複数の SSID の設定

この章では、アクセス ポイントで複数の Service Set Identifier（SSID）を設定および管理する方法について説明します。

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、ASCII 文字列です。ネットワークまたはサブネットワーク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。

アクセス ポイントには、最大 16 の SSID を設定でき、各 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にできます。つまり、クライアント 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。各 SSID には、次の設定を割り当てることができます。

- VLAN
- クライアント認証の設定

（注） クライアント認証タイプの詳細は、次を参照してください。第 11 章「認証タイプの設定」

- クライアントの認証済みキー管理の設定
- AP 認証パラメータの挿入（ブリッジなどの AP 間リンクを使用する場合）
- 管理フレーム保護設定の挿入（802.11w および/または Cisco MFP）
- 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（SSID 文字列をビーコンでブロードキャストするかどうかを定義）
- 古い AP 間認証メソッドの定義（AP 間リンクで PSK または LEAP セキュリティを使用する場合）
- クライアント デバイスから受信されたパケットのリダイレクション

ゲスト SSID を設定することで、アクセス ポイント SSID をすべての無線クライアント（該当する SSID に対するプロファイルを持っていないクライアントを含む）に対して表示できます。アクセス ポイントでは、ビーコンでゲスト SSID を示します。ゲスト モードが無効な場合も、AP はゲスト SSID のビーコンを送信しますが、SSID 文字列は示されません。SSID が事前設定されていないクライアントを除外する場合は、ゲスト SSID 機能を無効にします。クライアントはその特定の SSID 文字列を具体的に照会することによって、引き続き SSID を使用できることに注意してください。ブロードキャスト プローブ メッセージを送信するクライアントは、AP 応答で SSID 文字列を受け取りません。また、AP ビーコンの SSID 文字列も表示されません。ゲスト モード SSID の設定方法とゲスト モード SSID の無効化する方法については、「SSID のグローバルな作成」セクション（7-2 ページ）を参照してください。

アクセス ポイントをリピータまたは非ルート ブリッジとして機能させるには、リピータ側または非ルート ブリッジ側でクレデンシャルを設定し、ルートまたはプライマリ AP でリピータまたは非ルート ブリッジを認証できるようにします。リピータ モードの 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 デバイス同様、リピータでネットワークへの認証が可能になります。

ネットワークで複数の VLAN を使用する場合は、各 SSID を 1 つの VLAN に割り当てることができます。この割り当てた SSID を使用するクライアント デバイスは、その VLAN にグループ化されます。

複数の SSID の設定

次の項では、複数の SSID の設定情報を説明します。

- SSID のグローバルな作成（7-2 ページ）
- RADIUS サーバを使用した SSID の制限（7-5 ページ）

（注）　SSID をグローバルに設定してから、特定の無線インターフェイスに適用する必要があります。SSID をグローバルに設定するには、「SSID のグローバルな作成」セクション（7-2 ページ）の手順に従ってください。

SSID のグローバルな作成

Cisco IOS リリースでは、**dot11 ssid** 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 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、特定のインターフェイスにその SSID を割り当てることができます。

グローバル コンフィギュレーション モードで SSID を作成しておき、**ssid** 設定インターフェイス コマンドを実行すると、目的のインターフェイスにその SSID が割り当てられますが、SSID コンフィギュレーション モードにはなりません。SSID をグローバル コンフィギュレーション モードで作成していない場合は、**ssid** コマンドを実行すると、CLI が新しい SSID についての SSID コンフィギュレーション モードとなります。ただし、無線インターフェイスから SSID コンフィギュレーション モードで設定できるパラメータは、SSID グローバル コンフィギュレーション モードで設定できるパラメータより限られてます。

特権 EXEC モードから、次の手順に従って SSID をグローバルに作成します。SSID を作成した後、SSID を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 コンフィギュレーション モードを入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。 SSID には、最大 32 文字の英数字を使用でき、大文字と小文字が区別されます。 (注)　タブおよび末尾のスペースは、SSID には無効な文字です。
ステップ 3	**authentication client username** *username* **password** *password*	(任意) リピータ モードまたは非ルート ブリッジ モードで LEAP などのレガシー認証システムを使用する場合、アクセス ポイントがネットワークに対する認証で使用する認証ユーザ名とパスワードを設定します。リピータ アクセス ポイントがルート アクセス ポイントまたは別のリピータあるいは非ルート ブリッジにアソシエートするために使用するユーザ名およびパスワードを、SSID に設定します。
ステップ 4	**accounting** *list-name*	(任意) 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。方式のリストについて詳しくは、このリンク http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacct.html をクリックしてください。
ステップ 5	**vlan** *vlan-id*	(任意) ネットワーク上の VLAN に SSID を割り当てます。この 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。同じ VLAN に複数の SSID を割り当てることができますが、同じ SSID を複数の VLAN に割り当てることはできません。
ステップ 6	**guest-mode**	(任意) SSID をアクセス ポイントのゲスト モード SSID として指定します。ビーコンに SSID が含まれるアクセス ポイントは、プローブ要求で SSID を指定していないクライアント デバイスに可視になります。

	コマンド	目的
ステップ 7	**infrastructure-ssid** [**optional**]	このコマンドは、アクセス ポイントとブリッジが互いにアソシエートする際に使用する SSID を制御します。ルート アクセス ポイントでは、インフラストラクチャ SSID を使用してアソシエートができるのは、リピータ アクセス ポイントだけです。ルート ブリッジでは、インフラストラクチャ SSID を使用してアソシエートができるのは、非ルート ブリッジだけです。リピータ アクセス ポイントと非ルート ブリッジは、この SSID を使用してルート デバイスとアソシエートします。 アクセス ポイントとブリッジの GUI では、リピータの役割および非ルート ブリッジの役割にインフラストラクチャ SSID の設定が必要です。ワークグループ ブリッジの役割にインフラストラクチャ SSID を設定する必要はありません。レガシー IOS コードを使用している場合、無線に複数の SSID が設定されていない限り、CLI を使用してデバイスの役割を設定すれば、インフラストラクチャ SSID を設定する必要はありません。複数の SSID が無線に設定されている場合は、infrastructure-ssid コマンドを使用して、非ルート ブリッジがルート ブリッジとの接続に使用する SSID を指定する必要があります。 しかし、12.4(21a)JA1 および 12.3(8)JEC リリース以降では、1 つまたは複数の SSID の有無に関係なく、インフラストラクチャ SSID が設定されない場合、リピータはブリッジとアソシエートしません。
ステップ 8	**interface dot11radio** { **0** | **1** }	SSID の割り当て先とする無線インターフェイスに対して、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 802.11n 無線は 0 です。 5 GHz 無線および 5 GHz 802.11n 無線は 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**	(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)　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。認証タイプの設定方法については、第 9 章「ローカル認証サーバとしてのアクセス ポイントの設定」を参照してください。

(注)　802.11b と 802.11g が同じ 2.4 GHz 帯で動作するため、802.11g 無線にゲストの SSID モードを有効にすると、802.11b 無線にも適用されます。

SSID または SSID 機能を無効にするには、コマンドの **no** 形式を使用します。

次の例は、次の方法を示します。

- 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クライアント デバイスの最大数を 15 に設定
- 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
AP(config-if)#end
```

グローバルに設定された SSID の表示

グローバルに設定された SSID の設定詳細を表示するには、次のコマンドを使用します。

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

RADIUS サーバを使用した SSID の制限

クライアント デバイスが、不正な SSID を使用してアクセス ポイントにアソシエートするのを防ぐために、RADIUS 認証サーバでクライアントが使用する必要のある、許可された SSID のリストを作成します。

SSID 許可のプロセスは、次の手順で行われます。

1. クライアント デバイスはアクセス ポイントに設定された任意の SSID を使用して、アクセス ポイント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を許可された SSID のリストを返します。アクセス ポイントは、このリスト内に、クライアントが使用する SSID と一致する SSID があるかどうかをチェックします。次の 3 とおりの結果が予測されます。
   a. クライアントがアクセス ポイントとのアソシエーションに使用した SSID が、RADIUS サーバが返した許可リスト内のエントリに一致する場合、クライアントはすべての認証要件を満たした後にネットワークへのアクセスを許可されます。
   b. アクセス ポイントが、SSID の許可リストにクライアントと一致するエントリを検出できなかった場合は、このクライアントはアソシエーションを解除されます。
   c. RADIUS サーバがクライアントに SSID をまったく返さない場合（リストなし）は、管理者がリストを設定していないことを意味します。この場合、クライアントはアソシエーションと認証の試行を許可されます。

RADIUS サーバの返す SSID の許可リストは、シスコ Vendor-Specific Attribute（VSA; ベンダー固有の属性）の形式です。Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）のドラフト規格では、アクセス ポイントと RADIUS サーバ間で、ベンダー固有の属性（属性 26）を使用してベンダー固有の情報をやり取りする方法を指定しています。各ベンダーは、Vendor-Specific Attribute（VSA）を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。シスコが実装する RADIUS では、この仕様で推奨されるフォーマットを使用して、ベンダー固有のオプションを 1 つサポートしています。シスコのベンダー ID は 9 で、サポートするオプションはベンダー タイプ 1、名前は *cisco-avpair* です。RADIUS サーバには、クライアントあたり 0 以上の SSID VSA を指定できます。

次の例では、次の AV ペアにより、ユーザの SSID 許可リストに SSID *batman* が追加されます。

```
cisco-avpair= "ssid=batman"
```

VSA を認識して使用できるようにアクセス ポイントを設定する方法については、「ベンダー専用の RADIUS サーバ通信用アクセス ポイントの設定」セクション（13-17 ページ）を参照してください。

複数の基本 SSID の設定

アクセス ポイントの 802.11a、802.11b、802.11n 無線は、最大 16 の基本 SSID（BSSID）をサポートします。BSSID は、特定の SSID（ネットワーク名）文字列にアソシエートされる無線 MAC アドレスです。

複数の SSID を使用して、それぞれの SSID に一意の DTIM 設定を割り当て、SSID ごとに 1 つのビーコンをブロードキャストします。DTIM を大きな値に設定すると、SSID を使用する省電力モードのクライアント デバイスではバッテリの寿命が延びます。また、複数の SSID をブロードキャストすると、ゲストが無線 LAN にアクセスしやすくなります。

（注） アクセス ポイントの 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よう設定していた場合（クライアント デバイス、リピータ、ホット スタンバイ ユニット、ワークグループ ブリッジなど）、複数の BSSID の追加または削除を行うと、無線 LAN 上のデバイスがアソシエーションを損失することがあります。複数の BSSID を追加または削除する際には、特定のアクセス ポイントにアソシエートするよう設定されていたデバイスのアソシエーション状態を確認してください。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 MAC アドレスを使用するようにします。

複数 BSSID の設定要件

複数の BSSID を設定するには、アクセス ポイントが少なくとも次の要件を満たしている必要があります。

- VLAN が設定されていること。
- アクセス ポイントが Cisco IOS Release 12.3(4)JA 以降を実行していること。
- サポートされる基本 SSID の数を判別するには、**show controllers** *radio_interface* コマンドを入力します。結果に次の行が含まれていれば、その無線は複数の基本 SSID をサポートしています。

  ```
  Number of supported simultaneous BSSID on radio_interface: 16
  ```

複数の BSSID を使用する際のガイドライン

複数の BSSID を設定する際は、次のガイドラインに留意してください。

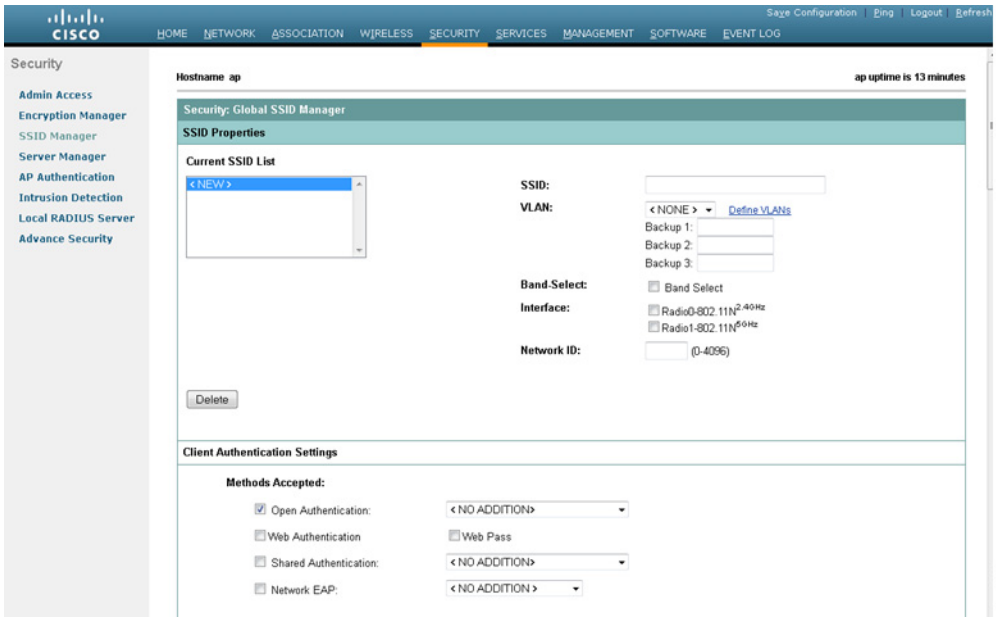
- 複数の BSSID を有効に設定すると、RADIUS サーバによる VLAN 割り当て機能がサポートされなくなります。
- BSSID を有効に設定すると、アクセス ポイントが各 SSID に BSSID を自動的にマッピングします。BSSID を特定の SSID に手動でマッピングすることはできません。
- アクセス ポイントで複数の BSSID を有効にすると、オプションの SSIDL IE には、SSID リストは追加されず、拡張機能だけが追加されます。
- Wi-Fi 認定済みクライアント デバイスであれば、どれでも複数 BSSID を使用したアクセス ポイントにアソシエートできます。
- Wireless Domain Service（WDS; 無線ドメイン サービス）を構成するアクセス ポイントでは、複数の BSSID を有効に設定できます。

複数の BSSID の設定

複数の BSSID（MBSSID）を設定するには、次の手順に従います。

ステップ 1　アクセス ポイントの GUI から、[Global SSID Manager] ページを表示します（GUI の代わりに CLI を使用する場合は、この項の最後の CLI の設定例に記載されている 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 リストから、SSID を割り当てる VLAN を選択します。

ステップ 4　SSID を有効に設定している無線インターフェイスを選択します。SSID 設定を検証して無線インターフェイスを有効にするまで、SSID はアクティブになりません。

ステップ 5　（任意）[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　このページの [Authentication Settings]、[Authenticated Key Management]、[Accounting Settings] セクションから、認証、認証済みキー管理、アカウンティング設定を SSID に設定します。MBSSID は、SSID でサポートされているすべての認証タイプをサポートします。

ステップ 7　（任意）SSID をビーコンに追加するには、[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ます。

ステップ 8　（任意）この SSID を使用する省電力モードのクライアントのバッテリの寿命を延ばすには、[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 レートを入力します。ビーコン レートによって、Delivery Traffic Indicator Message（DTIM）を追加したビーコンをアクセス ポイントが送信する頻度が決まります。

DTIM を追加したビーコンをクライアント デバイスが受信すると、通常は、保留中のパケットをチェックするためにクライアント デバイスが再起動します。DTIM の間隔が長くなると、クライアントのスリープ時間が長くなり、電力を節約できます。反対に、DTIM の間隔が短くなるとパケットの受信の遅延を抑えられますが、クライアントが頻繁に起動するためバッテリ残量が消費されます。

デフォルトのビーコン レートは 2 に設定されています。つまり、ビーコン 1 つおきに DTIM が追加されます。ビーコン レートは 1 ～ 100 の値で入力します。

（注）　DTIM 期間のカウントを増やすと、マルチキャスト パケットの送信は遅れます。マルチキャスト パケットはバッファリングされるため、DTIM 期間のカウントを大きくするとバッファがオーバーフローする可能性があります。

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

次の例は、無線インターフェイスで複数の BSSID を有効に設定する CLI コマンド、*visitor* を呼び出した SSID を作成する CLI コマンド、SSID を BSSID に指定する CLI コマンド、BSSID がビーコンに追加されていることを指定する CLI コマンド、BSSID に DTIM 間隔を設定する CLI コマンド、無線インターフェイスに SSID *visitor* を設定する CLI コマンドを示しています。

```
ap(config)# interface do0
ap(config-if)# mbssid
ap(config-if)# exit
ap(config)# dot11 ssid visitor vlan20
ap(config-ssid)# mbssid guest-mode dtim-period 3
ap(config-ssid)# exit
ap(config)# interface do0
ap(config-if)# ssid visitor
```

また、**dot11 mbssid** グローバル コンフィギュレーション コマンドを使用すると、複数の BSSID をサポートしてい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。

設定済み BSSID の表示

SSID と BSSID の関係、または MAC アドレスを表示するには、**show dot11 bssid** 特権 EXEC コマンドを使用します。次の例はコマンドの出力を示しています。

```
AP1230#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

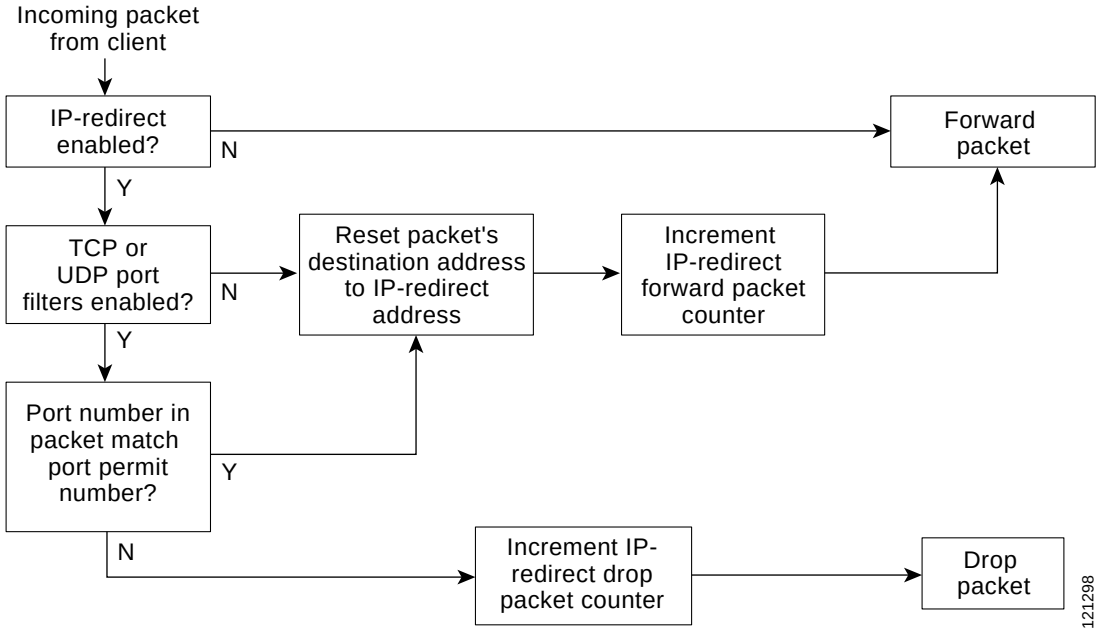
SSID に IP リダイレクションを設定すると、その SSID にアソシエートされたクライアント デバイスからアクセス ポイントに送信されたパケットはすべて、指定した IP アドレスにリダイレクトされます。IP リダイレクションが主に使用されるのは、特定の IP アドレスと通信するように静的に設定され、中央にあるソフトウェア アプリケーションを使用するハンドヘルド デバイスをクライアントとする無線 LAN です。たとえば、小売店や商品倉庫の無線 LAN 管理者は、バーコード スキャナに IP リダイレクションを設定できます。これらすべてのバー コード スキャナでは、同じスキャナ アプリケーションが使用され、すべてのデータは同じ IP アドレスに送信されます。

SSID を使用してアソシエートされているクライアント デバイスからのパケットをすべてリダイレクトできる他、アクセス コントロール リストで定義された特定の TCP ポートや UDP ポート宛てのパケットだけをリダイレクトすることもできます。特定のポート宛てのパケットだけがリダイレクトされるようにアクセス ポイントを設定すると、その SSID を使用しているクライアントからの該当のパケットがアクセス ポイントからリダイレクトされます。また、同じ SSID を使用しているクライアントからのその他のパケットは、アクセス ポイントでドロップされます。

（注） IP リダイレクトが設定された SSID を使用してアソシエートされているクライアント デバイスに対して、アクセス ポイントから ping テストを実行すると、そのクライアントからの応答パケットは、指定した IP アドレスにリダイレクトされ、アクセス ポイントでは受信されません。

図 7-2 は、IP リダイレクトが設定された SSID を使用してアソシエートされているクライアントからのパケットを、アクセス ポイントで受信した場合の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際のガイドライン

IP リダイレクションを使用する際は、次のガイドラインに留意してください。

- クライアント デバイスからブロードキャスト、ユニキャスト、またはマルチキャストで送信された BOOTP/DHCP パケットは、アクセス ポイントからリダイレクトされません。
- 受信パケットに対する ACL フィルタが存在する場合は、IP リダイレクションより優先して適用されます。

IP リダイレクションの設定

特権 EXEC モードから、次の手順に従って SSID に IP リダイレクションを設定します。

	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	**dot11 ssid** *ssid-string*	特定の SSID に対するコンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	**ip redirection host** *ip-address*	目的の IP アドレスに対して、IP リダイレクション コンフィギュレーション モードを開始します。ドットを使用して IP アドレスを入力します（例:10.91.104.92）。 リダイレクションの対象となる TCP ポートや UDP ポートを定義したアクセス コントロール リスト（ACL）を指定しない場合は、クライアント デバイスから受信されたパケットはすべてアクセス ポイントからリダイレクトされます。
ステップ 4	**ip redirection host** *ip-address* **access-group** *acl* **in**	（任意）パケットのリダイレクションに適用する ACL を指定します。ACL で定義した特定の UDP ポートまたは TCP ポート宛てに送信されたパケットだけがリダイレクトされます。ACL で定義した設定に一致しない受信パケットはすべて廃棄されます。**in** パラメータを指定すると、アクセス ポイントの受信インターフェイスに ACL が適用されます。

（注）　ACL ロギングは、アクセス ポイントのプラットフォームのブリッジング インターフェイスではサポートされていません。ブリッジング インターフェイスに適用すると、インターフェイスがログ オプションなしで設定されたように動作し、ロギングは実施されません。BVI インターフェイスに別の ACL を使用している限り、ACL ロギングは、BVI インターフェイスで動作します。

次の例は、ACL を適用せずに SSID に IP リダイレクションを設定する方法を示しています。*batman* という SSID にアソシエートされているクライアント デバイスから受信されたパケットはすべて、アクセス ポイントからリダイレクトされます。

```
AP# configure terminal
AP(config)# dot11 ssid batman
AP(config-if-ssid)# ip redirection host 10.91.104.91
AP(config-if-ssid-redirect)# end
```

SSID ビーコンに SSIDL IE を含める

アクセス ポイントは SSID ごとに 1 つのビーコンをブロードキャストします。デフォルトでは、SSID ビーコンのいずれか 1 つだけが、関連する SSID 名を示します。MBSSID 機能が使用されない限り、同じ無線のその他のビーコンでは SSID フィールドが空のままになります。

（注）　アクセス ポイントで複数の BSSID を有効に設定すると、SSIDL IE には、SSID リストは追加されず、拡張機能だけが追加されます。

特権 EXEC モードから、次の手順に従って SSIDL IE を SSID ビーコンに含めます。

	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*	特定の SSID に対するコンフィギュレーション モードを開始します。ゲスト モードに設定された SSID を選択することが推奨されます(つまり、SSID 文字列をビーコンにアドバタイズします)。
ステップ 3	**information-element ssidl** [**advertisement**] [**wps**]	アクセス ポイントの拡張機能をアドバタイズするアクセス ポイント ビーコンに、SSIDL IE を追加します。この拡張機能には、802.1x、Microsoft Wireless Provisioning Services (WPS)のサポートなどがあります。 SSIDL IE に SSID の名前と機能を追加するには、**advertisement** オプションを使用します。SSIDL IE に WPS 機能フラグを設定するには、**wps** オプションを使用します。

SSIDL IE を無効にするには、コマンドの **no** 形式を使用します。デフォルトでは、SSIDL IE は無効になっています。

MBSSID の NAC サポート

ネットワークは、ウイルス、ワーム、スパイウェアなどのセキュリティ脅威から保護する必要があります。これらのセキュリティ脅威によって業務に支障をきたし、ダウンタイムが生じたり、パッチの適用に追われたりすることになります。ネットワークにアクセスしようとするすべての有線/無線デバイスが、企業のセキュリティ ポリシーに適合するように、エンドポイントを視覚化して管理することが必要です。感染したエンドポイントや脆弱なエンドポイントを自動的に検出して切り離し、クリーンな状態にする必要があります。

NAC は、ネットワーク リソースにアクセスするすべての有線/無線のエンドポイント デバイス(PC、ノート パソコン、サーバ、PDA など)が適切にセキュリティ脅威から保護されるよう厳密に設計されています。NAC を使用することにより、企業は、ネットワークに参加するすべてのデバイスを分析して管理できるようになります。すべてのエンドポイント デバイスが企業のセキュリティ ポリシーに準拠し最新のセキュリティ保護策を確実に実行することにより、企業はウイルス感染やネットワークのセキュリティ侵害の経路となりやすいエンドポイント デバイスを大幅に削減または排除できます。

WLAN は、ウイルス、ワーム、スパイウェアなどのセキュリティ脅威から保護する必要があります。NAC アプライアンスも NAC フレームワークも、WLAN クライアントがネットワークにアクセスしようとするときにデバイス セキュリティ ポリシーを施行することで、WLAN をセキュリティ脅威から保護します。これらのソリューションは、ポリシーに準拠しない WLAN クライアントを検疫し、ポリシーに準拠するように修復するサービスを提供しています。

クライアントは、ソフトウェアのバージョンやウイルスのバージョンなどの状態に応じて、別々の VLAN に配置されます。必要なソフトウェアをダウンロードするよう VLAN を設定して、クライアントをネットワークのアクセスに必要なソフトウェアのバージョンにアップグレードします。NAC サポートには 4 つの VLAN が設定されます。そのうちの 1 つは通常の VLAN で、ここには、正しいソフトウェア バージョンを搭載したクライアントが配置されます。その他の VLAN は指定された検疫処理用に確保されています。クライアントがアップグレードされるまで、感染したすべてのクライアントはいずれか 1 つの VLAN に配置されます。

各 SSID では、最大 3 つの VLAN を「有害な」VLAN として設定できます。感染したクライアントは、感染状態に応じて、いずれか 1 つの VLAN に配置されます。クライアントがアソシエーション要求を送信すると、クライアントの感染ステータスをその要求に含めて RADIUS サーバへ送信します。クライアントを特定の VLAN に配置するポリシーのプロビジョニングが RADIUS サーバ上で行われます。

感染したクライアントがアクセス ポイントにアソシエートして RADIUS サーバにそのステートを送信すると、RADIUS サーバは状態に応じてそのクライアントを検疫 VLAN の 1 つに配置します。この VLAN は、dot1x クライアント認証プロセスの途中で、RADIUS サーバの Access Accept 応答内で送信されます。クライアントが健全な状態で、NAC に準拠している場合、RADIUS サーバは通常の VLAN 割り当てを SSID に返し、クライアントは正しい VLAN と BSSID に配置されます。

各 SSID には、通常の VLAN が割り当てられます。通常の VLAN とは、健全なクライアントが配置される VLAN のことです。また、SSID では、ステートに応じてクライアントが配置される検疫 VLAN 対応するバックアップ VLAN を最大 3 つまで設定できます。SSID 用のこれらの VLAN には、SSID の MBSSID によって割り当てた BSSID と同じものを使用します。

設定済み VLAN はそれぞれ異なり、同じ SSID 内で VLAN が重複することはできません。このため、VLAN を設定できるのは 1 つのインターフェイスにつき一度だけで、2 つの異なる SSID で VLAN は使用できません。

検疫 VLAN は、通常の VLAN を設定したインターフェイスで自動的に設定されます。検疫 VLAN は、通常 VLAN と同じ暗号プロパティを継承します。VLAN には、同じキー/認証タイプがあり、検疫 VLAN のキーは自動的に派生します。

Dot11 サブインターフェイスが生成され、dot1q カプセル化 VLAN（設定済み VLAN 数と同数）とともに自動的に設定されます。また、有線側のサブインターフェイスも、ブリッジ グループ設定と併せてギガビット イーサネット 0 サブインターフェイスに自動的に設定されます。

クライアントがアソシエートして RADIUS サーバが有害な状態と判断すると、dot1x 認証の RADIUS 認証応答内でサーバが検疫 NAC の VLAN のいずれかを返します。この VLAN は、クライアントの SSID で設定したバックアップ用 VLAN のうちの 1 つでなければなりません。この VLAN が、すでに設定したバックアップ用 VLAN のうちの 1 つでなければ、クライアントはアソシエートされません。

すべてのバックアップ用 VLAN に対応するデータは、SSID に割り当てられた BSSID を使用して送受信されます。このため、その SSID に対応する BSSID をリッスンしているすべてのクライアント（健全なクライアントおよび有害なクライアント）が再起動します。VLAN が健全か有害かに応じて、使用中のマルチキャスト キーに基づき、クライアントでパケットの復号化が行われます。有線側のトラフィックは、別の VLAN を使用しているため隔離されます。このようにして、感染したクライアントのトラフィックと感染していないクライアントのトラフィックが混在しないようにしています。

次に示すように、**dot11 ssid** <*ssid*> では、これまでの **vlan** <*name*> | <*id*> に、新キーワード **backup** が追加されます。

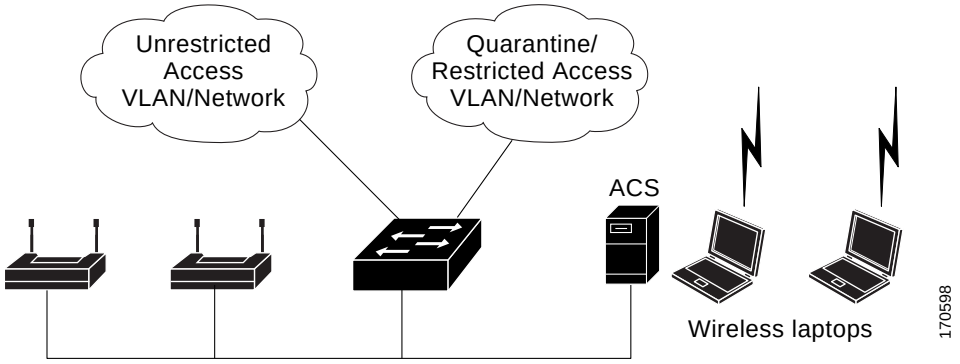
```
vlan <name>|<id> [backup <name>|<id>, <name>|<id>, <name>|<id>
```

MBSSID への NAC 設定

（注） この機能がサポートするのは、VLAN 内のレイヤ 2 モビリティだけです。この機能は、ネットワーク ID を使用するレイヤ 3 モビリティをサポートしません。

(注)　アクセス ポイントで MBSSID の NAC を有効にする前に、NAC が正しく機能するようにしてください。図 7-3 は、一般的なネットワーク設定を示しています。

図 7-3　一般的な NAC ネットワーク設定



詳細については、シスコ無線ネットワークに NAC を展開する方法のマニュアルを参照してください。

アクセス ポイントの MBSSID に NAC を設定する手順は、次のとおりです。

ステップ 1　図 7-3 に示すように、ネットワークを設定します。

ステップ 2　スタンドアロンのアクセス ポイントと、NAC 対応クライアントの EAP 認証を設定します。

ステップ 3　ポスチャを確認するため、ACS サーバにローカル プロファイルを設定します。

ステップ 4　クライアントが EAP-FAST を使用して正常に認証できるよう、クライアントとアクセス ポイントを設定します。

ステップ 5　クライアントのポスチャが有効であることを確認します。

ステップ 6　認証とポスチャ確認が完了したら、クライアントがアクセス ポイントとアソシエートしていること、クライアントが制限のない VLAN に配置されていることを確認します。

設定例を次に示します。

```
dot11 mbssid
dot11 vlan-name engg-normal vlan 100
dot11 vlan-name engg-infected vlan 102
dot11 vlan-name mktg-normal vlan 101
dot11 vlan-name mktg-infected1 vlan 103
dot11 vlan-name mktg-infected2 vlan 104
dot11 vlan-name mktg-infected3 vlan 105
!
dot11 ssid engg
    vlan engg-normal backup engg-infected
    authentication open
    authentication network-eap eap_methods
!
dot11 ssid mktg
    vlan mktg-normal backup mktg-infected1, mktg-infected2, mktg-infected3
    authentication open
    authentication network-eap eap_methods
```

```
!
interface Dot11Radio0
!
encryption vlan engg-normal key 1 size 40bit 7 482CC74122FD transmit-key
encryption vlan engg-normal mode ciphers wep40
!
encryption vlan mktg-normal key 1 size 40bit 7 9C3A6F2CBFBC transmit-key
encryption vlan mktg-normal mode ciphers wep40
!
ssid engg
!
ssid mktg
!
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
!
interface Dot11Radio0.100
encapsulation dot1Q 100 native
no ip route-cache
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio0.102
encapsulation dot1Q 102
no ip route-cache
bridge-group 102
bridge-group 102 subscriber-loop-control
bridge-group 102 block-unknown-source
no bridge-group 102 source-learning
no bridge-group 102 unicast-flooding
bridge-group 102 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
!
interface FastEthernet0.100
encapsulation dot1Q 100 native
no ip route-cache
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface FastEthernet0.102
encapsulation dot1Q 102
no ip route-cache
bridge-group 102
no bridge-group 102 source-learning
bridge-group 102 spanning-disabled
!
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。