



# 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。この章の内容は、次のとおりです。

- [リピータ アクセス ポイントの概要 \(P. 18-2\)](#)
- [リピータ アクセス ポイントの設定 \(P. 18-4\)](#)
- [ホット スタンバイの概要 \(P. 18-9\)](#)
- [ホット スタンバイ アクセス ポイントの設定 \(P. 18-10\)](#)
- [ワークグループブリッジ モードの概要 \(P. 18-14\)](#)
- [ワークグループブリッジ モードの設定 \(P. 18-17\)](#)

## 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。



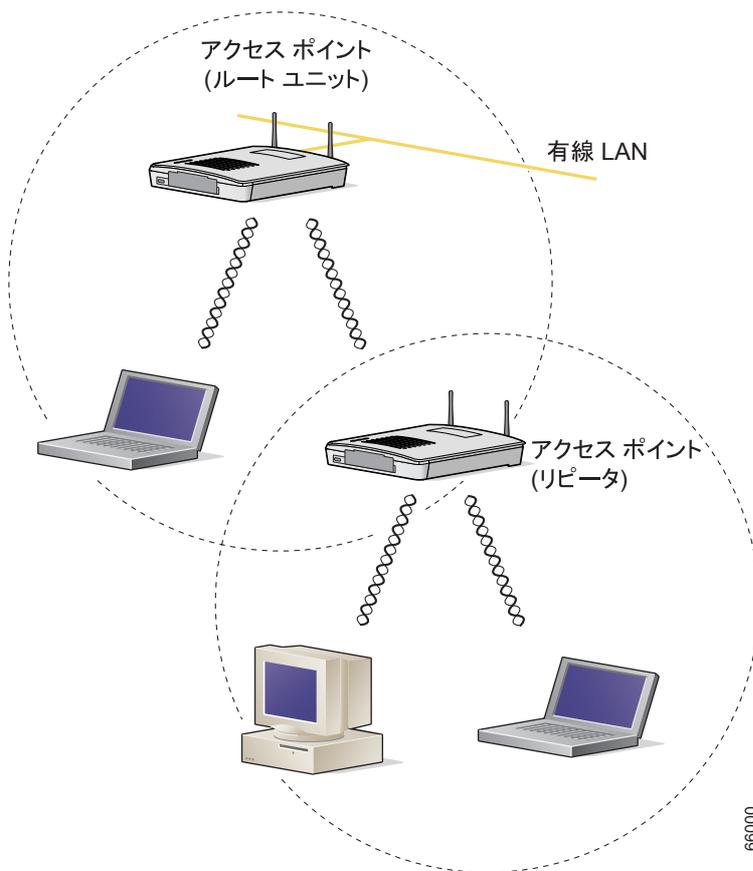
(注) アクセス ポイントは、各無線インターフェイスに対して仮想インターフェイスを生成するので、リピータ アクセス ポイントはルート アクセス ポイントに 2 回アソシエートします。1 回は実際のインターフェイス、もう 1 回は仮想インターフェイスに対してです。



(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 18-1 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 18-1 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。

- デフォルト設定 (P. 18-4)
- リピータのガイドライン (P. 18-4)
- リピータの設定 (P. 18-5)
- リピータ操作の確認 (P. 18-6)
- リピータの LEAP クライアントとしての設定 (P. 18-7)
- リピータの WPA クライアントとしての設定 (P. 18-8)

### デフォルト設定

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 18-1 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 18-1 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 の適用領域を拡大しますが、スループットを大きく減らしません。
- 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恐れがあります。
- 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」の項 (P.6-5) 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 BSSID が設定されている場合、親 アクセス ポイントで Basic Service Set Identifier (BSSID; 基本サービス セット ID) 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設定モードを開始します。2.4GHz 無線は Radio 0、5GHz 無線は Radio 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 Service Set Identifier (SSID; サービス セット ID) 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	<code>infrastructure-ssid [optional]</code>	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。 <b>optional</b> 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。
ステップ 5	<code>exit</code>	SSID 設定モードを終了し、無線インターフェイス設定モードに戻ります。
ステップ 6	<code>station-role repeater</code>	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	<code>dot11 extensions aironet</code>	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	<code>parent {1-4} mac-address [timeout]</code>	<p>(オプション) 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"> <li>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。</li> </ul> <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"> <li>(オプション) タイムアウト値、すなわち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。</li> </ul>
ステップ 9	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 10	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

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
```

## 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、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 Association Table 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、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 10 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のと同じ暗号スイートまたは WEP 認証方式と 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	<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設定モードを開始します。2.4GHz 無線は Radio 0、5GHz 無線は Radio 1 です。
ステップ 3	<code>ssid ssid-string</code>	SSID を作成し、新しい SSID の SSID 設定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	<code>authentication network-eap list-name</code>	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、 <b>aaa authentication login</b> 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	<code>authentication client username username password password</code>	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。

	コマンド	目的
ステップ 6	<code>infrastructure ssid [optional]</code>	(オプション) 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、 <b>optional</b> 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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

## 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 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	<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設定モードを開始します。2.4GHz 無線は Radio 0、5GHz 無線は Radio 1 です。
ステップ 3	<code>ssid ssid-string</code>	SSID を作成し、新しい SSID の SSID 設定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	<code>authentication open</code>	SSID 用の open 認証を有効にします。
ステップ 5	<code>authentication key-management wpa</code>	SSID 用の WPA 認証済みキー管理を有効にします。
ステップ 6	<code>infrastructure ssid</code>	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	<code>wpa-psk { hex   ascii } [ 0   7 ] encryption-key</code>	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 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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 9	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

## 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、監視するアクセス 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、監視するアクセス 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 クエリーを送信します。監視するアクセス 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、監視するアクセス ポイントの設定と一致している必要があります。監視するアクセス 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 ポイントを監視します。たとえば、アクセス ポイント alpha 内の 5GHz 無線を監視するようにスタンバイ アクセス ポイントの 5GHz 無線を設定したり、アクセス ポイント bravo 内の 2.4GHz 無線を監視するように 2.4GHz 無線を設定したりはできません。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) 監視するアクセス 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、監視するアクセス 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) 監視するユニット上の BSSID が追加または削除されると、監視するアクセス 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、監視するアクセス 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 ユニットが監視するアクセス 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、監視するアクセス 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、監視するアクセス 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 (および監視するアクセス 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、監視するアクセス 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 ポイント上で監視するアクセス ポイントの設定をすばやく複製するには、監視するアクセス 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](#)」の項 (P.19-9) 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	<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>iapp standby mac-address</code>	<p>アクセス ポイントをスタンバイ モードに移行し、監視するアクセス ポイントの無線の MAC アドレスを指定します。</p> <p> (注) 2 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 ポイントを監視するように設定する場合、監視する 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) 監視するユニット上の BSSID が追加または削除されると、監視するアクセス 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、監視するアクセス 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。</p>
ステップ 3	<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設定モードを開始します。2.4GHz 無線は Radio 0、5GHz 無線は Radio 1 です。
ステップ 4	<code>ssid ssid-string</code>	スタンバイ アクセス ポイントが監視するアクセス 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。監視するアクセス 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	<code>infrastructure-ssid [optional]</code>	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 を使用して監視するアクセス ポイントにアソシエートします。スタンバイ アクセス ポイントが監視するアクセス ポイントの役割を引き継ぐ場合、 <b>optional</b> 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	<code>authentication client username username password password</code>	監視するアクセス 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	<code>exit</code>	SSID 設定モードを終了し、無線インターフェイス設定モードに戻ります。
ステップ 8	<code>iapp standby poll-frequency seconds</code>	スタンバイ アクセス ポイントが監視するアクセス 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ー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。

	コマンド	目的
ステップ 9	<b>iapp standby timeout</b> <i>seconds</i>	<p>スタンバイ アクセス ポイントが、監視するアクセス 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。</p> <p> (注) スタンバイアクセス ポイントと監視するアクセス ポイント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。</p> <p> (注) 監視するアクセス 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。監視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。</p>
ステップ 10	<b>iapp standby primary-shutdown</b>	(オプション) スタンバイ アクセス ポイントが、監視するアクセス 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、監視するアクセス ポイントの無線を無効にします。この機能によって、監視するアクセス 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	<b>show iapp standby-parms</b>	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、監視するアクセス 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 12	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 13	<b>copy running-config startup-config</b>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

スタンバイ モードを有効にした後、監視するアクセス 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 18-2 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 18-2 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 ポイントが監視するアクセス 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 ポイントが監視するアクセス 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、監視するアクセス 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 モードが設定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 ポイントから監視するアクセス 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 ポイントから監視するアクセス 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、監視するアクセス 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、監視するアクセス 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 モードが設定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、監視するアクセス 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 シリーズと 1200 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。

1200 シリーズのアクセス 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。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、ほかの無線インターフェイスは自動的に無効になります。



### 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モードのアクセスポイントがアソシエートできるのは、Cisco Aironet のアクセス ポイントまたはブリッジだけです。



### (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。

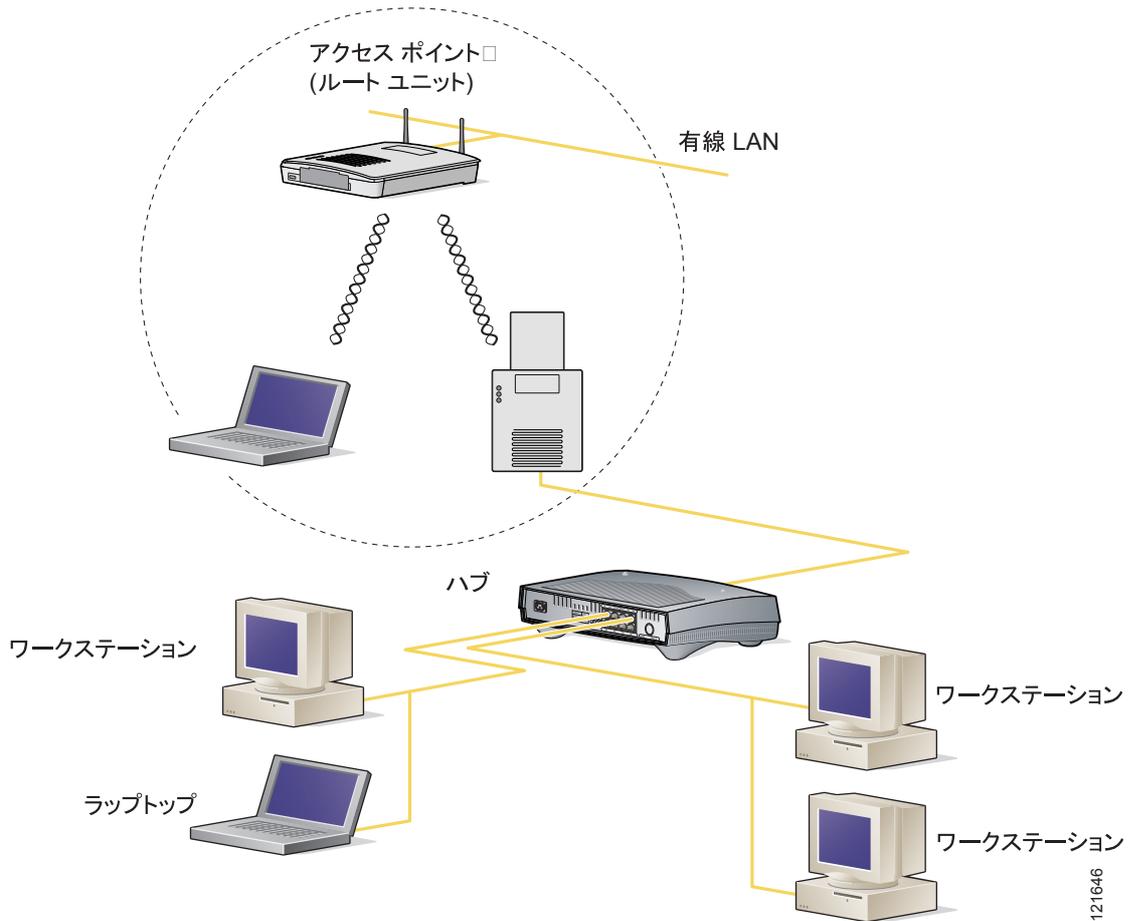


### (注)

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無線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 18-2 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 18-2 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 Address Resolution Protocol (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くと、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。これは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。

## 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 1100 シリーズまたは 1200 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設定モードを開始します。
ステップ 3	<code>station-role workgroup-bridge</code>	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	<code>ssid ssid-string</code>	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	<code>infrastructure-ssid</code>	SSID をインフラストラクチャ SSID に指定します。
		 <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 6	<code>authentication client username username password password</code>	(オプション) 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	<code>exit</code>	SSID 設定モードを終了し、無線インターフェイス設定モードに戻ります。
ステップ 8	<code>exit</code>	無線設定モードを終了し、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 9	<code>workgroup-bridge client-vlan vlan-id</code>	(オプション) 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 10	<code>mobile station</code>	(オプション) 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) 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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 12	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。

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
```