初に入力し、次に 5GHz MAC アドレスが続きます。</p> <p>(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 ユニットの状態を確認して、BSSID の新しい MAC アドレスを使用するようにします。</p> <p>(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。</p>

コマンド	目的
ステップ3 iapp standby poll-frequency <i>seconds</i>	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 <i>seconds</i>	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(スパン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ン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ン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、 <i>no iapp standby mac-address</i> 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、2.4GHz 無線または5GHz 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)、スキュナ、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。

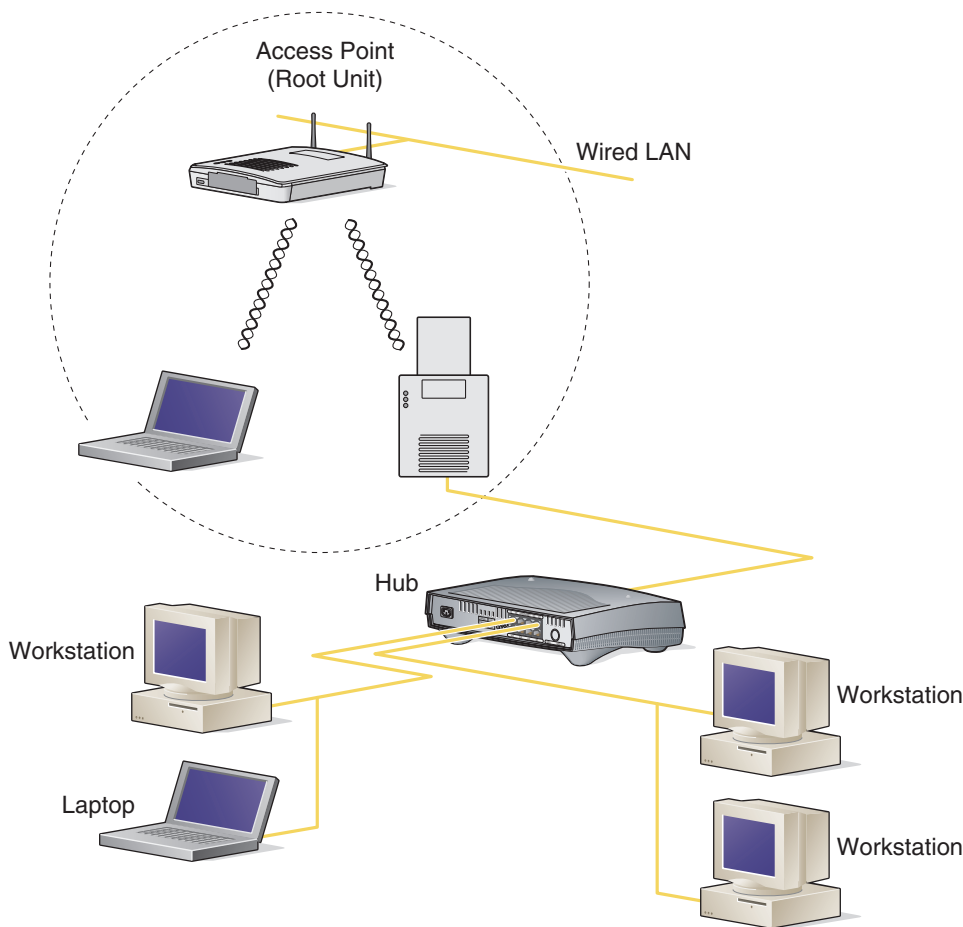


(注)

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



121646

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** コマンドを使用して次のスキャン 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時、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]	<p>ワークグループブリッジに無線の役割を設定します。</p> <p>(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。</p> <p>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。</p> <p>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。</p>

コマンド	目的
ステップ 4 station-role workgroup-bridge multicast mode {client infrastructure}	<p>(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。</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> 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	<p>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。</p>
ステップ 6 infrastructure-ssid	<p>SSIDをインフラストラクチャSSIDに指定します。</p> <p>(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。</p>
ステップ 7 authentication client username username password password	<p>(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。</p>
ステップ 8 exit	<p>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。</p>

コマンド	目的
ステップ 9 parent {1-4} <i>mac-address</i> [<i>timeout</i>]	<p>(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。</p> <ul style="list-style-type: none"> 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。 <p>(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。</p> <ul style="list-style-type: none"> (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	<p>(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。</p> <p>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。</p>
ステップ 11 mobile station period <i>number-of-seconds</i>	<p>(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。</p>
ステップ 12 mobile station minimum-rate <i>rate</i>	<p>(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。</p>
ステップ 13 mobile station scan	<p>(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ンネル リストを制限します。</p>
ステップ 14 mobile station ignore neighbor-list	<p>(任意) スキャンされたチャン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ンネルを示す 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。</p>

	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
```

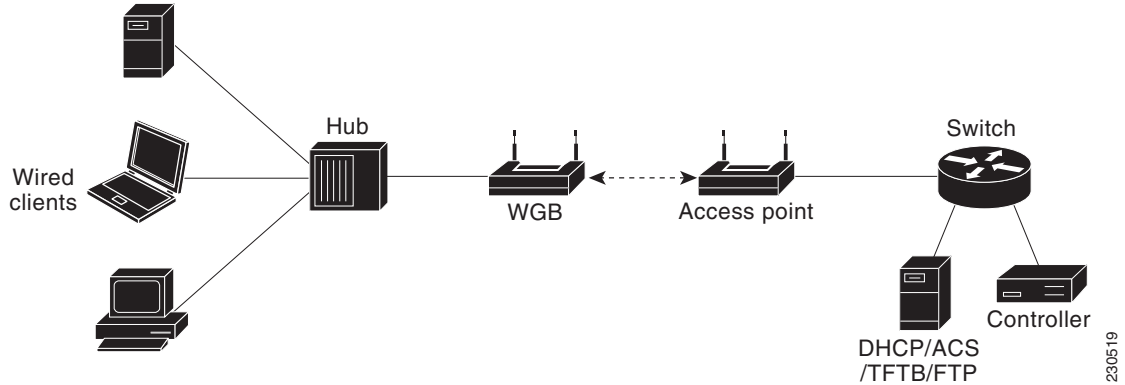
次に、親リストでタイムアウト値をディセーブルにする方法の例を示します。

```
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 (32MB 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 2.4GHz / Radio1-802.11N 5GHz] > [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。その代わりに、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、無線経路でユニキャスト 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 200~300m 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ンネルを識別します。

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

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。

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。

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}

■ 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

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。