複数の SSID の設定

この章では、アクセス ポイント / ブリッジに複数の Service Set Identifiers（SSID）を設定して、管理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。

- 複数の SSID の概要（P. 7-2）
- 複数の SSID の設定（P. 7-4）
- 複数の基本 SSID の設定（P. 7-8）
- SSID に対する IP リダイレクションの割り当て（P. 7-12）
- SSIDL Information Element（IE; 情報要素）に SSID を含める（P. 7-14）

複数の SSID の概要

SSID は、無線ネットワーキング デバイスが無線接続を確立および維持するために使用する、一意の識別子です。ネットワークまたはサブネット上の複数のアクセス ポイントは、同じ SSID を使用できます。SSID では大文字と小文字が区別され、最大 32 文字の英数字を使用できます。SSID にスペースは使用できません。

アクセス ポイント / ブリッジには最大 16 個の SSID を設定して、それぞれの SSID に異なる設定を割り当てることができます。すべての SSID は同時にアクティブです。つまり、クライアント デバイスは、いずれかの SSID を使用してアクセス ポイント / ブリッジにアソシエートすることができます。これらは各 SSID に割り当てることができる設定です。

- Virtual Local Area Network（VLAN; バーチャル LAN）
- クライアント認証方式

（注）　クライアント認証タイプの詳細は、第 10 章「認証タイプの設定」を参照してください。

- SSID を使用するクライアント アソシエーションの最大数
- SSID を使用するトラフィックの RADIUS アカウンティング
- ゲスト モード
- 認証ユーザ名とパスワードを含む、リピータ モード
- クライアント デバイスから受信したパケットのリダイレクション

アクセス ポイント / ブリッジが設定に SSID を指定しないクライアント デバイスからアソシエートできるようにする場合、ゲスト SSID を設定できます。アクセス ポイント / ブリッジには、そのビーコンにゲスト SSID が含まれます。デフォルト SSID *tsunami* は、ゲスト モードに設定されます。ただし、ネットワークの安全性を確保するため、ゲスト モード SSID を無効にする必要があります。

アクセス ポイント / ブリッジがリピータか、リピータの親として機能するルート アクセス ポイントである場合は、リピータ モードで使用するために SSID を設定できます。リピータ モード SSID に認証ユーザ名とパスワードを割り当てると、クライアント デバイスと同様にリピータでネットワークへの認証が可能になります。

ネットワークが VLAN を使用する場合、1 つの SSID を VLAN に割り当てることができ、SSID を使用するクライアント デバイスはその VLAN 内にグループ化されます。

SSID に対するソフトウェア バージョンの影響

シスコは、複数のインターフェイスにおける SSID パラメータの設定を容易にするため、Cisco IOS リリース 12.3(2)JA でグローバル モード SSID 設定を採用しました。インターフェイス レベルでの SSID パラメータの設定は、下位互換性を保つために Cisco IOS リリース 12.3(2)JA でサポートされていましたが、Cisco IOS リリース 12.3(4)JA より後のリリースでは完全に無効になります。表 7-1 に Cisco IOS リリースでサポートされる SSID 設定方式をリストします。

表 7-1　Cisco IOS リリースでサポートされている SSID 設定方式

Cisco IOS リリース	サポートされる SSID 設定方式
12.2(15)JA	インターフェイス レベルのみ
12.3(2)JA	インターフェイス レベルとグローバルの両方
12.3(4)JA	インターフェイス レベルとグローバルの両方。グローバル モードで保存されたすべての SSID
12.3(4)JA 以降	グローバルのみ

Cisco IOS リリース 12.3(4)JA は、Command-Line Interface（CLI; コマンドライン インターフェイス）でインターフェイス レベルでの SSID パラメータの設定をサポートしますが、SSID はグローバル モードで保存されます。すべての SSID をグローバル モードで保存すると、Cisco IOS リリース 12.3(4)JA より後のリリースにアップグレードする場合に SSID 設定は正しくなります。

Cisco IOS リリース 12.3(2)JA 以前のリリースから 12.3(4)JA より後のリリースにアップグレードする必要がある場合は、コンフィギュレーション ファイルを保存し、ターゲット リリースにアップグレードし、保存したコンフィギュレーション ファイルをロードします。このプロセスにより、インターフェイス レベル SSID 設定がグローバル モードに変換されます。12.3(4)JA 以前のリリースから 12.3(4)JA 以降のリリースに直接アップグレードする場合は、インターフェイス レベル SSID 設定は削除されます。

Cisco IOS リリース 12.3(4)JA からソフトウェア バージョンをダウングレードする場合、作成した SSID は無効になります。ダウングレード後に SSID の再設定を避けるため、Cisco IOS リリース 12.3(4)JA にアップグレードする前に以前のソフトウェア バージョンのコンフィギュレーション ファイルのコピーを保存します。Cisco IOS リリース 12.3(4)JA からソフトウェア バージョンをダウングレードする場合は、保存されたコンフィギュレーション ファイルをダウングレード後にロードします。

表 7-2 は、Cisco IOS リリース 12.2(15)JA を実行するアクセス ポイント / ブリッジの SSID 設定の例と Cisco IOS リリース 12.3(4)JA にアップグレードした後に表示される設定を示しています。

表 7-2　例：アップグレード後にグローバル モードに変換された SSID 設定

12.2(15)JA の SSID 設定	12.3(4)JA へのアップグレード後の SSID 設定
interface dot11Radio 0 　ssid engineering 　authentication open 　vlan 4 interface dot11Radio 1 　ssid engineering 　authentication open 　vlan 5	dot11 ssid engineering 　authentication open 　vlan 5 ! interface dot11Radio 0 　ssid engineering interface dot11Radio 1 　ssid engineering

各インターフェイスの VLAN 設定は、グローバル SSID 設定に保持されることに注意してください。

複数の SSID の設定

次の項では、複数の SSID の設定情報について説明します。

- デフォルトの SSID 設定（P. 7-4）
- SSID のグローバルな作成（P. 7-4）
- SSID を制限するための RADIUS サーバの使用（P. 7-6）

（注）　Cisco IOS リリース 12.3(4)JA およびそれ以降では、SSID をグローバルに設定し、特定の無線インターフェイスに適用します。「SSID のグローバルな作成」の項（P. 7-4）の手順に従って SSID をグローバルに設定します。

デフォルトの SSID 設定

Cisco IOS リリース 12.3(4)JA では、デフォルト SSID はありません。

SSID のグローバルな作成

Cisco IOS リリース 12.3(2)JA およびそれ以降では、SSID をグローバルに、または特定の無線インターフェイスに設定することができます。**dot11 ssid** グローバル設定コマンドを使用して SSID を作成すると、**ssid** 設定インターフェイス コマンドを使用して SSID を特定のインターフェイスに割り当てることができます。

SSID がグローバル コンフィギュレーション モードで作成された場合、**ssid** コンフィギュレーション インターフェイス コマンドは SSID をインターフェイスに割り当てますが、ssid コンフィギュレーション モードに移行しません。ただし、SSID がグローバル コンフィギュレーション モードで作成されていない場合、**ssid** コマンドにより CLI は新規 SSID のために SSID コンフィギュレーション モードに移行します。

（注）　ソフトウェア バージョンを以前のリリースにダウングレードする場合、Cisco IOS リリース 12.3(4)JA およびそれ以降で作成された SSID は無効になります。

特権 EXEC モードから SSID をグローバルに作成する手順は、次のとおりです。SSID を作成した後、特定の無線インターフェイスに割り当てることができます。

	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-string*	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 3	**認証クライアント** **username** *username* **password** *password*	（オプション）アクセス ポイント / ブリッジがリピータ モードでネットワークへの認証に使用する、認証ユーザ名とパスワードを設定します。ルート アクセス ポイントまたは他のリピータとアソシエートするためにリピータ アクセス ポイントが使用する SSID にユーザ名とパスワードを設定します。

	コマンド	目的
ステップ 4	**accounting** *list-name*	（オプション）この SSID の RADIUS アカウンティングを有効にします。*list-name* には、アカウンティング方式のリストを指定します。方式のリストの詳細は、次のリンクをクリックしてください。http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcfpart1/bcftb.htm
ステップ 5	**vlan** *vlan-id*	（オプション）ネットワーク上の VLAN に SSID を割り当てます。SSID を使用してアソシエートするクライアント デバイスは、この VLAN にグループ化されます。1 つの SSID のみを VLAN に割り当てることができます。
ステップ 6	**guest-mode**	（オプション）アクセス ポイント / ブリッジのゲスト モード SSID として SSID を指定します。アクセス ポイント / ブリッジにはそのビーコンに SSID が含まれ、SSID を指定しないクライアント デバイスからアソシエーションが可能です。
ステップ 7	**infrastructure-ssid** [**optional**]	（オプション）他のアクセス ポイントとワークグループ 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 SSID を指定します。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 デバイスは任意の SSID を使用してアクセス 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、**オプションの**キーワードも入力しない限り、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 8	**interface dot11radio** { **0** | **1** }	SSID を割り当てる無線インターフェイスに対するインターフェイス コンフィギュレーション モードに入ります。2.4GHz 無線は無線 0、5GHz 無線は無線 1 です。
ステップ 9	**ssid** *ssid-string*	ステップ 2 で作成したグローバル SSID を無線インターフェイスに割り当てます。
ステップ 10	**end**	特権 EXEC モードに戻ります。
ステップ 11	**copy running-config startup-config**	（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。

（注）　各 SSID に認証タイプを設定する場合は、**ssid** コマンドの認証オプションを使用します。認証タイプを設定する方法の詳細は、第 10 章「認証タイプの設定」を参照してください。

SSID、または SSID 機能を無効にする場合は、コマンドの **no** フォームを使用します。

次の例は、以下の方法を示しています。

- SSID の名前の指定
- RADIUS アカウンティングの SSID の設定
- この SSID を使用してアソシエートすることができるクライアント デバイスの最大数を 15 に設定します。
- SSID の VLAN への割り当て
- SSID の無線インターフェイスへの割り当て

```
AP# configure terminal
AP(config)# dot11 ssid batman
AP(config-ssid)# accounting accounting-method-list
AP(config-ssid)# max-associations 15
AP(config-ssid)# vlan 3762
AP(config-ssid)# exit
AP(config)# interface dot11radio 0
AP(config-if)# ssid batman
```

グローバルに設定された SSID の表示

このコマンドを使用して、グローバルに設定された SSID の設定の詳細を表示します。

```
AP# show running-config ssid ssid-string
```

SSID 内のスペースの使用

SSID にスペースを含めることができますが、特に SSID の末尾など、SSID に誤ってスペースを追加しないように注意してください。末尾にスペースを追加した場合、同じ SSID が同じアクセス ポイント / ブリッジに設定されたようにみえます。アクセス ポイント / ブリッジに同じ SSID を設定した場合、**show dot11 associations** 特権 EXEC コマンドを使用して SSID の末尾のスペースをチェックします。

たとえば、**show configuration** 特権 EXEC コマンドのこの出力例では、SSID のスペースを表示しません。

```
ssid buffalo
    vlan 77
    authentication open

ssid buffalo
    vlan 17
    authentication open

ssid buffalo
    vlan 7
    authentication open
```

ただし、**show dot11 associations** 特権 EXEC コマンドの出力例は SSID のスペースを表示します。

```
SSID [buffalo] :
SSID [buffalo] :
SSID [buffalo] :
```

SSID を制限するための RADIUS サーバの使用

不正な SSID を使用してクライアント デバイスがアクセス ポイント / ブリッジにアソシエートするのを防ぐために、クライアントが RADIUS 認証サーバで使用する必要がある正しい SSID のリストを作成できます。

SSID 認証プロセスは、次の手順から構成されます。

1. クライアント デバイスは、アクセス ポイント / ブリッジに設定された任意の SSID を使用してアクセス ポイント / ブリッジにアソシエートします。
2. クライアントは RADIUS 認証を開始します。

3. RADIUS サーバは、クライアントが使用できる SSID のリストを返します。アクセス ポイント / ブリッジは、クライアントによって使用される SSID と一致するものがリストにあるかどうかチェックします。次の 3 つの結果があります。

   a. クライアントがアクセス ポイント / ブリッジにアソシエートするために使用した SSID が、サーバによって返された許可されたリストのエントリと一致する場合は、すべての認証要件が完了後クライアントはネットワーク アクセスが許可されます。

   b. アクセス ポイント / ブリッジが、SSID の許可されたリストのクライアントとの一致を見つけることができない場合は、クライアントとのアソシエーションを解除します。

   c. RADIUS サーバがクライアントの SSID（リストなし）を返さない場合、管理者はリストを設定しておらず、クライアントはアソシエートすることができ、認証を試みます。

RADIUS サーバからの SSID の許可されたリストは、シスコ Vendor-Specific Attribute（VSA; ベンダー固有属性）の形式です。インターネット技術特別調査委員会（IETF; Internet Engineering Task Force）のドラフト規格では、アクセス ポイント / ブリッジと RADIUS サーバ間での、ベンダー固有の属性（属性 26）を使用した、ベンダー固有の情報の通信方法を指定しています。ベンダーは、Vendor-Specific Attributes（VSA; ベンダー固有の属性）を使用することで、汎用には適していない各社固有の拡張属性に対応できます。シスコの RADIUS 実装では、仕様で推奨される形式を使用することで、ベンダー固有オプションを 1 つサポートします。シスコのベンダー ID は 9 です。サポートされるオプションはベンダータイプ 1 であり、*cisco-avpair* という名前が付けられています。RADIUS サーバは、クライアントごとにゼロ個以上の SSID VSA を持つことができます。

この例では、次の AV の組み合わせは SSID *batman* を以下のユーザの許可された SSID のリストに追加します。

```
cisco-avpair= ”ssid=batman”
```

VSA を認識し、使用するためのアクセス ポイント / ブリッジの設定については、『Cisco IOS Software Configuration Guide for Cisco Aironet Access Points』の第 12 章を参照してください。

複数の基本 SSID の設定

アクセス ポイント 802.11g 無線は、8 個までの基本 SSID（BSSID）をサポートしています。これは Media Access Control（MAC; メディア アクセス制御）アドレスと類似します。複数の BSSID を使用して各 SSID の一意の DTIM 設定を割り当て、ビーコンの複数の SSID をブロードキャストします。DTIM 値が大きい場合、SSID を使用する節電クライアント デバイスのバッテリ寿命は伸び、複数の SSID をブロードキャストすると、無線 LAN がゲストにアクセスしやすくなります。

（注）　アクセス ポイント MAC アドレスに基づいて特定のアクセス ポイントにアソシエートするために設定された無線 LAN のデバイス（たとえば、クライアント デバイス、リピータ、ホット スタンバイ装置、またはワークグループ ブリッジ）は、複数の BSSID を追加または削除するときにアソシエーションを失うことがあります。複数の BSSID を追加または削除するときに、特定のアクセス ポイントにアソシエートするために設定されたデバイスのアソシエーション ステータスをチェックします。必要な場合、BSSID の新規 MAC アドレスを使用するためにアソシエーションが解除されたデバイスを再設定します。

複数の BSSID を設定するための要件

複数の BSSID を設定するには、アクセス ポイント / ブリッジは次の最小要件を満たす必要があります。

- VLAN を設定する必要があります。
- アクセス ポイント / ブリッジは Cisco IOS リリース 12.3(4)JA またはそれ以降を実行する必要があります。
- アクセス ポイント/ブリッジは複数の BSSID をサポートする 802.11g 無線を含む必要があります。

無線が複数の基本 SSID をサポートするかどうかを決定するには、**show controllers** *radio_interface* コマンドを入力します。結果に次の行が含まれる場合、無線は複数の基本 SSID をサポートします。

```
Number of supported simultaneous BSSID on radio_interface: 8
```

複数の BSSID を使用するためのガイドライン

複数の BSSID を設定するときに、次のガイドラインを考慮してください。

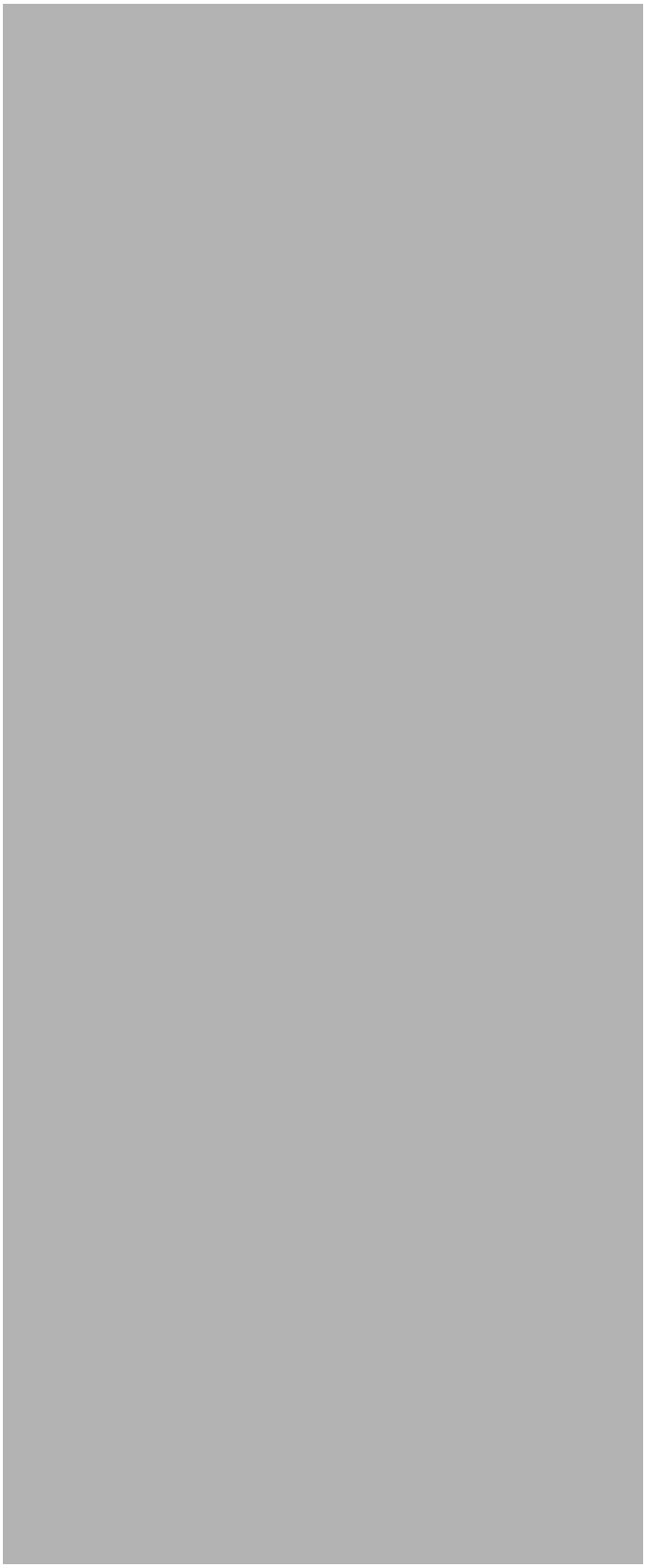
- 複数の BSSID を有効にすると、RADIUS によって割り当てられる VLAN はサポートされません。
- BSSID を有効にすると、アクセス ポイント / ブリッジは自動的に BSSID を各 SSID にマッピングします。BSSID を特定の SSID に手動でマッピングすることはできません。
- アクセス ポイント / ブリッジで複数の BSSID を有効にすると、SSIDL IE には SSID のリストは含まれず、拡張機能のみが含まれます。
- Wi-Fi によって認証されたクライアント デバイスは、複数の BSSID を使用してアクセス ポイント / ブリッジにアソシエートできます。
- WDS に参加するアクセス ポイント / ブリッジで複数の BSSID を有効にできます。

複数の BSSID の設定

複数の BSSID を設定する手順は、次のとおりです。

ステップ 1　アクセス ポイント GUI の Global SSID Manager ページにブラウズします（GUI の代わりに CLI を使用する場合、この項の終わりの CLI の設定例にリストされた CLI コマンドを参照してください）。図 7-1 は、Global SSID Manager ページの上部を示しています。

図 7-1　Global SSID Manager ページ



ステップ 2　**SSID** フィールドに SSID 名を入力します。

ステップ 3　**VLAN** ドロップダウン メニューを使用して、SSID が割り当てられる VLAN を選択します。

ステップ 4　SSID を有効にする無線インターフェイスを選択します。SSID は無線インターフェイスに有効にするまで非アクティブです。

ステップ 5　**Network ID** フィールドに SSID のネットワーク ID を入力します。

ステップ 6　認証、認証キー管理、およびアカウンティング設定をページの Authentication Settings、Authenticated Key Management、および Accounting セクションの SSID に割り当てます。BSSID は、SSID でサポートされるすべての認証タイプをサポートします。

ステップ 7　（オプション）Multiple BSSID Beacon Settings セクションで、**Set SSID as Guest Mode** チェックボックスをオンにして SSID をビーコンに含めます。

ステップ 8　（オプション）この　SSID　を使用する節電クライアントのバッテリ寿命を伸ばすには、**Set　Data Beacon Rate (DTIM)** チェックボックスをオンにして、SSID のビーコン比率を入力します。ビーコン比率は、アクセス ポイントがどれくらいの頻度で Delivery Traffic Indication Message（DTIM）を含むビーコンを送信するかを決定します。

クライアント デバイスが DTIM を含むビーコンを受信すると、通常、再起動し、保留中のパケットをチェックします。DTIM の間隔が長くなると、クライアントは長い時間スリープし、電力を節約します。逆に、DTIM 期間が短くなると、パケットの受信の遅延は低減されますが、クライアントはさらに頻繁に再起動されるので、バッテリ電力使用量が多くなります。

デフォルトのビーコン比率は 2 で、1 つおきのビーコンが DTIM を含みます。ビーコン比率を 1 ～ 100 の範囲で入力します。

（注）　DTIM 期間カウントを増加すると、マルチキャスト パケットの配信が遅延されます。マルチキャスト パケットはバッファされるので、DTIM 期間カウントが大きいと、バッファ オーバーフローの原因となることがあります。

ステップ 9　Guest Mode/Infrastructure SSID Settings セクションで、**Multiple BSSID** を選択します。

ステップ 10　**Apply** をクリックします。

CLI の設定例

この例は、無線インターフェイスで複数の BSSID を有効にし、*visitor* という SSID を作成し、BSSID として SSID を指定し、ビーコンに BSSID が含まれることを指定し、BSSID に DTIM 期間を設定し、SSID *visitor* を無線インターフェイスに割り当てるために使用する CLI コマンドを示しています。

```
ap(config)# interface d0
ap(config-if)# mbssid
ap(config-if)# exit
ap(config)# dot11 ssid visitor
ap(config-ssid)# mbssid guest-mode dtim-period 75
ap(config-ssid)# exit
ap(config)# interface d0
ap(config-if)# ssid visitor
```

dot11 mbssid グローバル コンフィギュレーション コマンドを使用して、複数の BSSID をサポートするすべての無線インターフェイスで複数の BSSID を同時に有効にすることもできます。

設定された BSSID の表示

show dot11 bssid 特権 EXEC コマンドを使用して、SSID および BSSID または MAC アドレス間の関係を表示します。この例は、次のコマンド出力を示しています。

```
ap#show dot11 bssid
Interface      BSSID         Guest  SSID
Dot11Radio1   0011.2161.b7c0  Yes  atlantic
Dot11Radio0   0005.9a3e.7c0f  Yes  WPA2-TLS-g
```

SSID に対する IP リダイレクションの割り当て

SSID に IP リダイレクションを設定すると、アクセス ポイント / ブリッジはその SSID にアソシエートされたクライアント デバイスから送信されたすべてのパケットを特定の IP アドレスにリダイレクトします。IP リダイレクションは、中央ソフトウェア アプリケーションを使用するハンドヘルド デバイスに対応する無線 LAN で主に使用され、特定の IP アドレスと通信するために静的に設定されます。たとえば、小売店や卸売店の無線 LAN 管理者はバー コード スキャナ用の IP リダイレクションを設定できます。バー コード スキャナはすべて同じスキャナ アプリケーションを使用して、同じ IP アドレスにデータを送信します。

SSID を使用してアソシエートされたクライアント デバイスからすべてのパケットをリダイレクトするか、特定の TCP または User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポート（アクセス コントロール リストに定義された）にリダイレクトされたパケットのみをリダイレクトすることができます。アクセス ポイント / ブリッジが特定のポートにアドレス指定されたパケットのみをリダイレトするように設定すると、アクセス ポイント / ブリッジは SSID を使用してこれらのパケットをクライアントからリダイレクトし、SSID を使用してその他のすべてのパケットをクライアントからドロップします。

（注）　IP リダイレクト SSID を使用してアソシエートされたクライアント デバイスにアクセス ポイント / ブリッジから PING テストを実行すると、クライアントからの応答パケットは特定の IP アドレスにリダイレクトされ、アクセス ポイント / ブリッジによって受信されません。

図 7-2 は、IP リダイレクト SSID を使用してアソシエートされたクライアントからアクセス ポイント / ブリッジがクライアントパケットを受信するときに実行される処理フローを示しています。

図 7-2　IP リダイレクションの処理フロー

IP リダイレクションを使用するためのガイドライン

IP リダイレクションを使用するときには、次のガイドラインを考慮してください。

- アクセス ポイント / ブリッジは、クライアント デバイスから受信したブロードキャスト、ユニキャスト、またはマルチキャスト BOOTP/DHCP パケットをリダイレクトしません。
- 受信パケット用の既存の Access Control List（ACL; アクセス コントロール リスト）フィルタは IP リダイレクションより優先されます。

IP リダイレクションの設定

特権 EXEC モードから SSID に IP リダイレクションを設定する手順は、次のとおりです。

	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設定モードを開始します。
ステップ 3	**ssid** *ssid-string*	特定の SSID に対するコンフィギュレーション モードに入ります。
ステップ 4	**ip redirection host** *ip-address*	IP アドレスに対する IP リダイレクト コンフィギュレーション モードに入ります。次の例のように、IP アドレスを 10 進表記で入力します。10.91.104.92。 リダイレクションのための TCP または UDP ポートを定義するアクセス コントロール リスト（ACL）を指定しない場合、アクセス ポイント / ブリッジはクライアント デバイスから受信するすべてのパケットをリダイレクトします。
ステップ 5	**ip redirection host** *ip-address* **access-group** *acl* **in**	（オプション）パケットのリダイレクションに適用するため ACL を指定します。ACL に定義された UDP または TCP ポートに送信されたパケットのみがリダイレクトされます。アクセス ポイント / ブリッジは、ACL に定義された設定に一致しないすべての受信パケットを破棄します。**in** パラメータは、ACL がアクセス ポイント / ブリッジの着信インターフェイスに適用されることを指定します。

この例は、ACL を適用しないで SSID の IP リダイレクションを設定する方法を示しています。アクセス ポイント / ブリッジは、SSID *batman* にアソシエートされたクライアント デバイスから受信するすべてのパケットをリダイレクトします。

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# ssid batman
sp(config-if-ssid)# ip redirection host 10.91.104.91
sp(config-if-ssid-redirect)# end
```

この例は、ACL に指定した TCP および UDP ポートに送信されたパケットのみの IP リダイレクションを設定する方法を示しています。アクセス ポイントが SSID *robin* を使用して、アソシエートされたクライアント デバイスからパケットを受信すると、指定されたポートに送信されたパケットをリダイレクトし、すべての他のパケットを破棄します。

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# ssid robin
ap(config-if-ssid)# ip redirection host 10.91.104.91 access-group redirect-acl in
ap(config-if-ssid)# end
```

SSIDL Information Element（IE; 情報要素）に SSID を含める

アクセス ポイント/ブリッジ ビーコンは 1 つのブロードキャスト SSID のみをアドバタイズします。ただし、アクセス ポイント / ブリッジ ビーコンの SSIDL 情報要素（SSIDL IE）を使用して、アクセス ポイント / ブリッジの追加 SSID のクライアント デバイスに警告することができます。SSIDL IE に含める SSID を指定する場合、クライアント デバイスは SSID が使用可能であることを検出し、その SSID を使用してアソシエートするのに必要なセキュリティ設定も検出します。

（注）　アクセス ポイント / ブリッジで複数の BSSID を有効にすると、SSIDL IE には SSID のリストは含まれず、拡張機能のみが含まれます。

特権 EXEC モードから SSIDL IE に SSID を含める手順は、次のとおりです。

	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設定モードを開始します。
ステップ 3	**ssid** *ssid-string*	特定の SSID に対するコンフィギュレーション モードに入ります。
ステップ 4	**information-element ssidl** [**advertisement**] [**wps**]	802.1x や Microsoft Wireless Provisioning Services（WPS）などの、アクセス ポイント / ブリッジの拡張機能をアドバタイズするアクセス ポイント / ブリッジ ビーコンに SSIDL IE を含めます。 **advertisement** オプションを使用して、SSIDL IE に SSID 名と機能を含めます。**wps** オプションを使用して SSIDL IE に WPS 機能フラグを設定します。

SSIDL IE を無効にする場合は、コマンドの **no** フォームを使用します。