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。この章で説明する内容は、次のとおりです。

- 「リピータ アクセス ポイントの概要」（P.19-2）
- 「リピータ アクセス ポイントの設定」（P.19-3）
- 「ホット スタンバイの概要」（P.19-9）
- 「ホット スタンバイ アクセス ポイントの設定」（P.19-10）
- 「ワークグループ ブリッジ モードの概要」（P.19-14）
- 「ワークグループ ブリッジ モードの設定」（P.19-18）
- 「Lightweight 環境でのワークグループ ブリッジ」（P.19-19）

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 種類の無線が設定されたアクセス ポイントでは、片方の無線だけをリピータに指定でき、もう一方の無線はルート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。

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。

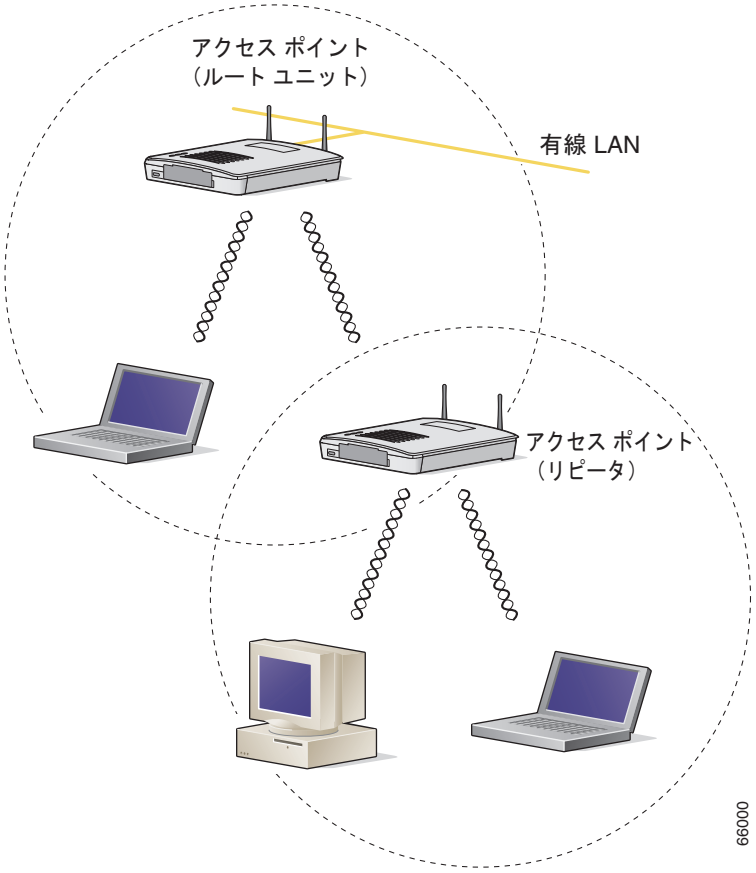
```
SSID [xxx] must be configured as native-vlan before enabling infrastructure-ssid
```

（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） リピータ アクセス ポイントには複数の VLAN を設定できません。リピータ アクセス ポイントはネイティブ VLAN だけをサポートします。

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」（P.19-4）
- 「リピータのガイドライン」（P.19-4）
- 「リピータの設定」（P.19-5）
- 「リピータ操作の確認」（P.19-7）
- 「アンテナの位置合わせ」（P.19-6）
- 「リピータの LEAP クライアントとしての設定」（P.19-7）
- 「リピータの WPA クライアントとしての設定」（P.19-8）

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	なし
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。シスコ以外のクライアント デバイスを使用すると、リピータ アクセス ポイントとの通信に問題が生じる可能性があります。
- 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」（P.6-7）を参照してください。
- リピータ アクセス ポイントはネイティブ VLAN だけをサポートします。リピータ アクセス ポイントには複数の VLAN を設定できません。

（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 モードに戻るように設定しないでください。

（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。 2.4GHz 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	**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 を作成します。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。
ステップ 4	**infrastructure-ssid** [**optional**]	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 5	**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。
ステップ 6	**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 7	**dot11 extensions 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 8	**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。リピータは、まず MAC アドレス 1 へのアソシエートを試行します。そのアクセス ポイントが応答しない場合、リピータは親リストで次のアクセス ポイントとのアソシエーションを試みます。 （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、つまりリピータが親アクセス ポイントとのアソシエーションを試みてから、リストの次の親とのアソシエーションを試みるまでの間隔を秒で入力できます。タイムアウト値は 0 ～ 65535 秒の範囲で入力します。
ステップ 9	**end**	特権 EXEC モードに戻ります。
ステップ 10	**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、3 つの親アクセス ポイントを使用してリピータ アクセス ポイントを設定する方法を示しています。

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid chicago
AP(config-ssid)# infrastructure-ssid
AP(config-ssid)# exit
AP(config-if)# station-role repeater
AP(config-if)# dot11 extensions aironet
AP(config-if)# parent 1 0987.1234.h345 900
AP(config-if)# parent 2 7809.b123.c345 900
AP(config-if)# parent 3 6543.a456.7421 900
AP(config-if)# end
```

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** }	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	**antenna-alignment** *timeout*	アンテナ位置合わせテストを実行するタイムアウトまでの時間を秒数で設定します。デフォルトは 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 アクセス ポイントの上部の LED を確認します。リピータが正常に機能している場合、リピータとリピータがアソシエートするルート アクセス ポイントの LED は、次のように表示されます。

- ルート アクセス ポイントのステータス LED が緑色に点灯し、少なくとも 1 つのクライアント デバイスが（この場合はリピータに）アソシエートされていることを示します。
- リピータ アクセス ポイントのステータス LED は、リピータ アクセス ポイントがルート アクセス ポイントにアソシエートされていて、さらにそのリピータ アクセス ポイントにクライアント デバイスがアソシエートされている場合、緑色に点灯します。リピータ アクセス ポイントがルート アクセス ポイントにアソシエートされていても、クライアント デバイスがリピータ アクセス ポイントにアソシエートされていなければ、ステータス LED は 7/8 秒 :1/8 秒の比率で点滅を繰り返します。

リピータ アクセス ポイントは、ルート アクセス ポイントのアソシエーション テーブルにも、アソシエートされているデバイスとして表示されます。

リピータの LEAP 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入力すると、リピータはシスコの無線認証方法である Light Extensible Authentication Protocol（LEAP; 拡張認証プロトコル）を使用してネットワークで認証され、動的な Wired Equivalent Privacy（WEP）キーを受け取ります。

リピータを LEAP クライアントとして設定する場合、次の 3 つの手順が必要です。

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 ポイントに、LEAP 認証を設定します。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. LEAP クライアントとして機能するようにリピータを設定します。特権 EXEC モードから、次の手順に従ってリピータを LEAP 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	**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 3	**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 4	**authentication network-eap** *list-name*	リピータで LEAP 認証を有効にして、LEAP が有効なクライアント デバイスがリピータを通じて認証されるようにします。list-name には、Extensible Authentication Protocol（EAP; 拡張認証プロトコル）認証に使用するリスト名を指定します。EAP および MAC アドレスのリスト名は、**aaa authentication login** コマンドを使用して定義します。これらのリストは、ユーザがログインしたときに有効となる認証方式を定義し、認証情報が保存された場所を間接的に識別します。
ステップ 5	**authentication client username** *username* **password** *password*	リピータが 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、認証サーバでリピータ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 6	**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 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。

リピータの WPA 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 WPA 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 WPA 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	**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 3	**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。SSID では、大文字と小文字が区別されます。
ステップ 4	**authentication open**	SSID 用の open 認証を有効にします。
ステップ 5	**authentication key-management wpa**	SSID 用の WPA 認証済みキー管理を有効にします。
ステップ 6	**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 7	**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 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**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。

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 MAC アドレスを入力する必要があります。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
- WEP 設定
- 認証タイプと認証サーバ

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、「コンフィギュレーション ファイルの操作」（P.20-9）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 種類の無線を装備した 1200 シリーズ アクセス ポイントで 2 種類の無線を装備した 1200 シリーズ 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。 **（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。
ステップ 3	**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 4	**ssid** *ssid-string*	スタンバイ アクセス ポイントがモニタするアクセス ポイントにアソシエートするときに使用する SSID を作成します。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。モニタするアクセス 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、スタンバイ アクセス ポイントにも同じ SSID を作成します。
ステップ 5	**infrastructure-ssid** [**optional**]	SSID をインフラストラクチャ SSID に指定します。スタンバイはこの SSID を使用して、モニタするアクセス ポイントにアソシエートします。モニタするアクセス ポイントの役割をスタンバイ アクセス ポイントが引き継ぐ場合、**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 を使用してスタンバイ 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 6	**authentication client username** *username* **password** *password*	モニタするアクセス 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、スタンバイ アクセス ポイントが 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、認証サーバでスタンバイ アクセス ポイント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 7	**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 8	**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 9	**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 10	**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 11	**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 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**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

1100、1130、1200、1230、1240、および 1250 シリーズのアクセス ポイントは、ワークグループ ブリッジとして設定できます。ワークグループ ブリッジ 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。1 つ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、別の無線インターフェイスは有効なままになります。

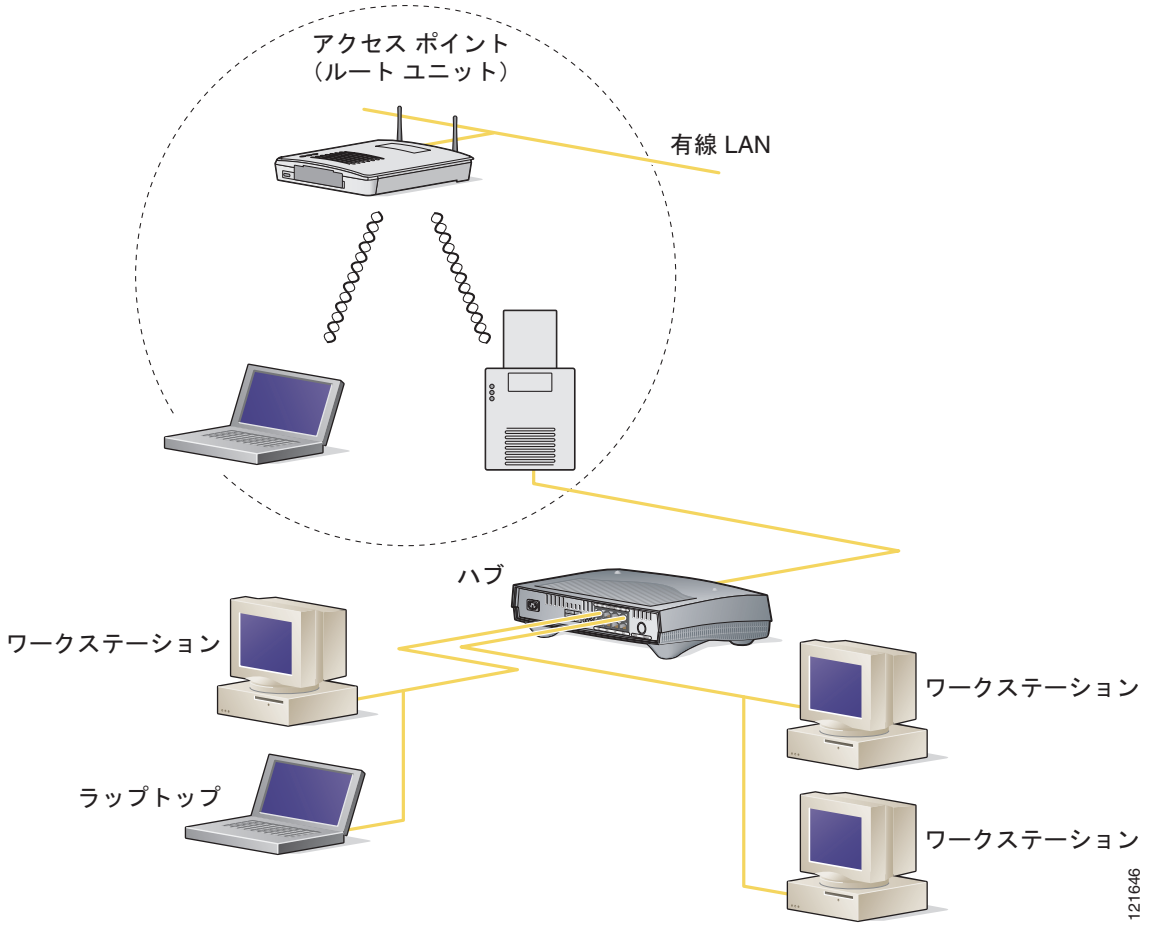
注意　ワークグループ ブリッジ モードのアクセス ポイントでイーサネットポートを有線 LAN に接続すると、ブリッジ ループが発生することがあります。ネットワークのブリッジ ループを防止するには、ワークグループ ブリッジとして設定する前または設定後すぐにワークグループ ブリッジを有線 LAN から切断します。

（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を確認できなくなるため、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 ブリッジでは IP 接続が失われる可能性があります。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。

ローミング用ワークグループ ブリッジの設定

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。

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 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**	ワークグループ ブリッジに無線の役割を設定します。アクセス ポイントに 2 つの無線が組み込まれている場合、ワークグループ ブリッジ モードに設定されていない無線は、自動的に無効になります。
ステップ 4	**ssid** *ssid-string*	ワークグループ ブリッジが親アクセス ポイントまたはブリッジへのアソシエーションに使用する SSID を作成します。
ステップ 5	**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 6	**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 7	**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。
ステップ 8	**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。ワークグループ ブリッジはまず MAC アドレス 1 へのアソシエートを試行します。そのアクセス ポイントが応答しない場合、ワークグループ ブリッジは親リストで次のアクセス ポイントとのアソシエーションを試みます。 **（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、つまりワークグループ ブリッジが親アクセス ポイントとのアソシエーションを試みてから、リストの次の親とのアソシエーションを試みるまでの間隔を秒で入力できます。タイムアウト値は 0 ～ 65535 秒の範囲で入力します。
ステップ 9	**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。

	コマンド	目的
ステップ 10	**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 11	**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 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**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。

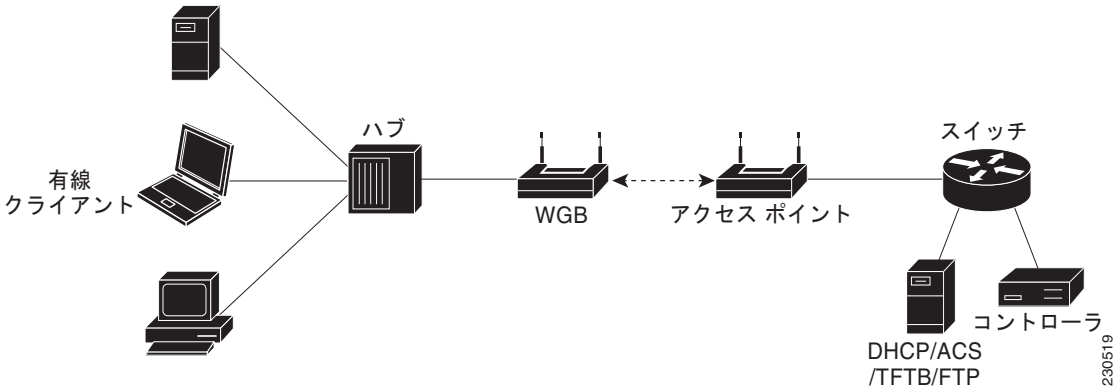
次の例は、1100 シリーズのアクセス ポイントをワークグループ ブリッジとして設定する方法を示しています。この例では、ワークグループ ブリッジは設定されたユーザ名とパスワードを使用して LEAP 認証を実行し、イーサネット ポートに接続されたデバイスが VLAN 22 に割り当てられます。

```
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
```

Lightweight 環境でのワークグループ ブリッジ

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。次の例を参照してください。

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、AP1121、AP1130、AP1231、AP1240、AP 1250、および AP1310 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推奨します。

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 ポイントの GUI の [Settings] > [Network Interfaces] ページで、無線ネットワークでの役割について [Workgroup Bridge] を選択します。
- ワークグループ ブリッジ アクセス ポイントの CLI で、コマンド **station-role workgroup-bridge** を入力します。
- ワークグループ ブリッジがアソシエートできるのは、Lightweight アクセス ポイントだけです（サポートされていない Cisco Airespace AP1000 シリーズ アクセス ポイントを除きます）。
- 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。インフラストラクチャ モードはサポートされません。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。
  - ワークグループ ブリッジ アクセス ポイントの GUI の、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のパラメータで、**Disabled** を選択します。

- ワークグループ ブリッジ アクセス ポイントの CLI で、コマンド **no infrastructure client** を入力します。

（注）　ワークグループ ブリッジでは VLAN の使用はサポートされていません。

- 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。

ワークグループ ブリッジの設定例

ここで、WEP キーが 40 ビットの静的 WEP を使用したワークグループ ブリッジ アクセス ポイントの設定例です。

```
ap#confure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)#dot11 ssid WGB_with_static_WEP
ap(config-ssid)#authentication open
ap(config-ssid)#guest-mode
ap(config-ssid)#exit
ap(config)#interface dot11Radio 0
ap(config)#station-role workgroup-bridge
ap(config-if)#encry mode wep 40
ap(config-if)#encry key 1 size 40 0 1234567890
ap(config-if)#WGB_with_static_WEP
ap(config-if)#end
```

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 の値は 1 ～ 255、seconds の値は 10 ～ 1,000,000 秒です。seconds パラメータは有線クライアントのアイドル時間よりも大きい値に設定することを推奨します。