無線の設定

この章では、ワイヤレス デバイスに無線を設定する手順を説明します。

無線インターフェイスのイネーブル化

ワイヤレス デバイスの無線はデフォルトではディセーブルに設定されています。

(注) Cisco IOS Release 12.3(8)JA から、デフォルトの SSID は存在しません。無線インターフェイスを有効にする前に、SSID を作成する必要があります。

特権 EXEC モードから、次の手順に従ってアクセス ポイントの無線を有効にします。

	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	**dot11 ssid** *ssid*	SSID 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 3	**interface dot11radio** {**0** | **1***slot*/*port*}	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 802.11n 2.4GHz 無線は Radio 0 です。 5GHz 無線および 802.11n 5GHz 無線は Radio 1 です。
ステップ 4	**ssid** *ssid*	ステップ 2 で作成した SSID を適切な無線インターフェイスに割り当てます。
ステップ 5	**no shutdown**	無線ポートを有効にします。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**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。

無線ポートをディセーブルにするには、**shutdown** コマンドを使用します。

無線ネットワークの役割の設定

表 6-1 は、各デバイスの無線ネットワークの役割を示しています。

表 6-1　　無線ネットワーク設定でのデバイスの役割

無線ネットワークでの役割	AP 1040	AP 1140	AP 1260	AP 1530	AP 1550	AP 1600	AP 1700	AP 2600	AP 3500	AP 3600	AP 3700	AP 700	AP 2700
アクセスポイント	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
アクセスポイント（無線シャットダウンにフォールバック）	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
アクセスポイント（リピータにフォールバック）	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
リピータ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ルート ブリッジ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
非ルート ブリッジ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ワイヤレス クライアントを持つ ルート ブリッジ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
無線クライアントを持つ非ルート ブリッジ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ワークグループ ブリッジ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ユニバーサル ワークグループ ブリッジ[1]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
スキャナ	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

表 6-1　無線ネットワーク設定でのデバイスの役割(続き)

無線ネットワークでの役割	AP 1040	AP 1140	AP 1260	AP 1530	AP 1550	AP 1600	AP 1700	AP 2600	AP 3500	AP 3600	AP 3700	AP 700	AP 2700
スペクトル	–	–	–	–	Yes	–	Yes	Yes	Yes	Yes	Yes	–	Yes
インストールするもの [自動 | 非ルート | ルート]	–	–	–	Yes	–	–	–	–	–	–	–	–	–

1. AES-CCM TKIP を使用してユニバーサル ワークグループ ブリッジを設定する場合、非ルート デバイスはルート デバイスとアソシエートするためには、TKIP または AES-CCM TKIP だけを暗号として使用する必要があります。AES-CCM だけで設定した場合、非ルート デバイスはルートとアソシエートできません。この設定により、ルート デバイスと非ルート デバイスの間でマルチキャスト暗号の不一致が発生します。

無線ネットワークでのアクセス ポイントまたはブリッジのロールを設定できます。ルート アクセス ポイントにフォールバック ロールを設定することもできます。ワイヤレス デバイスは、イーサネット ポートがディセーブルになるか、または有線 LAN から切り離されたときに自動的にフォールバック ロール(モード)に移行します。フォールバック ロールとして次の 2 つが挙げられます。

- **Repeater**:イーサネット ポートが無効になった場合、ワイヤレス デバイスはリピータになり、近くのルート アクセス ポイントにアソシエートします。フォールバック リピータがアソシエートするルート アクセス ポイントを指定する必要はありません。リピータは最適な無線接続を提供するルート アクセス ポイントに自動的にアソシエートします。
- **Shutdown**:ワイヤレス デバイスは無線をシャットダウンし、すべてのクライアント デバイスの接続を解除します。

(注)　AES-CCM TKIP を使用してユニバーサル ワークグループ ブリッジを設定する場合、非ルート デバイスはルート デバイスとアソシエートするためには、TKIP または AES-CCM TKIP だけを暗号として使用する必要があります。AES-CCM だけで設定した場合、非ルート デバイスはルートとアソシエートできません。この設定により、ルート デバイスと非ルート デバイスの間でマルチキャスト暗号の不一致が発生します。

特権 EXEC モードから、次の手順に従ってワイヤレス デバイスの無線ネットワークの役割とフォールバック ロールを設定します。

	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** }	次の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 802.11n 2.4GHz 無線はインターフェイス 0 です。 5GHz 無線および 802.11n 5GHz 無線はインターフェイス 1 です。

	コマンド	目的
ステップ 3	**station-role** **non-root {bridge | wireless-clients}** **repeater** **root {access-point | ap-only | bridge [wireless-clients] |fallback [repeater | shutdown]}** **scanner** **workgroup-bridge** {**multicast | mode** <*client* | *infrastructure*>**| universal** <*Ethernet client MAC address*>}	ワイヤレス デバイスの役割を設定します。 • 役割は、無線クライアントを持つまたは持たない非ルート ブリッジ、リピータ アクセス ポイント、ルート アクセス ポイントまたはブリッジ、スキャナ、またはワークグループ ブリッジに設定します。 • ブリッジ モードの場合、サポートされるブリッジ機能に限り、屋外アクセス ポイント/ブリッジと相互運用します。 • ブリッジ モード無線はポイントツーポイントおよびポイントツーマルチポイント構成をサポートします。 • 非ルート ブリッジとして機能する屋外アクセス ポイント/ブリッジは、非ルート ブリッジのステーション ロールが **non-root wireless clients** に設定されている限り、他の非ルート ブリッジにアソシエートすることができます。 • いずれかの無線がリピータとして設定されると、イーサネット ポートはシャットダウンします。ワークグループ ブリッジまたはリピータとして設定できるのは、アクセス ポイントにつき 1 つの無線だけです。 • **dot11radio 0|1 antenna-alignment** コマンドは、アクセス ポイントがリピータとして設定されるときに使用できます。 • 他の無線クライアントがルート ブリッジまたはアクセス ポイントにアソシエートされていないと仮定すると、ワークグループ ブリッジは最大 254 のクライアントを持つことができます。 • ユニバーサル ワークグループブリッジでは、アクセス ポイントをワークグループ ブリッジ モードで設定し、シスコ以外のアクセス ポイントと相互運用できます。イーサネット クライアントの MAC アドレスを入力する必要があります。ワークグループ ブリッジは、設定された MAC アドレスがブリッジ テーブルに存在し、静的エントリでない場合に限り、その MAC アドレスにアソシエートされます。検証に失敗した場合、ワークグループ ブリッジはその BVI の MAC アドレスを使用してアソシエートします。また、ユニバーサル ワークグループ ブリッジの役割では、1 つの有線クライアントだけがサポートされます。 • スパニングツリー プロトコル(STP)は、アクセス ポイントでブリッジ モードで設定できます。 • (任意)ルート アクセス ポイントのフォールバック ロールを選択します。ワイヤレス デバイスのイーサネット ポートが無効になるか、有線 LAN から切断された場合、ワイヤレス デバイスは無線ポートをシャットダウンするか、近くのルート アクセス ポイントにアソシエートしたリピータ アクセス ポイントになります。

	コマンド	目的
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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。

(注)　無線ネットワーク内での役割を非ルート ブリッジまたはワークグループ ブリッジとして有効化し、**no shut** コマンドを使用してインターフェイスを有効化する場合、インターフェイスの物理ステータスおよびソフトウェア ステータスは、相手端末のアクセス ポイントまたはブリッジが起動状態の場合だけ起動状態になります。それ以外の場合、デバイスの物理ステータスだけが起動状態になります。デバイスのソフトウェア ステータスが起動状態になるのは、相手端末のデバイスが設定されて起動しているときだけです。

ユニバーサル ワークグループ ブリッジ モード

ユニバーサル ワークグループ ブリッジの役割を設定する場合は、クライアントの MAC アドレスを含める必要があります。ワークグループ ブリッジがこの MAC アドレスにアソシエートされるのは、MAC アドレスがブリッジ テーブルに存在し、静的エントリでない場合に限られます。検証に失敗した場合、ワークグループ ブリッジはその BVI の MAC アドレスを使用してアソシエートします。ユニバーサル ワークグループ ブリッジ モードでは、ワークグループ ブリッジはイーサネット クライアントの MAC アドレスを使用してシスコまたはシスコ以外のルート デバイスとアソシエートします。ユニバーサル ワークグループ ブリッジは透過的で、管理されません。

(注)　ユニバーサル ワークグループ ブリッジの役割では、1 つの有線クライアントだけがサポートされます。

イーサネット クライアントを無効にし、ユニバーサル ワークグループ ブリッジが独自の BVI アドレスを使用してアクセス ポイントにアソシエートするようにすることによって、復元メカニズムを有効化し、ワークグループ ブリッジを再び管理可能にできます。

「国際線のフライト」シナリオをサポートするために、インターフェイス コマンド **world-mode dot11d country-code** *country* [**indoor** | **outdoor** | **both**] にローミング キーワードが追加されています。このキーワードにより、ワークグループ ブリッジはルート アクセス ポイントから認証が取り消されると、パッシブ スキャンを実行します。このコマンドの詳細については、「ワールド モードのイネーブル化とディセーブル化」セクション(6-21 ページ)を参照してください。

802.11n プラットフォームのポイントツーポイントおよびマルチポイント ブリッジングのサポート

ポイントツーポイントおよびポイントツーマルチポイント ブリッジングはすべての 802.11n アクセス ポイントでサポートされます。5 GHz 帯域は 20 MHz および 40 MHz をサポートし、2.4 GHz 帯域は 20 MHz をサポートします。

次のものはすべての 802.11n アクセス ポイントでサポートされます。

- MIMO、ショートレンジ ブリッジング(キャンパスまたはビルディング間での導入)、1 Km 未満の範囲内でダイポールおよび MIMO アンテナ(ライン オブ サイトおよびショート レンジ)を使用
- 20 MHz および 40 MHz の 802.11n サポート

- ワークグループ ブリッジ（WGB）ショートレンジのサポート
- SISO（Single-In、Single-Out）、1 本の屋外アンテナを使用した MCS 0-7 およびレガシー ブリッジ レート（802.11 a/b/g および 802.11n）

（注）　前述のサポートはショートレンジ リンクでのみサポートされ、AP 1400などのブリッジ製品の置き換えにはなりません。

内部アンテナを持つブリッジ モードの AP モデルでは、次のものはサポートされません。

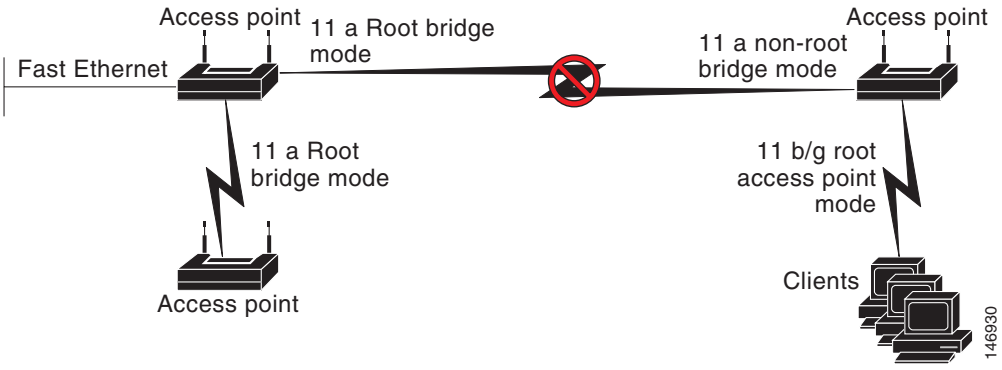
- **distance** コマンド。**distance** コマンドは、屋外での使用が認可されているアクセス ポイントでのみサポートされます。
- 外部アンテナを使用する外部 MIMO ブリッジング。

（注）　ポイントツーマルチポイント ブリッジングでは、ルート ブリッジによる WGB は推奨されません。ポイントツーマルチポイント ブリッジング設定では、WGB はルート AP に関連付ける必要があります。

デュアル無線フォールバックの設定

デュアル無線フォールバック機能を使用すると、アクセス ポイントをネットワーク インフラストラクチャに接続する非ルート ブリッジ リンクがダウンしたとき、クライアントがアクセス ポイントに接続する際に使用するルート アクセス ポイント リンクがシャットダウンするようにアクセス ポイントを設定できます。ルート アクセス ポイント リンクをシャットダウンすると、クライアントは別のアクセス ポイントにローミングを切り替えます。この機能がない場合、クライアントはアクセス ポイントに接続されたままになりますが、ネットワークとデータを送受信できません。

図 6-1　　デュアル無線フォールバック



（注）　この機能はすべてのデュアル無線アクセス ポイントでサポートされます。
この機能はシングル無線アクセス ポイントのフォールバック機能に影響しません。

デュアル無線フォールバックは、次の 3 つの方法で設定できます。

- 無線トラッキング
- ファスト イーサネット トラッキング
- MAC アドレス トラッキング

無線トラッキング

アクセス ポイントのいずれかの無線の状態を追跡またはモニタするようにアクセス ポイントを設定できます。追跡対象の無線がダウンするか無効になると、アクセス ポイントは別の無線をシャットダウンします。追跡対象の無線が起動すると、アクセス ポイントは別の無線をイネーブルにします。

- 無線 0 を追跡するには、無線 1 で次のコマンドを入力してください。

  # station-role root access-point fallback track d0 shutdown

- 無線 1 を追跡するには、無線 0 で次のコマンドを入力してください。

  # station-role root access-point fallback track d1 shutdown

ファスト イーサネット トラッキング

アクセス ポイントのイーサネット ポートがディセーブルになったり、または有線 LAN から切断されたりしたときにフォールバックするようにアクセス ポイントを設定できます。アクセス ポイントをファスト イーサネット トラッキング用に設定するには、「無線ネットワークの役割の設定」セクション（6-2 ページ）で説明するようにして行います。

(注)　ファスト イーサネット トラッキングは、リピータ モードをサポートしません。

- ファスト イーサネット トラッキングに対して 802.11n 以外のアクセス ポイントを設定するには、無線インターフェイス コンフィギュレーション モードで次のコマンドを入力します。

  # station-role root access-point fallback track fa 0

- ギガビット イーサネット トラッキングに対して 802.11n のアクセス ポイントを設定するには、無線インターフェイス コンフィギュレーション モードで次のコマンドを入力します。

  # station-role root fallback shutdown

MAC アドレス トラッキング

非ルート ブリッジまたはワークグループ ブリッジをその MAC アドレスを使用して別の無線でトラッキングすることによって、ルート アクセス ポイントの役割を持つ無線を起動またはダウンするように設定できます。クライアント アクセス ポイントからのアソシエーションが解除されると、ルート アクセス ポイントの無線はダウンします。クライアントがアクセス ポイントと再アソシエートすると、ルート アクセス ポイント無線は起動状態に戻ります。

クライアントがアップストリームの有線ネットワークに接続されている非ルート ブリッジ アクセス ポイントの場合、MAC アドレス トラッキングが最も便利です。

たとえば、MAC アドレスが 12:12:12:12:12:12 の非ルート ブリッジまたはワークグループ ブリッジをトラッキングするには、次のコマンドを入力します。

 # station-role root access-point fallback track mac-address 12:12:12:12:12:12 shutdown

無線ごとのクライアントの制限

インターフェイスにアソシエートされるクライアントの数を設定するには、dot11 無線インターフェイス設定で、コマンド **max-client** *1-255* を使用します。デフォルトでは、この機能はディセーブルになっています。許可されるクライアントの最小数は 1 で、最大数は 255 です。

```
ap(config-if)# max-client 1-255
```

この設定を GUI で行うには、次の手順に従います。

ステップ 1　［Network］>［Network Interfaces］に移動します。

ステップ 2　サイド メニューで、クライアントを制限する無線インターフェイスに応じて、［Dot11 Radio 2.4 GHz］または［Dot11 Radio 5 GHZ］をクリックします。

ステップ 3　無線インターフェイスの設定ページで、［Max-Client］オプションをイネーブルまたはディセーブルにできます。

ステップ 4　［Max-Client］オプションをイネーブルにした場合、［Max-Client］オプションの横にあるテキスト ボックスに、インターフェイスにアソシエートするクライアントの数を指定します。

ステップ 5　[Apply] をクリックします。

無線データ レートの設定

データ レート設定を使用して、ワイヤレス デバイスのデータ転送に使用されるデータ レートを選択します。レートの単位は Megabits per second（Mbps; メガビット/秒）です。ワイヤレス デバイスは、CLI または GUI インターフェイスで設定した最大のデータ レートで転送しようとします。障害や干渉などがある場合、ワイヤレス デバイスはデータ転送が可能な範囲で次に速いレートまで減速されます。各データ レートは、次の 3 つのステートのいずれかに設定できます。

- Basic（GUI では Basic レートを [Required] と表示）：ユニキャストとマルチキャストの両方で、すべてのパケットをこのレートで転送します。ワイヤレス デバイスのデータ レートの少なくとも 1 つは Basic に設定してください。
- Enabled：ワイヤレス デバイスでは、ユニキャスト パケットだけがこのレートで送信され、マルチキャスト パケットは、Basic に設定されているいずれかのデータ レートで送信されます。
- Disabled：ワイヤレス デバイスでは、データはこのレートで送信されません。

（注）　少なくともデータ レートの 1 つは **basic** に設定してください。

Data Rate の設定を使用すると、特定のレートでデータを転送するクライアント デバイスに対応するようにアクセス ポイントを設定できます。2.4GHz、802.11g 無線を、802.11g クライアント デバイスだけに対応するように設定するには、Orthogonal Frequency Division Multiplexing（OFDM; 直交周波数分割多重方式）データ レート（6、9、12、18、24、36、48、54）を、すべて **Basic** に設定します。

また、範囲またはスループットが最適になるようなデータ レートが自動的に設定されるように、ワイヤレス デバイスを設定することも可能です。データ レート設定に **range** を入力した場合、ワイヤレス デバイスでは 1Mbps レートは Basic に、他のレートは Enabled に設定されます。この range 設定によって、アクセス ポイントではデータ レートについて妥協することでカバレッジ領域を拡大できます。したがって、他のクライアントがアクセス ポイントに接続できるときに接続できないクライアントがいる場合、そのクライアントがアクセス ポイントのカバレッジ領域にいないことが

理由の 1 つである場合があります。そのような場合に range オプションを使用すると、カバレッジ領域を拡大するために役立ち、クライアントはアクセス ポイントに接続できる場合があります。通常、スループットと範囲が交換条件となります。(おそらくアクセス ポイントからの距離が原因で) 信号が劣化すると、リンクを維持するために (データ レートを下げて) レートが再ネゴシエートされます。これと対照をなすのはスループットを高く設定したリンクで、設定された高いデータ レートを維持できなくなるほど信号が劣化すると、スループットが低下します。または、十分な適用範囲を持つ他のアクセス ポイントが利用できる場合、そのアクセス ポイントにローミングが切り替わります。この 2 つ (スループットと範囲) のバランスは、決定する必要がある設計上の判断の 1 つです。判断を下す際、ワイヤレス プロジェクトに利用できるリソース、ユーザが渡すトラフィックのタイプ、必要なサービス レベル、そして常に RF 環境の品質が根拠となります。データ レート設定に **throughput** を入力すると、ワイヤレス デバイスではすべてのデータ レートを **basic** (たとえば、2.4 Ghz で 12 のレート、5 GHz で 8 のレート) に設定します。

(注)　802.11b クライアントと 802.11g クライアントが混在する環境の無線ネットワークの場合、1、2、5.5、および 11Mbps のデータ レートが必須 (**basic**) に設定され、他のすべてのデータ レートが **enable** に設定されていることを確認します。802.11b アダプタは 802.11g レートを認識せず、接続先のアクセス ポイントで 11Mbps よりも高いデータ レートが必要だと設定されている場合は動作しません。

マルチキャスト フレームと管理フレームを最高の Basic レートで送信するアクセス ポイント

最近のバージョンの Cisco IOS を実行するアクセス ポイントは、設定された最高の Basic レートでマルチキャスト フレームと管理フレームを送受信し、この状況で信頼性の問題が発生することがあります。

LWAPP または自律 IOS を実行するアクセス ポイントは、設定された最低の Basic レートでマルチキャスト フレームと管理フレームを送受信します。これはセルの端に十分なカバレッジを提供するために必要で、マルチキャスト無線送信を受信できないことがある受信応答しないマルチキャスト転送では特に必要です。

マルチキャスト フレームは MAC レイヤで再送信されないため、セルの端のステーションはマルチキャスト フレームを正常に受信できない場合があります。信頼性の高い受信が目的の場合、マルチキャストは低いデータ レートで送信する必要があります。高いデータ レートのマルチキャストをサポートする必要がある場合、セル サイズを縮小して低いデータ レートをすべて無効にすることが役立つ場合があります。

特定の要件に応じて、次の処置が可能です。

- 信頼性を最大限に高めてマルチキャスト データを送信する必要があって、マルチキャストの帯域幅は大きくする必要がない場合、単一の Basic レートを設定し、無線セルの端に到達するために十分な低さにします。
- 特定のスループットを達成するために特定のデータ レートでマルチキャスト データを送信する必要がある場合、そのレートを最高の Basic レートとして設定します。また、マルチキャスト以外のクライアントのカバレッジのために、低い Basic レートを設定することも可能です。

特権 EXEC モードから、次の手順に従って無線データ レートを設定します。

	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***slot*/*port*}	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 N 無線は Radio 0、5 GHz 無線および 5 GHz N 無線は Radio 1 です。

	コマンド	目的
ステップ 3	**speed** 802.11g、2.4GHz 無線の場合: {[**1.0**] [**2.0**] [**5.5**] [**6.0**] [**9.0**] [**11.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] [**basic-1.0**] [**basic-2.0**] [**basic-5.5**] [**basic-6.0**] [**basic-9.0**] [**basic-11.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-54.0**] | **range** | **throughput** [**ofdm**] | **default** } 802.11a 5GHz 無線の場合: {[**6.0**] [**9.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] [**basic-6.0**] [**basic-9.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-54.0**] | **range** | **throughput** | **ofdm-throughput** | **default**} 802.11n 2.4GHz 無線の場合: {[**1.0**] [**11.0**] [**12.0**] [**18.0**] [**2.0**] [**24.0**] [**36.0**] [**48.0**] [**5.5**] [**54.0**] [**6.0**] [**9.0**] [**basic-1.0**] [**basic-11.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-5.5**] [**basic-54.0**] [**basic-6.0**] [**basic-9.0**] [**default**] [**m0-7**] [**m0.**][**m1.**][**m10.**][**m11.**][**m12.**][**m13.**][**m14.**][**m15.**][**m2.**][**m3.**][**m4.**][**m5.**][**m6.**][**m7.**][**m8-15**] [**m8.**][**m9.**][**ofdm**] [**only-ofdm**] | **range** | **throughput**} 802.11n 5GHz 無線の場合: {[**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] [**6.0**] [**9.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-54.0**] [**basic-6.0**] [**basic-9.0**] [**default**] [**m0-7**] [**m0.**][**m1.**][**m10.**][**m11.**][**m12.**][**m13.**][**m14.**][**m15.**][**m2.**][**m3.**][**m4.**][**m5.**][**m6.**][**m7.**][**m8-15**] [**m8.**][**m9.**]| **range** | **throughput**}	各データ レートを **Basic** または **Enabled** に設定するか、**range** を入力して範囲を最適化するか、あるいは **throughput** を入力してスループットを最適化します。 • (任意) **basic-1.0**、**basic-2.0**、**basic-5.5**、**basic-6.0**、**basic-9.0**、**basic-11.0**、**basic-12.0**、**basic-18.0**、**basic-24.0**、**basic-36.0**、**basic-48.0**、および **basic-54.0** を入力すると、802.11g、2.4GHz 無線でこれらのデータ レートが **basic** に設定されます。 (注)　選択した Basic レートをクライアントがサポートしている必要があります。そうでないと、クライアントはそのワイヤレス デバイスにアソシエートできません。802.11g 無線の Basic データ レートに 12 Mbps 以上を選択した場合、802.11b クライアント デバイスは、ワイヤレス デバイスの 802.11g 無線にアソシエートできません。 **basic-6.0**、**basic-9.0**、**basic-12.0**、**basic-18.0**、**basic-24.0**、**basic-36.0**、**basic-48.0**、および **basic-54.0** を入力すると、5 GHz 無線でこれらのデータ レートが **basic** に設定されます。 (任意) あるいは、**range** または throughput または ofdm-throughput (ERP 保護なし) を入力すると、無線範囲またはスループットが自動的に最適化されます。**range** を入力すると、ワイヤレス デバイスは最も低いデータ レートを Basic に設定し、他のレートを **Enabled** に設定します。**throughput** を入力すると、ワイヤレス デバイスはすべてのデータ レートを **basic** に設定します。 (任意) 802.11g 無線で、すべての OFDM レート (6、9、12、18、24、36、および 48) を Basic (Required) に設定し、すべての Complementary Code Keying (CCK; 相補コードキー入力) レート (1、2、5.5、および 11) を Disabled に設定するには、**speed throughput ofdm** を入力します。この設定により、802.11b 保護機能がディセーブルとなり、802.11g クライアントに最大のスループットが提供されます。ただし、802.11b クライアントはそのアクセス ポイントにアソシエートできなくなります。 • (任意) **default** を入力すると、データ レートは工場出荷時の設定になります (802.11b 無線ではサポートされていません)。 802.11g 無線では、**default** オプションによって、レート 1、2、5.5、および 11 は Basic に、レート 6、9、12、18、24、36、48、および 54 は Enabled に設定されます。これらのレート設定を使用すると、802.11b および 802.11g の両方のクライアント デバイスをワイヤレス デバイス 802.11g 無線に関連付けできるようになります。 5GHz 無線では、**default** オプションによって、レート 6.0、12.0、および 24.0 は Basic に、レート 9.0、18.0、36.0、48.0、および 54.0 は Enabled に設定されます。

	コマンド	目的
	speed（続き）	802.11n 2.4GHz 無線では、**default** オプションによって、レート 1.0、2.0、5.5、および 11.0 が Enabled に設定されます。 802.11n 5GHz 無線では、**default** オプションによって、6.0、12.0、および 24.0 が Enabled に設定されます。 802.11n 無線のデフォルト MCS レート設定は 0 ～ 15 です。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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。

設定から 1 つ以上のデータ レートを削除する場合は、**speed** コマンドの **no** 形式を使用します。次の例は、設定からデータ レート basic-2.0 と basic-5.5 を削除する方法を示しています。

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# no speed basic-2.0 basic-5.5
ap(config-if)# end
```

MCS レートの設定

Modulation Coding Scheme（MCS; 変調および符号化方式）は、変調順序（BPSK、QPSK、16-QAM、64-QAM）および FEC コード レート（1/2、2/3、3/4、5/6）で構成される PHY パラメータの仕様です。MCS は、802.11n 無線で使用されており、32 個の対称設定を定義します（空間ストリームあたり 8 個）。

- MCS 0 ～ 7
- MCS 8 ～ 15
- MCS 16 ～ 23
- MCS 24 ～ 31

MCS は高いスループットを実現する可能性があるため、重要な設定です。高いスループットのデータ レートは、*MCS*、*帯域幅*、および*ガード間隔*の関数です。802.11 a、b、および g 無線は 20MHz のチャネル幅を使用します。

ヒント　アクセス ポイントに対する MCS インデックス、ガード インターバル（GI）、チャネル幅に基づくデータ レートの最新情報については、Cisco.com サイトの『*Cisco Aironet (AP series name) Series Access Points Data Sheet*』を参照してください。

MCS レートは **speed** コマンドを使用して設定します。次の例は、802.11n 5GHz 無線の **speed** 設定を示しています。

```
interface Dot11Radio0
    no ip address
    no ip route-cache
    !
    ssid 1260test
    !
    speed basic-1.0 2.0 5.5 11.0 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0 m0. m1. m2. m3. m4.
    m8. m9. m10. m11. m12. m13. m14. m15.
```

11ac MCS レートのイネーブル化

MCS レートは **speed** コマンドを使用して設定します。

11ac レートをイネーブルにするには、少なくとも 1 つの基本レートと 1 つの 11n レートをイネーブルにする必要があります。

次の例は、802.11ac 5-GHz 無線の **speed** 設定を示しています。

```
interface Dot11Radio1
!
!
ssid 11ac
!
speed 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0 m0. m1. m2. m3. m4. m5. m6. m7. m8. m9. m10.
m11. m12. m13. m14. m15. m16. m17. m18. m19. m20. m21. m22. m23. a1ss9 a2ss9 a3ss9
Channel width 80
```

無線の送信電力の設定

無線の送信電力は、使用するアクセス ポイントに導入されている 1 つ以上の無線のタイプと、アクセス ポイントが動作する規制ドメインに基づきます。アクセス ポイントで使用できる伝送電力と、アクセス ポイントが動作する規制地域について調べるには、デバイスのハードウェア インストレーション ガイドを参照してください。ハードウェア インストレーション ガイドは、cisco.com から入手できます。表示およびダウンロードする手順は、次のとおりです。

ステップ 1　http://www.cisco.com を表示します。

ステップ 2　[Technical Support & Documentation] をクリックします。テクニカルサポート リンクのリストを含む小さいウィンドウが表示されます。

ステップ 3　[Technical Support & Documentation] をクリックします。[Technical Support and Documentation] ページが表示されます。

ステップ 4　[Documentation & Tools] セクションで、[Wireless] を選択します。[Wireless Support Resources] ページが表示されます

ステップ 5　[Wireless LAN Access] セクションで、操作するデバイスを選択します。デバイスの概要ページが表示されます。

ステップ 6　[Install and Upgrade] セクションで、[Install and Upgrade Guides] を選択します。デバイスの [Install and Upgrade Guides] ページが表示されます。

ステップ 7　デバイスのハードウェア インストレーション ガイドを選択します。ガイドのホームページが表示されます。

ステップ 8　左のフレームで、[Channels and Antenna Settings] をクリックします。

表 6-2 は、mW と dBm の関係を示しています。

表 6-2　mW と dBm との変換

dBm	-1	2	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
mW	1	2	3	4	5	6	8	10	12	15	20	25	30	40	50	60	80	100	125	150	200	250

特権 EXEC モードから、次の手順に従ってアクセス ポイントの無線の伝送電力を設定します。

	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***slot*/*port*}	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 無線は Radio 0、5GHz 無線は Radio 1 です。 2.4GHz 802.11n 無線は 0、5GHz 802.11n 無線は 1 です。
ステップ 3	**power local** これらのオプションは、802.11a、5-GHz 無線（dBm）、および 2.4-GHz 802.11n 無線（dBM）で利用可能です。 **{22 | 19 | 16 | 13 | 10 | 7 | 4}**	802.11b、2.4GHz 無線または 5GHz 無線の伝送電力を、現在の規制地域で許可される電力レベルのいずれかに設定します。 （注）　規制地域の電力設定について調べるには、アクセス ポイントのハードウェア インストレーション ガイドを参照してください。
ステップ 4	**power local** 次のオプションは、802.11g、2.4GHz 無線について使用できます。 **power local cck** 設定： { **-1** | **2** | **5** | **8** | **11** | **14** | **17** | **20** | **maximum** } **power local ofdm** 設定： { **-1** | **2** | **5** | **8** | **11** | **14** | **17** |**maximum** } （注）　これらのオプションは 802.11n AP では利用できません。	802.11g、2.4GHz 無線の伝送電力を、現在の規制地域で許可される電力レベルのいずれかに設定します。設定は dBm 単位です。 2.4GHz の 802.11g 無線では、直交周波数分割多重方式（OFDM）と Complementary Code Keying（CCK; 相補コードキー入力）のいずれかの電力レベルを設定できます。CCK 変調は、802.11b デバイスおよび 802.11g デバイスによってサポートされています。OFDM 変調は、802.11g デバイスおよび 802.11a デバイスによってサポートされています。 （注）　規制地域の電力設定について調べるには、アクセス ポイントのハードウェア インストレーション ガイドを参照してください。 （注）　802.11g 無線の最大送信電力レベルは AP モデルによって異なります。電力レベルについては AP データ シートを参照してください。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**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。

電力設定をデフォルトの **maximum** に戻すには、power コマンドの **no** 形式を使用します。

アソシエートしたクライアント デバイスの電力レベルの制限

ワイヤレス デバイスにアソシエートしたクライアント デバイスの電力レベルを制限することもできます。クライアント デバイスがワイヤレス デバイスにアソシエートするとき、ワイヤレス デバイスはクライアントに最大電力レベル設定を送信します。

（注）　Cisco AVVID のマニュアルでは、アソシエートされたクライアント デバイスの電力レベルの制限を示すのに Dynamic Transmit Power Control（DTPC; 送信電力の動的制御）という用語を用います。

特権 EXEC モードから、次の手順に従ってワイヤレス デバイスにアソシエートするすべてのクライアント デバイスに、最大許可電力設定を指定します。

	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***slot*/*port*}	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 無線は Radio 0、5GHz 無線は Radio 1 です。 2.4GHz 802.11n 無線は 0、5GHz 802.11n 無線は 1 です。
ステップ 3	**power client** これらのオプションは、802.11n 2.4-GHz と 5-GHz クライアント（dBm）の両方で利用可能です。 {*-127 to 127* | **local** | **maximum**}	ワイヤレス デバイスにアソシエートするクライアント デバイスに、許可電力レベルを設定します。次の操作を実行できます。 • -127 ～ 127 dBm の任意の電力レベル値を設定します。 • クライアント電力レベルをアクセス ポイントの電力レベルに設定するには、電力レベルを **local** に設定します。 • クライアント電力を許可される最大値に設定するには、電力レベルを **maximum** に設定します。 （注）　規制ドメインで許容される設定は、ここで取り上げる設定と異なる場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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。

アソシエートしたクライアントの最大電力レベルを無効にするには、client power コマンドの **no** 形式を使用します。

（注）　アソシエートしたクライアント デバイスの電力レベルを制限する場合は、Aironet 拡張機能をイネーブルにする必要があります。Aironet 拡張機能はデフォルトでは有効に設定されています。

無線チャネルの設定

ワイヤレス デバイスの無線のデフォルト チャネル設定は Least Congested です。起動時にワイヤレス デバイスは最も混雑の少ないチャネルをスキャンして選択します。ただし、サイト調査の後も一貫したパフォーマンスが維持されるように、各アクセス ポイントにスタティック チャネル設定を指定することを推奨します。ワイヤレス デバイスのチャネル設定は、規制ドメインで使用できる周波数に対応します。ドメインで許可されている周波数については、アクセス ポイントのハードウェア インストレーション ガイドを参照してください。

（注）　RF 干渉が原因でクライアントが無線からときどき切断されている場所では、チャネル 1（2412）などの別のチャネルで動作するように無線インターフェイスを設定すると干渉を回避できる場合があります。

2.4GHz 帯チャネル利用帯域幅は、チャネルあたり 22MHz になります。チャネル 1、6、11 は重複していないため、干渉を起こさずに、同じ圏内に複数のアクセス ポイントを設定できます。802.11b および 802.11g の 2.4GHz 無線はいずれも同じチャネルと周波数を使用します。

5-GHz 無線は、802.11n AP で 5180 ～ 55825 MHz の 9 つのチャネル、1140 シリーズ AP で 5180 ～ 5805 の 8 つのチャネルで動作します。各チャネルは 20MHz に対応し、チャネルの帯域幅は少しずつ重複しています。最適なパフォーマンスを得るため、互いに近い位置にある無線の場合は、隣接していないチャネル（たとえば、44 と 46）を使用します。

（注）　同じ圏内に多くのアクセス ポイントを設定しすぎると、無線の輻輳が発生し、スループットが減少します。無線のサービス範囲とスループットを最大にするには、慎重なサイト調査を行って、アクセス ポイントの最適な設置場所を決定する必要があります。

チャネル設定は頻繁に変更されるため、このマニュアルには記載されていません。ご使用のアクセス ポイントまたはブリッジのチャネル設定についての最新情報は、『*Channels and Maximum Power Settings for Cisco Aironet Autonomous Access Points and Bridges*』を参照してください。このマニュアルは cisco.com の次の URL から入手できます。

http://cisco.com/en/US/products/ps6521/tsd_products_support_install_and_upgrade.html

802.11n のチャネル幅

802.11n では、20 MHz および 40 MHz の両方のチャネル幅が使用可能です。チャネル幅は、2 つの連続する重複しないチャネル（たとえば、5 GHz のチャネル 36 およびチャネル 40）で構成されます。802.11n 無線は、同じ帯域で動作します。ただし、チャネル幅は個別に設定できます。

20MHz チャネルの 1 つは*コントロール チャネル*と呼ばれます。レガシー クライアントおよび 20MHz の高いスループットのクライアントはコントロール チャネルを使用します。ビーコンを送信できるのはこのチャネルだけです。2 番目の 20MHz チャネルは*拡張チャネル*と呼ばれます。40MHz のステーションは、このチャネルとコントロール チャネルを同時に使用できます。

40 MHz チャネルは、チャネルとして指定され、拡張は -1 として指定されます。ここでは、コントロール チャネルはチャネル 40 MHz、拡張チャネルがその下の 36 MHz です。

特権 EXEC モードから、次の手順に従ってワイヤレス デバイスのチャネル幅を設定します。

	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***slot*/*port*}	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 802.11n 2.4 GHz 無線は Radio 0 です。 5GHz 無線および 802.11n 5GHz 無線は Radio 1 です。

	コマンド	目的
ステップ 3	**channel** {*frequency* | **least-congested** | **width** [**20** | **40-above** | **40-below**] | **dfs**}	ワイヤレス デバイス無線のデフォルト チャネルを設定します。起動時に最も混雑の少ないチャネルを探す場合は、**least-congested** を入力します。 使用する帯域幅を指定するには **width** オプションを使用します。このオプションはすべての 802.11n AP で利用できますが、d1（5 GHz）無線のみです。設定は 3 つあります。20、40-above、40-below です。20 を選択すると、チャネル幅が 20 MHz に設定されます。40-above を選択すると、拡張チャネルをコントロール チャネルの上に重ねた状態でチャネル幅が 40 MHz に設定されます。40-below を選択すると、拡張チャネルをコントロール チャネルの下に重ねた状態でチャネル幅が 40 MHz に設定されます。 （注）　動的周波数選択（DFS）に関する欧州連合の規制に準拠する 5 GHz の無線については、**channel** コマンドはディセーブルに設定されています。詳細については、「802.11n ガード間隔の設定」セクション（6-20 ページ）を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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。

Dynamic Frequency Selection（動的周波数選択）

工場出荷時に 5GHz 無線が設定されている、米国、ヨーロッパ、シンガポール、韓国、日本、イスラエル、および台湾向けのアクセス ポイントは、無線デバイスがレーダー信号を検出して干渉しないようにする動的周波数選択（DFS）の使用を必須とする規制に従うようになりました。アクセス ポイントが特定のチャネルでレーダーを検出すると、そのチャネルを 30 分間使用しないようにします。その他の規制地域向けに設定する無線では、DFS を使用しません。

DFS を有効に設定した 5GHz 帯無線を 表 6-3 に記載した 15 チャネルのいずれかで動作させると、アクセス ポイントが自動的に DFS を使用して動作周波数を設定します。DFS が有効に設定されると、アクセス ポイントが自身の動作周波数にレーダー信号がないかモニタするようになります。同じチャネルにレーダー信号を検出した場合は、アクセス ポイントが次の処理を実行します。

- チャネル上でそれ以降の伝送をブロックします。
- 省電力モードのクライアントからのキューを消去します。
- 802.11h チャネル切り替えの通知を同報通信します。
- 残りのクライアント デバイスのアソシエーションを解除します。
- Wireless Domain Service（WDS; 無線ドメイン サービス）に参加している場合、周波数を終了する DFS 通知をアクティブな WDS デバイスに送信します。
- 別の 5GHz チャネルを無作為に選択します。
- 選択したチャネルが 表 6-3 のいずれかのチャネルだった場合は、そのチャネルにレーダー信号がないか 60 秒間スキャンします。
- そのチャネルにレーダー信号がなければ、ビーコンを有効にしてクライアントのアソシエーションを受け入れます。
- WDS に参加している場合、アクティブな WDS デバイスに新しい動作周波数を知らせる DFS 通知を送信します。

(注)　規制要件に従い、一部の地域では、DFS を有効に設定した 5 GHz 帯無線のチャネルを手動で選択できません。この場合、アクセス ポイントが無作為にチャネルを選択します。

DFS が必要なチャネルのすべてのリストを、表 6-3 に示します。

表 6-3　DFS チャネル リスト

チャネル	周波数	チャネル	周波数	チャネル	周波数
52	5260MHz	104	5500MHz	124	5620MHz
56	5280MHz	108	5520MHz	128	5640MHz
60	5300MHz	112	5560MHz	132	5660MHz
64	5320MHz	116	5580MHz	136	5680MHz
100	5500MHz	120	5600MHz	140	5700MHz

自律動作を行うために、DFS では 表 6-3 にリストされているチャネルから無作為にチャネルを選択することが必要です。表 6-3 にリストされていないチャネルは無作為な選択が不要で、手動で設定できます。

動的周波数選択（DFS）が必要なチャネルは 5 GHz の無線設定メニューから手動で選択することができます。DFS チャネルを確認するには、**show controllers d1** コマンドを使用します。

また、手動で非 DFS チャネルを設定する場合の GUI/CLI を使用して、DFS チャネルを選択することもできます。デフォルトのチャネル選択は「DFS」であり、無作為にチャネルが選択されます。

手動で設定された DFS チャネルでレーダーが検出された場合、そのチャネルは自動的に変更され、設定したチャネルには戻りません。

表 6-3 にリストされているチャネルで送信する前に、アクセス ポイント無線は Channel Availability Check（CAC）を実行します。CAC はチャネルに無線信号が存在するかを調べる 60 秒のスキャンです。次のメッセージ例は、CAC スキャンの開始と終了を示すもので、アクセス ポイントのコンソールに表示されます。

```
*Mar 6 07:37:30.423: %DOT11-6-DFS_SCAN_START: DFS: Scanning frequency 5500 MHz for
60 seconds

*Mar 6 07:37:30.385: %DOT11-6-DFS_SCAN_COMPLETE: DFS scan complete on frequency
5500 MHz
```

表 6-3 に記載されている DFS チャネルを稼働すると、アクセス ポイントでは、CAC を実行しているため、チャネル上にレーダーがないかどうかを常に監視します。レーダーが検出されると、アクセス ポイントはデータ パケットの転送を 200 ミリ秒間停止し、802.11h チャネル切り替えの通知を含む 5 つのビーコンを同報通信し、アクセス ポイントが使用を開始するチャネル番号を指示します。次のメッセージ例は、レーダーが検出されたときにアクセス ポイント コンソールに表示されます。

```
*Mar 6 12:35:09.750: %DOT11-6-DFS_TRIGGERED: DFS: triggered on frequency 5500 MHz
```

チャネルにレーダーが検出されると、そのチャネルは 30 分間使用できません。アクセス ポイントは、過去 30 分のうちにチャネルにレーダーを検出した各チャネルのフラグを不揮発性ストレージに維持します。30 分が過ぎると、対応するチャネルのフラグがクリアされます。フラグがクリアされる前にアクセス ポイントがリブートすると、チャネルの初期化中に非占有時間が 30 分にリセットされます。

(注)　適法な最大送信電力については、他のチャネルよりも 5GHz チャネルの方が大きくなるものがあります。無作為に選択した 5GHz チャネルが電力を制限されていた場合、アクセス ポイントはそのチャネルの電力上限に合うように自動的に送信電力を下げます。

(注)　DFS が有効に設定された無線で国番号を設定するには、**world-mode dot11d** *country-code* 設定インターフェイス コマンドを使用することを推奨します。IEEE 802.11h プロトコルでは、アクセス ポイントはビーコンとプローブ応答に国情報エレメント（IE）を含める必要があります。ただしデフォルトでは、IE の国番号は空白に設定されています。**world-mode** コマンドで、国番号 IE を入力してください。

DFS チャネルでのレーダー検出

AP がレーダー ステーションの近くに設置されている場合、複数のチャネルでレーダーのアクティビティを検出できます。インターフェイス dot11radio1 で **peakdetect** コマンドを使用することによって、AP でレーダー信号を検出し、動的周波数選択（DFS）を使用してそれらが干渉しないようにすることができます。デフォルトでは、このコマンドはイネーブルです。

ただし、物理的な RF 信号フィルタを使用して解決することができないインバンド/オフチャネル気象レーダー信号が原因で、AP が誤った DFS トリガーを取得していると思われる場合は、レーダー信号を検出しないように AP を設定することができます。AP でレーダー信号を検出しない場合、インターフェイス dot11radio1 で **no peakdetect** コマンドを使用します。

DFS チャネルでアクセス ポイントがレーダーを検出すると、そのアクセス ポイントはフラッシュ メモリ内にファイルを作成します。このファイルは 802.11a 無線のシリアル番号に基づいたもので、レーダーが検出されたチャネルの番号が記録されています。これは正常な動作です。このファイルは削除しないでください。

CLI コマンド

次の項では、DFS に適用される CLI コマンドを説明します。

DFS が有効に設定されているかどうかの確認

DFS が有効に設定されているかどうかを確認するには、**show controllers dot11radio1** コマンドを使用します。コマンドには、均一拡散（Uniform Spreading）が必須であること、およびレーダーの検出が原因で非占有期間にあるチャネルの表示も含まれます。

次の例は、DFS が有効になっているチャネルで show controller コマンドを実行した時の出力行を示しています。前のパラグラフにリストで表示された内容は、**太字**で記載されています。

```
ap#sh controllers dot11Radio 1
!
interface Dot11Radio1
Radio ElliotNess 5, Base Address f4ea.6710.6590, BBlock version 0.00, Software version
4.10.1
Serial number: FOC16145K24
Unused dynamic SQRAM memory: 0x00007CB4 (31 KB)
Unused dynamic SDRAM memory: 0x0008E490 (569 KB)
Spectrum FW version: 1.14.2
Number of supported simultaneous BSSID on Dot11Radio1: 16
Carrier Set: Americas (OFDM) (US) (-A)
```

```
Uniform Spreading Required: Yes
Configured Frequency: 0 MHz  Channel 0
Allowed Frequencies: * Dynamic Frequency Selection (DFS) only
         5180( 36)  5200( 40)  5220( 44)  5240( 48) *5260( 52) *5280( 56) *5300( 60)
*5320( 64) *5500(100) *5520(104)
        *5540(108) *5560(112) *5580(116) *5660(132) *5680(136) *5700(140)  5745(149)
5765(153)  5785(157)  5805(161)
         5825(165)
Listen Frequencies:
         5180( 36)  5200( 40)  5220( 44)  5240( 48)  5260( 52)  5280( 56)  5300( 60)
5320( 64)  5500(100)  5520(104)
         5540(108)  5560(112)  5580(116)  5600(120)  5620(124)  5640(128)  5660(132)
5680(136)  5700(140)  5745(149)
         5765(153)  5785(157)  5805(161)  5825(165)

DFS Blocked Frequencies: none
Beacon Flags: 0, Interface Flags 20109, Interface Events 0, Mode 9; Beacons are disabled;
Probes are disabled
Configured TxPower:             14 dBm
Allowed Power Levels:           14 11  8  5  2  dBm
Allowed Client Power Levels:    14 11  8  5  2  dBm
Antenna:                        Rx[a b c d ]
                                Tx[a b c d  ofdm all]
                                External
                                Gain [Allowed 12, Reported 0, Configured 0, In Use 12]
(dBi x 2)
```

チャネルの設定

チャネルを設定するには **channel** コマンドを使用します。インターフェイスのコマンドは、特定のチャネル番号を選択して DFS を有効にすることだけをユーザに許可するように変更されています。

	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 dot11radio1 dfs**	802.11a 無線のインターフェイス設定を開始します。
ステップ 3	**channel** {*number* | **dfs** |**band** <*1 - 4*>}	*number* には、36 から 5825 のチャネル周波数を入力します。 選択されたチャネルで動的周波数選択を使用するには、**dfs** および次のいずれかの周波数帯を入力します。 1：5.150 ～ 5.250 GHz 2：5.250 ～ 5.350 Ghz 3：5.470 ～ 5.725 GHz 4：5.725 ～ 5.825 GHz DFS だけで選択できるチャネルを設定しようとすると、次のメッセージが表示されます。 `This channel number/frequency can only be used by Dynamic Frequency Selection (DFS)` （注）　**channel dfs** コマンドは、-P および -Q 規制ドメインではサポートされません。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show running-config**	入力内容を確認します。
ステップ 6	**copy running-config startup-config**	(任意)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。

次の例では、DFS を使用するように 5 GHz の無線を設定します。

```
ap# configure terminal
ap(config)# interface dot11radio1
ap(config-if)# channel dfs
ap(config-if)# end
```

DFS 選択によるチャネル ブロック

屋内や屋外など特定地域で使用できるチャネルを制限している規制地域の場合、DFS が有効になっている時にアクセス ポイントがそれらを選択しないようチャネルをまとめてブロックすることができます。DFS 選択によってチャネルをまとめてブロックするには、次の設定インターフェイス コマンドを使用してください。

[no] dfs band [1] [2] [3] [4] block

オプション 1、2、3、4 で、ブロック対象のチャネルを指定します。

- **1**:5.150 ～ 5.250GHz の周波数を指定します。この周波数グループは UNII-1 帯域とも呼ばれています。
- **2**:5.250 ～ 5.350GHz の周波数を指定します。この周波数グループは UNII-2 帯域とも呼ばれています。
- **3**:5.470 ～ 5.725GHz の周波数を指定します。この周波数グループは UNII-2 拡張とも呼ばれています。
- **4**:5.725 ～ 5.825GHz の周波数を指定します。この周波数グループは UNII-3 帯域とも呼ばれています。

次の例は、DFS 中にアクセス ポイントが 5.150 ～ 5.350GHz の周波数を選択しないようにする方法を示しています。

```
ap(config-if)# dfs band 1 2 block
```

次の例は、DFS について 5.150 ～ 5.350GHz の周波数をブロック解除する方法を示しています。

```
ap(config-if)# no dfs band 1 2 block
```

次の例は、DFS についてすべての周波数をブロック解除する方法を示しています。

```
ap(config-if)# no dfs band block
```

802.11n ガード間隔の設定

802.11n ガード間隔は、パケット間のナノ秒単位の時間です。短時間(400ns)および長時間(800ns)の 2 つの設定が可能です。

特権 EXEC モードから、次の手順に従って 802.11n ガード間隔を設定します。

	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。 802.11n 2.4GHz 無線は Radio 0 です。 802.11n 5GHz 無線は Radio 1 です。
ステップ 3	**guard-interval** {**any** | **long**}	ガード間隔を入力します。 • any では、ショート GI をサポートするクライアントで AP が 400 ns を使用できるようにし、また ショート GI をサポートしないクライアントでは 800 ns を使用できるようにします。つまり、ショート（400ns）またはロング（800ns）いずれかのガード間隔です。 • long では、ロング（800ns）ガード間隔のみを使用できます。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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。

ワールド モードのイネーブル化とディセーブル化

ワイヤレス デバイスで、802.11d ワールド モード、Cisco レガシー ワールド モード、またはワールド モード ローミングをサポートするよう設定できます。ワールド モードをイネーブルにすると、AP はそのビーコンにチャネル キャリア セット情報を追加します。ワールド モードがイネーブルになっているクライアント デバイスは、キャリア セット情報を受信して、それぞれの設定を自動的に調整します。たとえば、日本で主に使用されるクライアント デバイスがイタリアに移され、そこでネットワークに参加した場合、ワールド モードに依存して、そのチャネルと電力の設定を自動的に調整することができます。

ワールド モードはデフォルトではディセーブルに設定されています。

特権 EXEC モードから、次の手順に従ってワールド 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	**interface dot11radio** {**0***slot*/*port* | **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。

	コマンド	目的
ステップ 3	**world-mode dot11d country_code** *code* { **both** | **indoor** | **outdoor** } **world-mode roaming** | **legacy**	ワールド モードを有効にします。 • 802.11d ワールド モードをイネーブルにするには、**dot11d** オプションを入力します。 – **dot11d** オプションを入力する場合、2 文字の ISO 国番号（たとえば、米国の ISO 国番号は **US**）を入力する必要があります。ISO 国番号の一覧は ISO の Web サイトに掲載されています。 – 国番号の後に、ワイヤレス デバイスの配置場所を示すために **indoor**、**outdoor**、または **both** と入力します。 • シスコのレガシー ワールド モードをイネーブルにするには、**legacy** オプションを入力します。 • アクセス ポイントを継続的なワールド モード構成に配置するには、**world-mode roaming** と入力します。 （注）　レガシー ワールド モードを使用するには、Aironet 拡張機能をイネーブルにする必要がありますが、802.11d ワールド モードではこの拡張機能は不要です。Aironet 拡張機能はデフォルトではイネーブルに設定されています。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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。

ワールド モードを無効にするには、コマンドの **no** 形式を使用します。

short 無線プリアンブルのイネーブル化とディセーブル化

無線プリアンブルは、AP とクライアントが通信を同期するのに役立つフレームの先頭にあるデータのセクションです。無線プリアンブルを long または short に設定できます。

- Short：short プリアンブルを使用すると、スループットのパフォーマンスが向上します。Cisco Aironet 無線 LAN クライアント アダプタは、短いプリアンブルをサポートします。802.11b または 802.11g 認定デバイスはどれも短いプリアンブルをサポートします。ただし、クライアント デバイスによっては、802.11b/g 認定の場合でも、長いプリアンブルを必要とします。
- Long：長いプリアンブルは、レガシー 802.11 のみのデバイス、および最適な運用で長いプリアンブルを予期する一部の 802.11b/g デバイスで使用されます。これらのクライアント デバイスがワイヤレス デバイスにアソシエートしない場合、short プリアンブルを使用する必要があります。

5 GHz 無線では無線プリアンブルに short と long を設定できません。

特権 EXEC モードから、次の手順に従って短い無線プリアンブルを無効にします。

	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	**interface dot11radio { 0*slot/port* }**	2.4GHz 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 モードに切り替えます。
ステップ 3	**no preamble-short**	短いプリアンブルを無効にし、長いプリアンブルを有効にします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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。

デフォルトでは short プリアンブルがイネーブルに設定されています。short プリアンブルがディセーブルになっている場合、イネーブルにするには **preamble-short** コマンドを使用します。

送受信アンテナの設定

ワイヤレス デバイスがデータの送受信に使用するアンテナを選択できます。受信アンテナと送信アンテナでそれぞれ 3 つのオプションがあります。

- Gain:結果のアンテナ ゲインを dB 単位で設定します。
- Diversity:デフォルト設定。最適な信号を受信するアンテナがワイヤレス デバイスで使用されます。ワイヤレス デバイスに 2 つの固定(取り外し不能)アンテナが使用されている場合は、受信と送信の両方にこの設定を使用します。デバイスに 3 つの取り外し可能アンテナが使用されている場合、この設定を使用して、それらすべてのアンテナを Diversity モードで動作させることが可能です。
- Right:ワイヤレス デバイスに取り外し可能なアンテナが使用されており、高ゲイン アンテナがワイヤレス デバイスの右側のコネクタに取り付けられている場合は、受信と送信の両方にこの設定を使用します。ワイヤレス デバイスの背面パネルに向かって、右にあるのが右側のアンテナになります。
- Middle:無線デバイスに取り外し可能なアンテナが使用されており、高ゲイン アンテナが無線デバイスの中央コネクタに取り付けられている場合は、この設定を受信だけに使用する必要があります。3 アンテナ構成での送信に使用できるアンテナは、右と左のアンテナです。
- Left:ワイヤレス デバイスに取り外し可能なアンテナが使用されており、高ゲイン アンテナがワイヤレス デバイスの左側のコネクタに取り付けられている場合は、受信と送信の両方にこの設定を使用します。ワイヤレス デバイスの背面パネルに向かって、左にあるのが左側のアンテナになります。
  これは、1600、2600、および 3600 シリーズなどのデュアル アンテナ AP には適用されません。詳細情報については、それぞれのハードウェア ガイドを参照してください。

特権 EXEC モードから、次の手順に従ってワイヤレス デバイスがデータの送受信に使用するアンテナを選択します。

	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***slot*/*port*}	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 無線は Radio 0、5GHz 無線は Radio 1 です。 802.11n 2.4GHz 無線は Radio 0 です。 802.11n 5GHz 無線は Radio 1 です。
ステップ 3	**antenna again** *dB*	デバイスに接続されたアンテナの結果のゲインを指定します。–128 ～ 128 dB の値を入力します。 (注)　この設定は無線デバイスの動作に影響せず、ネットワークの管理プラットフォームにデバイスのアンテナ ゲインを通知するだけです。
ステップ 4	**antenna receive** {**diversity** | **left** | **middle** | **right**} **2600 および 3600 シリーズでは、このコマンドは次のとおりです。** **antenna receive** {**a-antenna** | **ab-antenna** | **abc-antenna** | **abcd-antenna**}	受信アンテナを diversity、left、middle、right、または all に設定します。 (注)　2 つのアンテナを使用してパフォーマンスを最適にするには、受信アンテナの設定にデフォルトの **diversity** を使用します。1 つのアンテナの場合、アンテナを右側に取り付け、アンテナを **right** に設定します。 2600 および 3600 シリーズの AP では次のようになります。 • a-antenna：アンテナ A のみを利用 • ab-antenna：アンテナ A、B を利用 • abc-antenna：アンテナ A、B、C を利用 • abcd-antenna：アンテナ A、B、C、D を利用
ステップ 5	**antenna transmit** {**diversity** | **left** | **right**} **2600 および 3600 シリーズでは、このコマンドは次のとおりです。** **antenna transmit** {**a-antenna** | **ab-antenna** | **abc-antenna** | **abcd-antenna**}	送信アンテナを Diversity、Left、Right のいずれかに設定します。 (注)　2 つのアンテナを使用してパフォーマンスを最適にするには、受信アンテナの設定にデフォルトの **diversity** を使用します。1 つのアンテナの場合、アンテナを右側に取り付け、アンテナを **right** に設定します。 2600 および 3600 シリーズの AP では次のようになります。 • a-antenna：アンテナ A のみを利用 • ab-antenna：アンテナ A、B を利用 • abc-antenna：アンテナ A、B、C を利用 • abcd-antenna：アンテナ A、B、C、D を利用
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**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。

Gratuitous Probe Response の有効化と無効化

Gratuitous Probe Response（GPR）は、携帯および WLAN の動作モードをサポートするデュアル モード電話で、バッテリ残量を節約します。GPR は 5GHz 無線で使用可能で、デフォルトで無効に設定されています。GPR の設定には、次の 2 種類の設定があります。

- Period：（ビーコン間隔と同じように）GPR 伝送間の時間を 10 ～ 255 の Kusec（またはミリ秒）間隔で決定します。
- Speed：GPR の伝送に使用するデータ レートの速度です。

長い期間を選択すると、GPR によって消費される RF 帯域幅の量が減少し、バッテリ寿命が短くなる可能性があります。高い伝送速度を選択すると、消費される帯域幅の量が減少し、代わりにセル サイズが小さくなります。

特権 EXEC モードから、次の手順に従って GPR を有効にし、パラメータを設定します。

	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 {1}*slot/port***	5GHz 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 モードに切り替えます。
ステップ 3	**probe-response gratuitous** {**period** | **speed**}	デフォルトの period（10 Kusec）および speed（6.0 Mbps）を使用して Gratuitous Probe Response 機能を有効にします。
ステップ 4	**period** *Kusec*	（任意）10 ～ 255 の範囲の値を入力します。デフォルト値は 10 です。
ステップ 5	**speed** {[**6.0**] [**9.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] }	（任意）応答速度を Mbps 単位で設定します。デフォルト値は 6.0 です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**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。

オプション パラメータのデフォルトを使用したくない場合、次の例に示すようにオプション パラメータを個別に設定したり、または結合して設定したりできます。

```
(config-if)# probe-response gratuitous speed 30
(config-if)# probe-response gratuitous speed 12.0
(config-if)# probe-response gratuitous period 30 speed 12.0
```

GPR 機能を無効にするには、コマンドの **no** 形式を使用します。

Aironet 拡張機能の無効化と有効化

デフォルトでは、ワイヤレス デバイスは Cisco Aironet 802.11 拡張機能を使用して Cisco Aironet クライアント デバイスの機能を検出し、ワイヤレス デバイスとアソシエートしたクライアント デバイスとの間での特定の相互作用に必要な機能をサポートします。次の機能をサポートするには、Aironet 拡張機能をイネーブルにする必要があります。

- ロード バランシング：ワイヤレス デバイスは Aironet 拡張機能を使用して、ネットワークとの最適な接続性を確保できるアクセス ポイントにクライアント デバイスを自動的に誘導します。これは、ユーザ数、ビット エラー レート、信号強度などの要因に基づいて行われます。

- メッセージ整合性チェック（MIC）：暗号化されたパケットへの攻撃（ビットフリップ攻撃）を阻止するために新しく追加された WEP セキュリティ機能。MIC は、ワイヤレス デバイスと、それにアソシエートされたすべてのクライアント デバイスに実装され、数バイトを各パケットに付加することによって、パケットの改ざんを防ぎます。
- Cisco Key Integrity Protocol（CKIP）：IEEE 802.11i セキュリティ タスク グループによって提供された初期アルゴリズムに基づく、シスコの WEP キー置換技術です。標準規格に基づくアルゴリズムである Temporal Key Integrity Protocol（TKIP）では、Aironet 拡張機能を有効にする必要はありません。
- リピータ モード：Aironet 拡張機能はリピータ アクセス ポイントと、それらがアソシエートするルート アクセス ポイントで有効に設定されていなければなりません。
- ワールド モード（レガシーのみ）：レガシー ワールド モードがイネーブルになっているクライアント デバイスは、ワイヤレス デバイスからキャリア セット情報を受信して、それぞれの設定を自動的に調整します。802.11d ワールド モードを使用する場合、Aironet 拡張機能は不要です。
- アソシエートされたクライアント デバイスの電力レベルの制限：クライアント デバイスがワイヤレス デバイスにアソシエートするとき、そのワイヤレス デバイスは最大許可電力レベル設定をクライアントに送信します。

Aironet 拡張機能をディセーブルにすると、上記の機能はディセーブルになりますが、シスコ以外のクライアント デバイスがワイヤレス デバイスにアソシエートしやすくなる場合があります。

Aironet 拡張機能はデフォルトではイネーブルに設定されています。特権 EXEC モードから、次の手順に従って Aironet 拡張機能を無効にします。

	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	**interface dot11radio** {**0** | **1***slot*/*port* }	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 無線は Radio 0、5GHz 無線は Radio 1 です。 802.11n 2.4GHz 無線は Radio 0 です。 802.11n 5GHz 無線は Radio 1 です。
ステップ 3	**no dot11 extension aironet**	Aironet 拡張機能を無効にします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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。

Aironet 拡張機能がディセーブルになっている場合、イネーブルにするには **dot11 extension aironet** コマンドを使用します。

イーサネット カプセル化変換方式の設定

フレームには、使用する上位レイヤ プロトコルを指定するフィールドがあります（IP、IPX、ARP など）。このフィールドは、レシーバ ネットワーク スタックでフレームに適切に指示するために、レシーバ レベルで必要です。

プロトコル表示には、主に 2 つの手法があります。

- EtherType：フレームで実行されるプロトコルを示す 16 ビットの値。EtherType はイーサネット 2.0/DIX ネットワークで使用されます。
- LLC/SNAP：802.2 リンク レイヤ プロトコル表示を可能にする 6 バイト ヘッダー。LLC/SNAP は 802.3 および 802.11 ネットワークで使用されます。

アクセス ポイントが EtherType の情報を使用する有線ネットワーク フレームから受信した場合、この EtherType の情報を SNAP/LLC の情報に変換するメカニズムが必要です。2 つの変換方法があります。

- 802.1H：Cisco Aironet 無線製品に対して良好なパフォーマンスを提供します。
- RFC1042：Cisco Aironet 以外の無線機器との良好な相互運用性を確保するには、この設定を使用します。RFC 1042 は、他の無線機器の製造業者によって使用されており、デフォルト設定となっています。これがデフォルト設定です。

特権 EXEC モードから、次の手順に従ってカプセル化変換方式を設定します。

	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***slot*/*port*}	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 無線は Radio 0、5GHz 無線は Radio 1 です。 802.11n 2.4GHz 無線は Radio 0 です。 802.11n 5GHz 無線は Radio 1 です。
ステップ 3	**payload-encapsulation** **rfc1042** | **dot1h**	カプセル化変換方式を RFC 1042（**rfc1042**、デフォルト設定）または 802.1h（**dot1h**）に設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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。

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有効化と無効化

Reliable multicast messages from the access point to workgroup bridges 設定は、マルチキャスト メッセージの信頼できる送信を、AP にアソシエートしている最大 20 の Cisco Aironet ワークグループ ブリッジに制限します。デフォルト設定の **disabled** では、マルチキャスト送信の信頼性は低下しますが、ワイヤレス デバイスにアソシエートされるワークグループ ブリッジを増やせます。

通常、アクセス ポイントやブリッジでは、ワークグループ ブリッジはクライアント 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 デバイスとして扱われます。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、ワイヤレス デバイスは、Address Resolution Protocol（ARP）パケットなどのマルチキャスト パケットや一部のブロードキャスト パケットを、確実にワークグループ ブリッジに送信します。

AP は、マルチキャスト アドレスにマルチキャスト フレームを送信し、その後、ワークグループ ブリッジから認識される、ユニキャスト フレームにカプセル化されたマルチキャスト フレームをワークグループ ブリッジに再度送信します。この検証メカニズムにより、無線オーバーヘッドが発生し、アクセス ポイントのスループットが低下します。

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)、ワークグループ ブリッジなどワイヤレス デバイスにアソシエートできるインフラストラクチャ デバイスの数は制限されます。ワイヤレス デバイスへの無線リンクを維持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、ワイヤレス デバイスがマルチキャスト 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、ワイヤレス デバイスはマルチキャスト 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、ワイヤレス デバイス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。

(注)　この機能は、固定型のワークグループ ブリッジでの使用に最適です。モバイル型のワークグループ ブリッジの場合、ワイヤレス デバイスのカバレッジ領域内でマルチキャスト パケットを受信できないスポットに入る可能性があり、この場合、ワイヤレス デバイスにアソシエートされていても接続が失われてしまいます。

Cisco Aironet ワークグループ ブリッジでは、最大 8 つのイーサネット対応デバイスとの無線 LAN 接続を提供します。

特権 EXEC モードから、次の手順に従ってカプセル化変換方式を設定します。

(注)　信頼できるマルチキャスト転送を設定するには、この設定はワークグループ ブリッジではなく、AP で行う必要があります。

	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}**	2.4GHz 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 モードに切り替えます。
ステップ 3	**infrastructure-client**	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 メッセージを有効にします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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。

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 メッセージを無効にするには、コマンドの **no** 形式を使用します。

ワークグループ ブリッジは、マルチキャスト フレームそして同じフレームのユニキャスト フレームを受け取るようになり、レシーバ レベルでフレームの重複が生じて非効率となります。

ワークグループ ブリッジの無線レベルでマルチキャスト フレームまたはユニキャスト コピーだけを考慮するようにワークグループ ブリッジを設定するには、次のコマンドを使用します。

コマンド	目的
station-role workgroup-bridge multicast mode {**client** | **infrastructure**}	次のいずれかを設定できます: • 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 AP に信頼できるマルチキャストを設定した場合、ワークグループ ブリッジ レベルでインフラストラクチャを使用することが推奨されます。AP に信頼できるマルチキャストを設定しない場合、ワークグループ ブリッジ レベルでクライアントを使用します。

たとえば、次のコマンドはワークグループ ブリッジ レベルでインフラストラクチャを使用します。

```
WGB(config-if)# station-role workgroup-bridge multicast mode infrastructure
```

Public Secure Packet Forwarding のイネーブル化とディセーブル化

Public Secure Packet Forwarding（PSPF）を使用すると、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 デバイスと、同じアクセス ポイントにアソシエートする他のクライアント デバイスとの偶発的なファイル共有や通信を防ぐことができます。PSPF は、クライアント デバイスに LAN におけるインターネット アクセスだけを許可し、その他の権限は与えません。この機能は、空港や大学の構内などに敷設されている公衆ワイヤレス ネットワークに有用です。

(注)　異なるアクセス ポイントにアソシエートするクライアント間での通信を防ぐために、ワイヤレス デバイスを接続するスイッチに保護ポートを設定する必要があります。保護ポートの設定方法については、「保護ポートの設定」セクション（6-30 ページ）を参照してください。

ワイヤレス デバイス上で CLI コマンドを使用して PSPF をイネーブルまたはディセーブルにするには、ブリッジ グループを使用します。次の文書に、ブリッジ グループに関する詳細な説明と、ブリッジ グループを実装する手順が収められています。

- 『*Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2*』。このリンクをクリックすると、「Configuring Transparent Bridging」の章が表示されます。
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcfpart1/bcftb.htm

PSPF は Web ブラウザ インターフェイスを使用して有効および無効にできます。PSPF 設定は [Radio Settings] ページで行います。

PSPF はデフォルトでディセーブルに設定されています。特権 EXEC モードから、次の手順に従って PSPF 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	**interface dot11radio** {**0** | **1***slot*/*port*}	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 無線は Radio 0、5GHz 無線は Radio 1 です。 802.11n 2.4GHz 無線は Radio 0 です。 802.11n 5GHz 無線は Radio 1 です。
ステップ 3	**bridge-group** *group* **port-protected**	PSPF を有効にします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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。

PSPF を無効にするには、コマンドの **no** 形式を使用します。

保護ポートの設定

無線 LAN の異なるアクセス ポイントにアソシエートするクライアント デバイス間での通信を防ぐために、無線デバイスを接続するスイッチに保護ポートを設定することができます。また、通信が発生しないようにする AP 同士をつなぐ同じスイッチのポートを分離する必要があります。

特権 EXEC モードから、次の手順に従ってスイッチ上のポートをプロテクテッド ポートとして定義します。

	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** *interface-id*	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、設定するスイッチポート インターフェイスのタイプと番号を **gigabitethernet0/1** のように入力します。
ステップ 3	**switchport protected**	インターフェイスを保護ポートに設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show interfaces** *interface-id* **switchport**	入力内容を確認します。
ステップ 6	**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。

保護ポートをディセーブルにするには、**no switchport protected** インターフェイス コンフィギュレーション コマンドを使用します。このコマンドは、個別のスイッチ レベルでのみ有効です。これは異なるスイッチに接続された AP は分離しません。このコマンドは、通信が発生しないようにする任意のスイッチのすべての AP のポートで使用できます。また、AP にプライベート VLAN 設定を使用できます。

(注)　無線ドメイン サービス(WDS)を使用する場合、AP と そのWDS と間の通信を遮らないようにします。

プライベート VLAN の設定、保護ポート、およびポート ブロッキングの詳細については、次の URL にある『*Catalyst 3750 Software Configuration Guide*』を参照してください:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_55_se/configuration/guide/scg3750.html

ビーコン間隔と DTIM の設定

ビーコン間隔はアクセス ポイントのビーコン間の時間（キロマイクロ秒）です。1 Kμsec は 1,024 マイクロ秒に相当します。常にビーコン間隔の倍数となるデータ ビーコン レートにより、ビーコンに Delivery Traffic Indication Message（DTIM）が格納される頻度が決定されます。DTIM は、省電力モードのクライアント デバイスに、パケットがクライアント待ちであることを通知します。

たとえば、ビーコン間隔がデフォルト設定の 100 に設定され、DTIM がデフォルト設定の 2 に設定されている場合、AP は DTIM を含むビーコンを 2 ビーコンごと、または 200 Kμsec ごと、または 200 ミリ秒ごとに送信します。1 Kμsec は 1,024 マイクロ秒に相当します。

デフォルトのビーコン間隔は 100、デフォルトの DTIM は 2 です。特権 EXEC モードから、次の手順に従ってビーコン間隔および DTIM を設定します。

	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***slot*/*port*}	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 802.11n 2.4GHz 無線は 0 です。 5GHz 無線および 802.11n 5GHz 無線は 1 です。
ステップ 3	**beacon period** *value*	ビーコン間隔を 20 ～ 4000 の範囲で設定します。値をキロマイクロ秒で入力します。
ステップ 4	**beacon dtim-period** *value*	DTIM を 1 ～ 100 の範囲で設定します。値をキロマイクロ秒で入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**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。

RTS しきい値と再試行回数の設定

Request To Send（RTS; 送信要求）しきい値は、パケットの送信前にワイヤレス デバイスが RTS を発行するときのパケット サイズを決定します。多数のクライアント デバイスがワイヤレス デバイスにアソシエートされているエリアや、クライアントが遠く分散しているために、ワイヤレス デバイスは検知できても、クライアント同士が互いに検知できないエリアでは、RTS しきい値を低く設定すると効果的です。設定値を 0 ～ 23472347 バイトの範囲で入力します。

最大 RTS 再試行は、ワイヤレス デバイスが無線を介したパケット送信の試行を中止するまでに RTS を発行する最大回数です。1 ～ 128 の範囲の値を入力します。

どのアクセス ポイントおよびブリッジでもデフォルトの RTS しきい値は 2347 で、デフォルトの最大 RTS 再試行回数の設定は 3264 です。特権 EXEC モードから、次の手順に従って RTS しきい値と最大 RTS リトライを設定します。

	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***slot*/*port*}	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	**rts threshold** *value*	RTS しきい値を設定します。RTS しきい値は 0 ～ 23472347 の範囲で入力します。
ステップ 4	**rts retries** *value*	最大 RTS リトライ回数を設定します。1 ～ 128 の範囲の値を入力します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**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。

RTS 設定をデフォルトにリセットする場合は、コマンドの **no** 形式を使用します。

最大データ パケット再試行回数の設定

最大データ リトライ設定は、ワイヤレス デバイスがパケット送信を放棄し、そのパケットをドロップするまでに行うパケット送信の最大再送回数です。

デフォルト設定は 32 です。特権 EXEC モードから、次の手順に従って最大データ リトライを設定します。

	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***slot*/*port*}	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	**packet retries** *value* [**drop-packet**]	最大データ リトライ回数を設定します。1 ～ 128 の範囲の値を入力します。 drop-packet オプションを使用する場合、デバイスは現在のパケットの送信を停止し、接続を解除せずに、キューにある次のパケットの送信を試みます。 drop-packet オプションを使用しない場合、ワイヤレス デバイスはリンクが使用可能でないと判断して、現在のパケットの送信を停止し、接続を終了します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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。

設定をデフォルトにリセットする場合は、コマンドの **no** 形式を使用します。

フラグメンテーションしきい値の設定

フラグメンテーションしきい値は、断片化されて複数のブロックとして送信されるパケットの最小サイズを決定します。通信状態の悪いエリアや電波干渉が非常に多いエリアでは、低い数値を設定します。

デフォルト設定は 23382346 バイトです。特権 EXEC モードから、次の手順に従ってフラグメンテーションしきい値を設定します。

	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***slot*/*port*}	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	**fragment-threshold** *value*	フラグメンテーションしきい値を設定します。2.4GHz 無線の場合は 256 ～ 2346 バイトの間で入力します。5GHz 無線の場合は 256 ～ 2346 バイトの間で入力します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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。

設定をデフォルトにリセットする場合は、コマンドの **no** 形式を使用します。

802.11g 無線の short スロット時間のイネーブル化

802.11g、2.4GHz 無線のスループットは、短いスロット時間を有効にすることで向上します。スロット時間を標準の 20 マイクロ秒から 9 マイクロ秒の short スロット時間まで短縮すると、全体のバックオフが減少し、スループットが向上します。バックオフは、スロット時間の倍数であり、LAN 上にパケットを送信するまでにステーションが待機するランダムな長さの時間です。

多くの 802.11g 無線は short スロット時間をサポートしていますが、サポートしていないものもあります。短いスロット時間を有効にした場合、ワイヤレス デバイスは、802.11g、2.4GHz 無線にアソシエートされたすべてのクライアントが短いスロット時間をサポートしている場合だけこれを使用します。

短いスロット時間は、802.11g、2.4GHz 無線だけでサポートされています。短いスロット時間は、802.11b クライアントではサポートされていません。短いスロット時間を有効にすると、802.11b クライアントは、AP 無線への参加または AP 無線との通信を行えなくなります。short スロット時間は、デフォルトではディセーブルに設定されています。

無線インターフェイス モードで、次のコマンドを入力して短いスロット時間を有効にします。

```
ap(config-if)# short-slot-time
```

no short-slot-time を入力し、Short スロット時間をディセーブルにします。

キャリア話中検査の実行

キャリア ビジー テストを実行して、ワイヤレス チャネルでの無線活動をチェックします。キャリア ビジー テストでは、キャリア検査を実行して検査結果を表示するまでの約 4 秒間、ワイヤレス デバイスはワイヤレス ネットワーキング デバイスとのアソシエーションをすべて停止します。

特権 EXEC モードで、次のコマンドを入力して、キャリア ビジー テストを実行します。

dot11 *interface-number* **carrier busy**

interface-number については、**dot11radio 0** を入力して、2.4GHz 無線上の検査を実行するか、**dot11radio 1** を入力して、5GHz 無線上の検査を実行します。

(注)　インターフェイスは、キャリア ビジー テストを実行するためにイネーブルにする必要があります。

show dot11 carrier busy コマンドを入力して、キャリア話中検査結果を再表示します。

```
ap#dot11 dot11Radio 1 carrier busy
ap#show dot11 carrier busy
Frequency  Carrier Busy %
---------  --------------
   5180           2
   5200           0
   5220           2
   5240           1
   5260           1
   5280           0
   5300           1
   5320           0
   5500           0
   5520           0
   5540           0
   5560           0
   5580           0
   5660           0
   5680           0
   5700           0
   5745           0
   5765           0
   5785           0
   5805           0
   5825           0
```

VoIP パケット処理の設定

アクセス ポイントの無線ごとの VoIP パケット処理の質は、ワイヤレス サービス クラス 5（ビデオ）およびワイヤレス サービス クラス 6（音声）の低遅延における 802.11 MAC 動作を強化することで改善できます。

アクセス ポイントの VoIP パケット処理を設定する手順は、次のとおりです。

ステップ 1　ブラウザを使用して、アクセス ポイントにログインします。

ステップ 2　Web ブラウザ インターフェイスの上部にあるタスク メニューで [Services] をクリックします。

ステップ 3　左側のメニューで、[Stream] をクリックします。

[Stream] ページが表示されます。

ステップ 4　設定する無線のタブをクリックします。

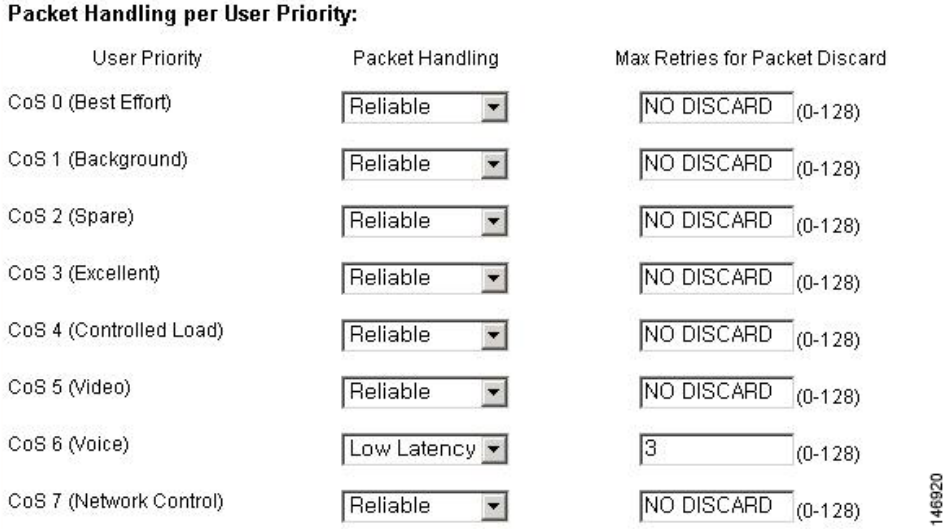
ステップ 5　CoS 5（ビデオ）および CoS 6（音声）の両方のユーザの優先順位について、[Packet Handling] ドロップダウン リストから [Low Latency] を選択し、パケット廃棄の最大リトライ回数の値を、対応するフィールドに入力します。他のキューのパケットはキューが解除され、遅延に影響されやすいデータは他のトラフィックよりも優先して処理されます。

最大再試行回数のデフォルト値は、Low Latency 設定では 3 です（図 6-2）。この値は、損失したパケットを廃棄する前に、アクセス ポイントがパケットを再送信しようとする回数を示します。

（注）　CoS 4（負荷制御）ユーザの優先順位およびその最大再試行回数も設定できます。

ステップ 6　[Apply] をクリックします。

図 6-2　　パケット処理の設定



CLI を使用して VoIP パケット処理を設定することも可能です。CLI を使用して VoIP パケット処理を設定するための Cisco IOS コマンドのリストについては、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

再試行のレベルを定義すると、それらのフレームを送信する速度も設定できるようになります。これは、ページ下部にある [**Low Latency Packet Rates**] セクションで行えます。各レートを次に設定できます。

- Nominal：AP は、低遅延パケットを送信するときに、このレートを使用します（クライアントの信号レベルに応じて、最初に高速レートを使用）。
- Non-nominal：AP はそのレートを使用しないようにしますが、公称レートが使用できない場合にはこれを使用します。
- Disabled：AP は、そのレートを使用することはありません。

CLI から、次の無線インターフェイス コンフィギュレーション コマンドを使用します（CLI コマンドは GUI ページよりも多くのオプションを提供します）：

packet max-retries *number 1 number 2* **fail-threshold** *number 3 number 4* **priority** *value* **drop-packet**

このコマンドの各項目の意味は以下のとおりです。

- Number 1：特定のプライオリティ レベルで、正しく受信されなかった（確認応答がなかった）パケットの再送信を AP が試みる回数を定義します。number 1 に達すると、AP はパケットをドロップし、（同じ受信者に）次のパケットの送信を試みます。
- Number 3：許容可能なしきい値をフェイル レートが超えたと AP が判断する前に、何回連続して（1 人の受信者に送信された）パケットが失敗できるかを指定します
- Number 2：失敗しきい値を超えた場合でも、AP は失敗したパケットを再送信するできますが、しきい値を超過する前とは試行回数が異なります。これは、number 2 です。たとえば、最初は各パケットを 3 回（number 1）再送信するよう設定できます。その後、AP が一定の数の連続するパケット（たとえば、number 3 として指定する 100）の送信に失敗した場合、条件が劣化しているため、AP が後続の各パケットの再送信を 1 回（number 2）だけ試みるように指定できます。
- Number 4：ターゲット クライアントのアソシエートを解除する前に、number 2 の再送信で、AP がさらにどれだけの連続するパケットの再送信を試みるかを指定します。

例：

```
ap(config-if)# packet max-retries 3 0 fail-threshold 100 500 priority 6 drop-packet
```

この例では、AP はプライオリティ レベル 6 の各パケットの再送信を 3 回試行します（number one = 3）。連続するパケット 100 個が同じ宛先に対して失敗した場合（number three = 100）、AP はその宛先に対して連続するパケットを 1 度だけ送信します（number two = 0）。同じ宛先に対してさらに 500 のパケットが失敗すると（number four = 500）、AP はそのクライアントを切断します。

GUI を使用する場合、number one は手動で定義します（デフォルト値は 3）。number 2 のデフォルト値は 0、number 3 のデフォルト値は 100、number 4 のデフォルト値は 500 です。これらの数値は CLI から変更できます。

```
ap(config-if)#packet max-retries ?
  <0-128>  # packet retries before dropping pkt if first fail-threshold not
           reached


ap(config-if)#packet max-retries 3 ?
  <0-128>  # packet retries before dropping pkt if 2nd fail-threshold not
           reached

ap(config-if)#packet max-retries 3 0 ?
  fail-threshold  maximum # consecutive dropped packets thresholds

ap(config-if)#packet max-retries 3 0 fa
ap(config-if)#packet max-retries 3 0 fail-threshold ?
  <0-1000>  # consecutive dropped packets before switching max-retries
            しきい値

ap(config-if)#packet max-retries 3 0 fail-threshold 100 ?
  <0-1000>  number of consecutive dropped packets before disassociating client

ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 ?
  priority  qos user-priority

ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 p
ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 priority ?
  <0-7>  qos user-priority number
```

```
ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 priority 6 ?
  drop-packet  Don't retry pkts, just drop packets when max retries reached

ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 priority 6 d
ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 priority 6 drop-packet
```

低遅延パケット レートも、公称レートと許可されるレートを定義する次のコマンドを使って、インターフェイス レベルで定義できます。

traffic-stream priority *value* **sta-rates {[***nominal rates***] | [***rates***]}**

```
ap(config-if)# traffic-stream priority 6 sta-rates ?
  12.0      Allow 12.0 Mb/s rate
  18.0      Allow 18.0 Mb/s rate
  24.0      Allow 24.0 Mb/s rate
  36.0      Allow 36.0 Mb/s rate
  48.0      Allow 48.0 Mb/s rate
  54.0      Allow 54.0 Mb/s rate
  6.0       Allow 6.0 Mb/s rate
  9.0       Allow 9.0 Mb/s rate
  nom-12.0  Allow Nominal 12.0 Mb/s rate
  nom-18.0  Allow Nominal 18.0 Mb/s rate
  nom-24.0  Allow Nominal 24.0 Mb/s rate
  nom-36.0  Allow Nominal 36.0 Mb/s rate
  nom-48.0  Allow Nominal 48.0 Mb/s rate
  nom-54.0  Allow Nominal 54.0 Mb/s rate
  nom-6.0   Allow Nominal 6.0 Mb/s rate
  nom-9.0   Allow Nominal 9.0 Mb/s rate
 <cr>
```

例:

```
ap(config-if)# traffic-stream priority 6 sta-rates nom-5.5 nom-11.0 nom-6.0 9.0 nom-12.0
nom-24.0
```

音声キューの場合（具体的には UP 6）、音声キューでパケットを送信するために使用できるレートを決定するために interface コマンドの packet speed を使用できます。

packet speed 5.5 11.0 6.0 9.0 12.0 24.0 priority 6

packet speed コマンドは許可されるレートの定義を主に行うのに対し、traffic-stream priority コマンドは許可されたレートの中で優先されるレートも定義します。音声キューで両方のコマンドを使用する場合、traffic stream priority コマンドで公称として定義されたレートが最初に試され、その後に非公称レートやパケット速度レートが試されます。

ClientLink の設定

Cisco ClientLink（Beam Forming とも呼ばれます）はインテリジェントなビームフォーミング テクノロジーです。RF 信号を 802.11a/g デバイスに送信して、パフォーマンスを 65 % 向上させ、カバレッジを最大 27 % 拡大し、カバレッジ ホールを減少させます。

Cisco ClientLink は、既存の混合クライアント ネットワークの 802.11a/g デバイスと単一トラフィック ストリームのみをサポートする 802.11n クライアントの耐用年数を延長するのに役立ちます。Cisco ClientLink は、802.11n に移行し、種類に関係なく、ネットワーク上のすべてのクライアントで必要な帯域幅およびスループットを確保することを求める組織にとって有益です。

(注)　CLientLink バージョン 1 は 802.11 a/g デバイスをサポートし、ClientLink バージョン 2 は単一空間ストリームがある 802.11 a/g デバイスと 802.11n デバイスをサポートします。

(注)　1040、702 シリーズ アクセス ポイントでは、ClientLink はサポートされていません。

CLI を使用した ClientLink の設定

ClientLink を有効にするには、インターフェイス コンフィギュレーション モードの 802.11n 無線インターフェイスで、次の CLI コマンドを入力します。

```
beamform ofdm
```

(注)　現在、ClientLink 設定オプションは、GUI では使用できません。

ClientLink を開始するしきい値を決定するには、次のコマンドを使用します。

ap(config-if)# **beamform rssi** *30to128-rssi-threshold-in-dBm*

ClientLink はデフォルトでは無効に設定されています。詳細は、cisco.com の次の URL を参照してください。
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10092/white_paper_c11-516389.html

無線機能のデバッグ

無線機能のデバッグを開始するには、**debug dot11** 特権 EXEC コマンドを使用します。デバッグ操作を停止するには、このコマンドの **no** 形式を使用します。コマンド構文は次のとおりです。

```
[no] debug dot11
{events | packets | forwarding | mgmt | network-map | syslog | virtual-interface}
```

構文は、表 6-4 に示すとおりです。

表 6-4　debug dot11 コマンドの構文

Syntax	説明
events	無線に関連するすべてのイベントのデバッグをアクティブにします。
パケット	送受信された無線パケットのデバッグをアクティブにします。
フォワーディング	転送された無線パケットのデバッグをアクティブにします。
mgmt	無線アクセス ポイントの管理アクティビティのデバッグをアクティブにします。
network-map	無線アソシエーション管理のネットワークマップのデバッグをアクティブにします。

Syntax	説明
syslog	無線システム ログのデバッグをアクティブにします。
virtual interface	無線仮想インターフェイスのデバッグをアクティブにします。

この例では、無線に関連するすべてのイベントのデバッグを開始する方法を示します。

```
AP# debug dot11 events
```

この例では、無線パケットのデバッグを開始する方法を示します。

```
AP# debug dot11 packets
```

この例では、無線システム ログのデバッグを開始する方法を示します。

```
AP# debug dot11 syslog
```

この例では、無線に関連するすべてのイベントのデバッグを停止する方法を示します。

```
AP# no debug dot11 events
```

(注)　デバッグが有効になっていない状態が、コマンドのデフォルトです。

802.11r の設定

802.11r は無線ドメイン サービスを使用して同じサブネット上のアクセス ポイント間で高速ローミングをイネーブルにします。802.11r をイネーブルにすると、モビリティ ドメイン情報要素（MDIE）が AP はビーコンでアドバタイズされます。同じ WDS にアソシエートされたすべての AP で同じ MDIE がアナウンスされます。WDS BVI IP アドレス（IPv4 または IPv6）の最後の 2 バイトは MDIE として使用されます。802.11r 互換性のあるクライアントは、この MDIE を使用して、同じドメインに属していて、高速ローミングが可能な AP を識別します。

FT プロトコルを使用して現在の AP からターゲット AP に移動するクライアントでは、メッセージ交換は次の 2 つの方法のいずれかを使用して行われます。

- Over-the-Air：クライアントは、FT 認証アルゴリズムを使用する IEEE 802.11 認証を使用して、ターゲット AP と直接通信を行います。これを設定するには、次のコマンドを使用します。
  ap(config-if)**#dot11 dot11r pre-authentication over-air**
- Over-the-DS：クライアントは、現在の AP 経由でターゲット AP と通信します。クライアントとターゲット AP との間の通信は、クライアントと現在の AP 間の FT アクション フレームで実行され、その後 WDS 経由でターゲット AP に送信されます。これを設定するには、次のコマンドを使用します。
  ap(config-if)**#dot11 dot11r pre-authentication over-ds**

AP 無線では、802.11r サポートをイネーブルにしてローミング ダイアログを無線（デフォルト）で行うか DS 上で行うかを決定し、クライアントがローミング トランザクションを完了するまでに許可される最大時間を設定できます。クライアントがローミング トランザクションを完了するまでに許可される最大時間は、リアソシエーション タイマーと呼ばれます。このタイマーは、攻撃者が多数の 802.11r トランザクションを開き、いずれも完了しないという状態（これにより AP が過負荷状態になる）を防ぐことにより、ネットワークのセキュリティを強化できます。このタイマーは次のコマンドで設定できます。

ap(config-if)**#dot11 dot11r reassociation-time value** *20to1200-timeout-value-in-milli-seconds*

例：DS 上の認証で 802.11r をイネーブルにして、リアソシエーションの時間値を 200 ミリ秒にします。

```
aap(config-if)#dot11 dot11r pre-authentication over-ds
ap(config-if)#dot11 dot11r reassociation-time value 200
```

（注）　ネットワークに導入する前に 802.11r をテストします。一部の非 802.11r クライアントは 802.11r MDIE をサポートせず、802.11r 環境で正しく機能しません。

SSID および無線インターフェイスのトラフィック レート制限の設定

無線クライアント デバイスによる使用帯域幅を制限するには、無線クライアント デバイス間のトラフィック レートを制限できます。このレート制限機能には、次のような特徴があります。

- 各 SSID で設定でき、片方または両方の無線インターフェイスに適用できる
- IPv4 の TCP/UDP にのみ適用されるIPv6 トラフィックに対してはサポートされない
- 無線インターフェイスの入力トラフィックおよび出力トラフィックの両方に適用される

レート制限機能は VLAN で利用可能です。同じインターフェイス上で複数の SSID が設定されている場合、VLAN なしではレート制限は設定できません。

複数の SSID の設定については、第 7 章「複数の SSID の設定」を参照してください。

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。

Quality of Service（QoS）機能の一部として、ユーザ定義の基準に基づいて、トラフィックのクラスの入力または出力送信レートを制限するレート制限機能があります。詳細については、第 15 章「QoS の設定」を参照してください。

レート制限の設定

レート制限を設定するには、コマンド
rate-limit {tcp | udp} {input | output} data-rate *rate* **burst-size** *size* を使用します。ここで、

- date-rate はデータ転送の平均レートで、キロビット/秒で指定されます。
- burst-size はトラフィックがスロットリングされる前に転送できる合計データです。これはキロビットで指定されます。

これらのパラメータは 8 の倍数の最近値に変換および制限されます。data-rate はキロバイト/秒、burst-size はバイトに変換され、レート制限で考慮されます。

これらのパラメータの機能を理解するために、次の例を考えます。平均データ速度を 10 バイト/秒、バースト サイズを 20 バイトとします。ここで適用されるレート制限は、2 秒間（バースト サイズ/平均レートとして計算）となり、合計データ伝送は 20 バイトを超えることはできません。これにより、平均データ速度が 10 バイト/秒を超えない限り、1 秒あたりにより多くのデータを送信することができます。

GUI 経由で設定するには、[Security] > [SSID Manager] にアクセスします。[Rate Limit Parameters] セクションで、必要に応じて TCP または UDP の入力トラフィックまたは出力トラフィックを制限できます。また、それぞれのレートおよびバースト サイズも指定できます。

レート制限統計情報の表示

レート制限の統計情報を表示するには、任意のインターフェイスに設定された各 SSID について、次のコマンドを使用します：**show interface dot11radio {0 | 1} qos-info**

統計情報カウンタをクリアするには、次のコマンドを使用します：**clear counters dot11Radio {0 | 1}**

GUI 経由でレート制限統計情報を表示するには、[Network] > [Network Interface] > [Radio0-802.11N 2.4GHz] または [Radio1-802.11N 5GHz] にアクセスします。統計情報をクリアするには、[Clear] をクリックします。