



## 複数の SSID の設定

---

この章では、アクセス ポイントで複数のサービス セット ID (SSID) を設定および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 \(P. 7-9\)](#)
- [SSID に対する IP リダイレクションの割り当て \(P. 7-13\)](#)
- [SSID IE への SSID の追加 \(P. 7-16\)](#)
- [MBSSID の NAC サポート \(P. 7-17\)](#)

## 複数のSSIDの概要

SSIDは、無線ネットワーク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。SSIDには、スペースを含めないようにしてください。

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なります。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
- クライアント認証方式



(注) クライアント認証タイプの詳細は、第11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Remote Authentication Dial-In User Service (RADIUS) アカウンティング
- ゲストモード
- リピータモード(認証ユーザ名とパスワードを含む)
- 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

アクセスポイントに対し、設定内にSSIDが指定されていないクライアントデバイスからのアソシエーションを許可する場合、ゲストSSIDを設定できます。アクセスポイントでは、ビーコンにゲストSSIDが追加されます。ゲストモードが無効になっていると、SSIDがビーコンメッセージで同報通信されません。設定済みSSIDのないクライアントが無線ネットワークに接続しないようにするには、このゲストSSID機能を無効に設定してください。ゲストモードSSIDの設定方法とゲストモードSSIDの無効方法については、「SSIDのグローバルな作成」の項(P. 7-4)を参照してください。

アクセスポイントをリピータとして使用する場合、またはリピータの親として機能するルートアクセスポイントとする場合は、SSIDをリピータモードで使用するよう設定できます。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VLANに1つのSSIDを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せん。

## ソフトウェアバージョンのSSIDに対する影響

Cisco IOS リリース 12.3(2)JA には、複数インターフェイス環境でSSIDパラメータを簡単に設定できるよう、グローバルモードのSSID設定が導入されました。Cisco IOS リリース 12.3(2)JA リリースでは、下位互換性があるようインターフェイスレベルでSSIDパラメータを設定できましたが、Cisco IOS リリース 12.3(4)JA 以降のリリースではインターフェイスレベルでSSIDパラメータを設定できなくなります。表 7-1 は、Cisco IOS リリースでサポートされているSSID設定方法を示しています。

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

Cisco IOS リリース	サポートされている SSID 設定方法
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 および 12.3(7)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 モードではすべての SSID を保存。
12.3(4)JA 以降	グローバルのみ。

Cisco IOS リリース 12.3(10b)JA は、Command-Line Interface ( CLI; コマンドライン インターフェイス )を使用してインターフェイス レベルで SSID パラメータを設定できますが、SSID はグローバル モードで保存されます。SSID をすべてグローバル モードで保存すると、Cisco IOS リリース 12.4(10b)JA 以降のリリースにアップグレードしても SSID 設定が維持されます。

Cisco IOS リリース 12.3(2)JA 以前を 12.3(4)JA 以降のリリースにアップグレードする必要がある場合は、まず Cisco IOS リリース 12.3(4)JA にアップグレードして設定ファイルを保存してから、目的のリリースにアップグレードし、保存しておいた設定ファイルをロードします。この手順を行うと、インターフェイス レベルの SSID 設定がグローバル モードに正しく変換されます。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と、インターフェイス レベルの SSID 設定は削除されます。

Cisco IOS リリース 12.4(10b)JA からソフトウェア バージョンをダウングレードすると、以前に作成した SSID はすべて無効になります。ダウングレード後に SSID を再設定しなくて済むよう、Cisco IOS リリース 12.3(7)JA にアップグレードする前に旧ソフトウェア バージョンの設定ファイルのコピーを保存しておいてください。Cisco IOS リリース 12.3(7)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、ダウングレード後に、保存しておいたこの設定ファイルをロードしてください。

表 7-2 は、Cisco IOS リリース 12.2(15)JA を実行しているアクセス ポイントでの SSID 設定と、Cisco IOS リリース 12.3(7)JA にアップグレードした後の設定の例を示しています。

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 での SSID 設定	12.3(7)JA にアップグレードした後の SSID 設定
<pre>interface dot11Radio 0   ssid engineering   authentication open   vlan 4  interface dot11Radio 1   ssid engineering   authentication open   vlan 5</pre>	<pre>dot11 ssid engineering   authentication open   vlan 5 ! interface dot11Radio 0   ssid engineering  interface dot11Radio 1   ssid engineering</pre>

インターフェイスごとの VLAN 設定が、グローバルの SSID 設定に残っていることに注意してください。



(注)

SSID、VLAN、および暗号化方式は、1 対 1 対 1 の関係で相互にマッピングされます。つまり、1 つの SSID を 1 つの VLAN にマッピングでき、1 つの VLAN を 1 つの暗号化方式にマッピングできます。グローバル SSID 設定を使用する場合、1 つの SSID を 2 つの異なる暗号化方式に設定することはできません。たとえば、インターフェイス dot11 0 では SSID *north* を Temporal Key Integrity Protocol ( TKIP ) に適用して、インターフェイス dot11 1 では SSID *north* を Wired Equivalent Privacy ( WEP ) 128 に適用することはできません。

## 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。

- [デフォルトの SSID 設定 \(P. 7-4\)](#)
- [SSID のグローバルな作成 \(P. 7-4\)](#)
- [RADIUS サーバを使用した SSID の制限 \(P. 7-8\)](#)



**(注)** Cisco IOS リリース 12.3(4)JA 以降では、SSID をグローバルに設定できるほか、特定の無線インターフェイスに適用することもできます。SSID をグローバルに設定するには、「[SSID のグローバルな作成](#)」の項 (P. 7-4) の手順に従ってください。

## デフォルトの SSID 設定

Cisco IOS リリース 12.3(7)JA には、デフォルトの SSID は存在しません。

## SSID のグローバルな作成



Cisco IOS リリース 12.3(2)JA 以降では、SSID をグローバルに設定できるほか、特定の無線インターフェイスについて設定することもできます。`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、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 設定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 設定モードとなります。



**(注)** ソフトウェア バージョンを旧バージョンのリリースにダウングレードすると、Cisco IOS Releases 12.3(7)JA 以降で作成した SSID は無効になります。

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、それ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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>dot11 ssid <i>ssid-string</i></code>	<p>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。</p> <p>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。</p> <p> (注) 先頭の文字に !、#、; の文字は使用できません。</p> <p> (注) +、\、/、"、TAB、末尾のスペースは、SSID には無効な文字です。</p>
ステップ 3	<code>authentication client</code> <code>username <i>username</i></code> <code>password <i>password</i></code>	(オプション) アクセス ポイントがリピータ モードのときに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。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	<code>accounting <i>list-name</i></code>	(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。 <i>list-name</i> 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。 <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcftb.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcftb.htm</a>
ステップ 5	<code>vlan <i>vlan-id</i></code>	(オプション) 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。1 つの VLAN には、1 つの SSID だけを割り当てることができます。
ステップ 6	<code>guest-mode</code>	(オプション) 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。アクセス ポイントはビーコンに SSID を追加し、SSID を指定していないクライアント デバイスからのアソシエーションを許可します。

	コマンド	目的
ステップ 7	<code>infrastructure-ssid [optional]</code>	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 アクセス ポイント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、ワークグループ ブリッジの役割、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。ただし、デバイスの役割の設定に CLI を使用すれば、複数の SSID が無線に設定されていない限り、インフラストラクチャ SSID の設定は不要になります。複数の SSID が無線に設定されている場合は、 <code>infrastructure-ssid</code> 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。
ステップ 8	<code>interface dot11radio { 0   1 }</code>	SSID の割り当て先とする無線インターフェイスに対して、インターフェイス設定モードを開始します。  2.4GHz 無線と 2.4GHz 802.11n 無線は 0 です。  5GHz 無線と 5GHz 802.11n 無線は 1 です。
ステップ 9	<code>ssid ssid-string</code>	<a href="#">ステップ 2</a> 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	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 11	<code>copy running-config startup-config</code>	(オプション) コンフィギュレーション ファイルに入力内容を保存します。



(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。認証タイプの設定手順については、[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 2.4GHz 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 無線に適用されます。

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
```

## SSID でのスペースの使用

Cisco IOS リリース 12.3(7)JA 以降では、SSID にスペースを含めることができますが、末尾のスペース (SSID の末尾のスペース) は無効になります。ただし、以前のバージョンで作成した SSID に末尾のスペースがある場合は、認識されます。末尾のスペースがあると、同じアクセス ポイント上で、同一の SSID が複数設定されているように表示されます。アクセス ポイント上で同一の複数の SSID があると考えられる場合は、特権 EXEC コマンド `show dot11 associations` を使用して、以前のリリースで作成した SSID に末尾にスペースがないか確認してください。

たとえば、次の特権 EXEC コマンド `show configuration` からの出力例では、SSID 中のスペースが表示されません。

```
ssid buffalo
  vlan 77
  authentication open

ssid buffalo
  vlan 17
  authentication open

ssid buffalo
  vlan 7
  authentication open
```

ところが、次の特権 EXEC コマンド `show dot11 associations` からの出力例では、SSID 中のスペースが表示されます。

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



(注)

このコマンドで表示するのは、SSID の最初の 15 文字だけです。15 文字以上の SSID を表示するには、`show dot11 associations client` コマンドを使用してください。

## 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 通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 Attributes (VSA; ベンダー固有の属性) の形式です。Internet Engineering Task Force (IETF) 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。ベンダーは Vendor-Specific Attributes (VSA; ベンダー固有の属性) を使用して、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のベンダー タイプは 1 で、*cisco-avpair* と名前が付けられています。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 (属性値) 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](#)」の項 (P. 13-17) 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 802.11a、802.11g、および 802.11n 無線が、Media Access Control (MAC; メディア アクセス制御) アドレスと同様、最大 8 つまでの Basic Service Set Identifier (BSSID; 基本サービス セット ID) をサポートできるようになりました。複数の BSSID を使用して SSID ごとに固有の Delivery Traffic Indication Message (DTIM) 設定を割り当て、複数の SSID をビーコンに同報通信できます。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ーの寿命が延びます。また、複数の SSID を同報通信すると、ゲストがワイヤレス 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に設定していた場合 (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、ワイヤレス 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に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、アソシエートが解除されたデバイスを再設定して、BSSID の新しい MAC アドレスを使用するようにしてください。

## 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。
- アクセス ポイントに、複数の BSSID をサポートする 802.11a または 802.11g 無線が組み込まれていること。無線が複数の基本 SSID をサポートしているかどうかを調べるには、`show controllers radio_interface` コマンドを入力してください。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: 8
```

## 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。

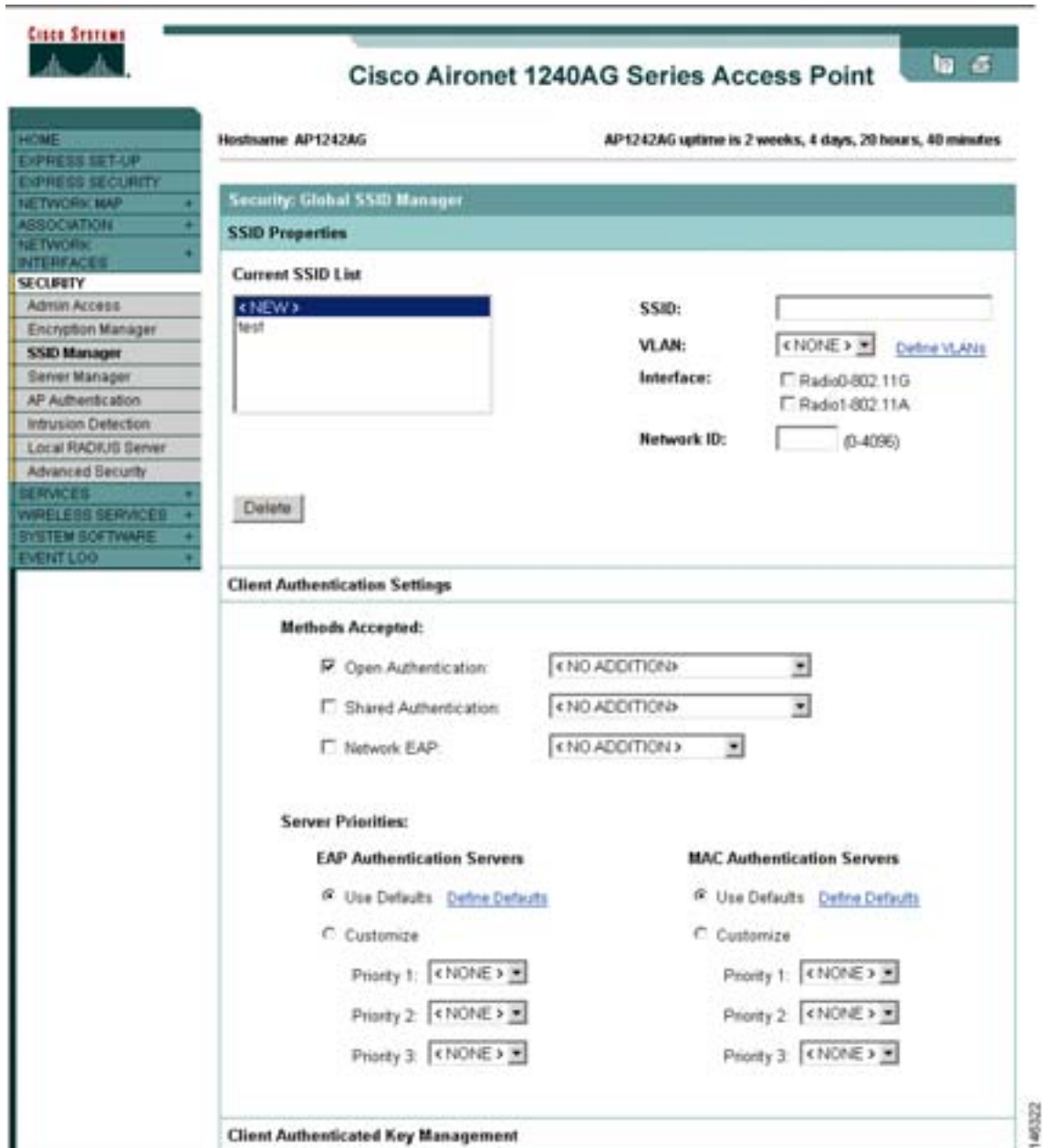
- 複数の BSSID を有効に設定すると、RADIUS サーバによる VLAN 割り当て機能がサポートされなくなります。
- BSSID を有効に設定すると、アクセス ポイントが各 SSID に BSSID を自動的にマッピングします。BSSID を特定の SSID に手動でマッピングすることはできません。
- アクセス ポイントで複数の BSSID を有効に設定すると、SSIDL Information Element (SSIDL IE; SSIDL 情報エレメント) に SSID リストが追加されず、拡張機能だけが追加されます。
- Wi-Fi 認定済みクライアント デバイスであれば、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 Services (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 を設定する手順は、次のとおりです。

- ステップ1** アクセスポイントの GUI から、Global SSID Manager ページを表示します（GUI ではなく CLI を使用する場合は、この項の最後の「CLI の設定例」に記載している 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 ドロップダウンメニューから、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。無線インターフェイスに SSID を有効に設定しない限り、SSID はアクティブになりません。
- 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** 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、アカウント設定を SSID に設定します。BSSID 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** (オプション) 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** (オプション) 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ー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ー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ので、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 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
```

また、`dot11 mbssid` グローバル設定コマンドを使用すると、複数の BSSID をサポートしている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ほか、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 User Datagram Protocol (UDP; ユーザ データグラム プロトコル) ポート宛てのパケットのみ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のみ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 ポイントで廃棄されます。

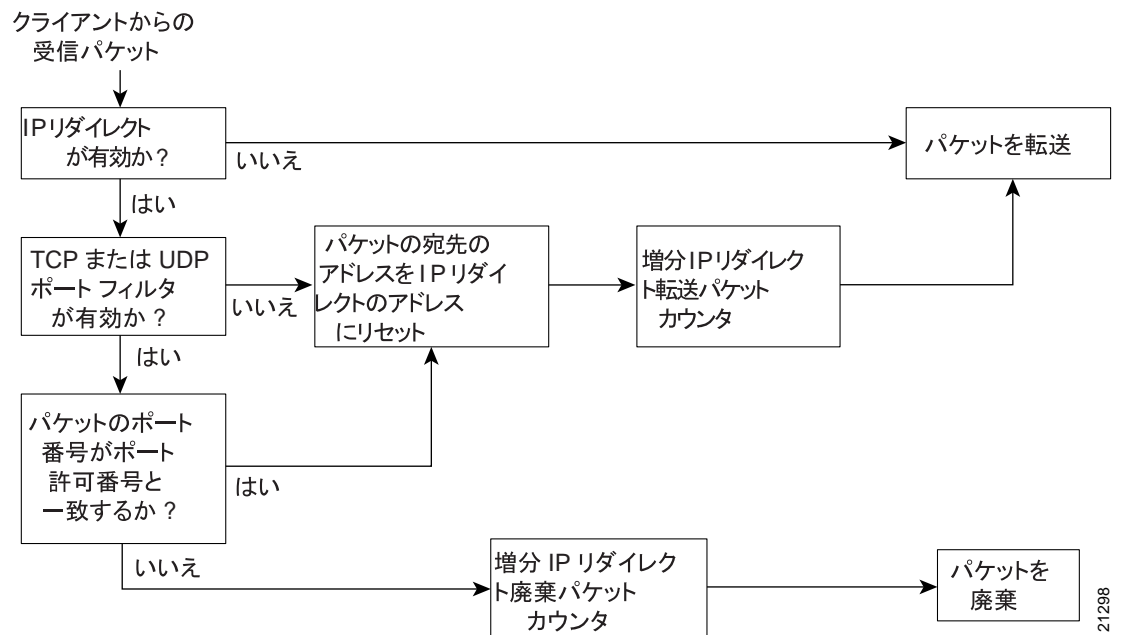


(注)

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 Access Control List (ACL; アクセス コントロール リスト) 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio { 0   1 }</code>	無線インターフェイスのインターフェイス設定モードを開始します。  2.4GHz 無線と 2.4GHz 802.11n 無線は 0 です。  5GHz 無線と 5GHz 802.11n 無線は 1 です。
ステップ 3	<code>ssid ssid-string</code>	特定の SSID に対する設定モードを開始します。
ステップ 4	<code>ip redirection host ip-address</code>	目的の IP アドレスに対して、IP リダイレクション設定モードを開始します。10.91.104.92 のように、ドットを使用して IP アドレスを入力します。  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 5	<code>ip redirection host ip-address access-group acl in</code>	(オプション) 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のみ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は動作しません。

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)# interface dot11radio 0
AP(config-if)# ssid batman
AP(config-if-ssid)# ip redirection host 10.91.104.91
AP(config-if-ssid-redirect)# end
```

次の例は、BVI1 インターフェイスに適用済みのACLで指定された特定のTCPポートまたはUDPポート宛てに送信されたパケットのみを対象とするIPリダイレクションを設定する方法を示しています。*robin* という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受信されたパケットは、指定のIPアドレス宛にアクセスポイントからリダイレクトされます。それ以外のパケットはすべて破棄されます。

```
AP# configure terminal
AP(config)# interface bvi1
AP(config-if-ssid)# ip redirection host 10.91.104.91 access-group redirect-acl in
AP(config-if-ssid)# end
```

## SSIDL IE への SSID の追加

アクセス ポイントのビーコンでアドバタイズできる SSID は、1 つのブロードキャスト SSID のみです。ただし、アクセス ポイントのビーコンに SSIDL IE を使用すれば、そのアクセス ポイントには他にも SSID があることをクライアント デバイスに通知できます。ある SSID を指定して SSIDL IE に追加しておく、クライアント デバイスではその SSID の存在が検出され、さらにその SSID を使用したアソシエートに必要なセキュリティ設定も検出されます。



(注) アクセス ポイントで複数の BSSID を有効に設定すると、SSIDL 情報エレメント ( 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 SSID を SSIDL IE に追加します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio { 0   1 }</code>	無線インターフェイスのインターフェイス設定モードを開始します。  2.4GHz 無線と 2.4GHz 802.11n 無線は 0 です。  5GHz 無線と 5GHz 802.11n 無線は 1 です。
ステップ 3	<code>ssid ssid-string</code>	特定の SSID に対する設定モードを開始します。
ステップ 4	<code>information-element ssidl [advertisement] [wps]</code>	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、 <b>advertisement</b> 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、 <b>wps</b> オプションを使用します。

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。

## 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ることとなります。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する際にデバイスセキュリティポリシーを施行することにより、WLAN をセキュリティ脅威から保護するよう対策を講じています。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 サーバにその状態を送信すると、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、状態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) と共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、ファーストイーサネット 0 サブインターフェイスのブリッジグループ設定に合わせて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 つでなくてはなりません。この VLAN が、既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 をリスニング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ざら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

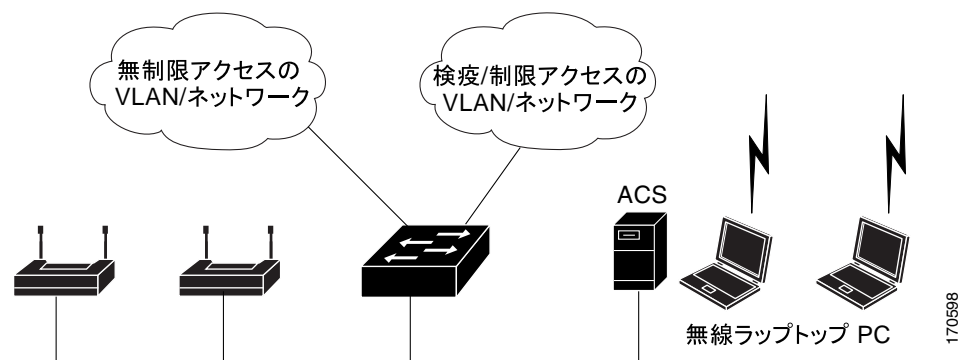


(注) この機能がサポートするのは、VLAN 内のレイヤ 2 モビリティだけです。この機能は、ネットワーク ID を使用するレイヤ 3 モビリティをサポートしません。



(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
!
```